UNIVERSIDAD AUTÓNOMA METROPOLITANA
UNIDAD IZTAPALAPA

TESIS

que con el título

CRIPTOGRAFÍA Y CURVAS ELÍPTICAS

presenta

José de Jesús Ángel Ángel

Para obtener el grado de Maestría en Matemáticas del Departamento de Matemáticas de la Universidad Autónoma Metropolitana-Iztapalapa.

Director de Tesis: Horacio Tapia Recillas

México D.F., 1998

Agradecimientos

Agradezco antes que nada la gran ayuda que recibí por parte de varios investigadores alrededor del mundo, por enviarme de inmediato todos los requerimientos de información que les hice y por sus excelentes respuestas a mis abundantes dudas, siendo esto determinante para el desarollo de mi tesis. Entre los cuales se encuentran: L. Adleman, D. Coppersmith, S. Gao, B. Kalinski, N. Koblitz, A.K. Lenstra, H.W. Lenstra, R. Lercier, A.J. Menezes, V. Miller, A. Miyaji, R.C. Mullin, A. Odlyzko, T. Okamoto, F.C. Piper, R. Rivest, B. Schneier, N.P. Smart, H.C. Williams y R.J. Zuccherato.

Quiero también agradecer la no menos valiosa ayuda de Edna N. Vázquez C. de la UAM-Izt., por su ayuda en la revisión ortográfica. A Shari Oto de RSA Data Security, por su valiosa disposición y atención a mis peticiones y a Ignacio Mendívil G., Director General de SeguriDATA por su apoyo al término de mi trabajo.

Tengo un agradecimiento especial para los profesores: Neal Koblitz, Horacio Tapia R., Carlos Renteria M. y Carlos Signoret P., por haber revisado mi trabajo, por sus valiosas sugerencias, así como también por su interés al aceptar ser sinodales en mi examen de grado.

Finalmente quiero mencionar que este trabajo fue financiado parcialmente por el proyecto "Teoría Algebraica de Códigos, Algebra Conmutativa y Geometría Algebraica", No. 400200-5L0076-E9607, apoyado por CONACYT, cuyo responsable es el Dr. H. Tapia. Este proyecto agrupa hoy en día a investigadores de la UAM-Izt., del IPN y la UNAM interesados en la investigación sobre Criptografía y Teoría de Códigos.

Prefacio

En los últimos años las curvas elípticas han sido incorporadas al estudio de diferentes áreas, como son: pruebas de primacidad, factorización de números enteros, generación de números aleatorios, teoría de códigos y criptografía, entre otras. Este proceso ha sido determinado principalmente por la gran riqueza y complejidad que ofrece la teoría alrededor de las curvas elípticas. Por otra parte, la criptografía ha alcanzado en estos momentos uno de los más altos niveles de atención en todo el mundo. La seguridad que ésta ofrece en el manejo de la información, le ha permitido penetrar a una gran variedad de actividades.

Este trabajo tiene por objetivo general, proporcionar los elementos básicos que combinan las dos ramas antes mencionadas; con esto obtenemos una nueva área dentro de las matemáticas aplicadas a la seguridad en la transmisión de información confidencial: la criptografía elíptica.

El objetivo central es dar los elementos necesarios en la construcción de un criptosistema elíptico, usando una curva elíptica no-supersingular definida sobre el campo finito $\mathbb{F}_{2^n}$, que se obtiene a partir de una curva elíptica no-supersingular anómala definida sobre $\mathbb{F}_2$. Este tipo de curvas tiene la propiedad de que al utilizar el mapeo de Frobenius en la ecuación característica se pueden doblar los puntos racionales de forma eficiente, además de que el número de puntos racionales es fácil de obtener. La seguridad de este tipo de criptosistemas está por el momento garantizada por la elección de una curva elíptica no-supersingular, donde el número de puntos racionales tenga un factor primo alrededor de 45 dígitos, ya que en este caso es aún "imposible" calcular logaritmos discretos sobre curvas elípticas. Además se debe de considerar el proceso de implementación, que requiere efectuar óptimamente operaciones sobre el grupo de los puntos racionales de la curva elíptica, que finalmente se reducen a efectuar operaciones sobre el campo finito de característica 2. Por lo tanto, es preferible buscar la mejor forma de efectuar dichas operaciones; esto se logra, por ejemplo, al elegir una base normal óptima.

Desde 1985, año en que las curvas elípticas fueron propuestas por N. Koblitz y V. Miller para ser usadas en criptografía, las ventajas que éstas han proporcionado se reconocen día tras día. Por ejemplo, el usar llaves de menor longitud, el proporcionar soluciones donde se requiere gran número de firmas electrónicas o donde se tiene espacio y poder de cómputo limitado (el caso de las tarjetas electrónicas), etc., e incluso estan desplazando al sistema RSA.

Todo lo anterior reune algúnos de los rasgos más generales conocidos hasta hoy, de seguridad e implementación de un criptosistema elíptico, los cuáles aquí serán tratados.

Existen en este momento varios problemas por resolver, por ejemplo: el optimizar el cálculo, en forma eficiente, del número de puntos racionales de una curva elíptica definida sobre un campo finito de característica 2 que se genere aleatoriamente, y que este número tenga un factor primo "grande", de al menos 45 dígitos; el mejorar los métodos para efectuar las operaciones sobre el grupo que forman los puntos racionales de una curva elíptica; y principalmente encontrar nuevos "ataques" a éste tipo de sistemas o resolver el problema de calcular logaritmos discretos sobre curvas elípticas no-supersingulares. Estos son algunos problemas que todavía están abiertos y su tratamiento requiere de un estudio más profundo.

El orden que tomaremos es el siguiente: en el capítulo 1 se describe la construcción de los campos finitos, particularmente de característica 2. En el capítulo 2 se detalla algunos de los criptosistemas de llave pública más populares como son el **RSA** y **ElGAMAL**. Para entender el uso de las curvas elípticas, en el capítulo 3 se desarrollan las propiedades básicas de éstas, teniendo especial atención en curvas elípticas definidas sobre un campo finito de característica 2. Finalmente en los capítulos 4 y 5 se ve cómo las curvas elípticas sobre los campos finito $\mathbb{Z}_p$ y $\mathbb{F}_{2^n}$ se pueden usar para diseñar sistemas criptográficos, especialmente se verifican cuáles de éstas son las "mejores", en seguridad e implementación.

Contenido

Capítulo 4: Criptosistemas sobre $E(\mathbb{Z}_p)$

Capítulo 5: Criptosistemas elípticos

Introducción

En varias áreas del quehacer humano como en economía, política, diplomacia, comercio, etc., la información es de gran importancia. Las decisiones que ahí se toman dependen mucho, tanto de la información que se tenga como de la rapidez y seguridad con que se maneje. Por lo tanto, es natural clasificar cierta información como estratégica. El clasificar así a la información tuvo como origen el campo militar y diplomático, precisamente donde la información siempre ha tenido un valor especial. La necesidad de tener información al mismo tiempo en diferentes puntos y la posibilidad de hacerlo obliga a cuidarla en su transmisión de un punto a otro. De entre los muchos aspectos para obtener seguridad en el manejo de la información está la *criptografía.*

Del griego *kryptos* "esconder" y *gráphein* "escribir", la criptografía ([5.13]) estudia las diferentes maneras de "esconder" información en forma escrita, como sonidos o imágenes y así, pueda ser transmitida por cualquier línea insegura, sin temor a ser entendible al ser interceptada por personas no autorizadas. Por otra parte, el *criptoanálisis* estudia técnicas para poder leer mensajes que hayan sido escondidos, gracias a la criptografía. Al conjunto de la criptografía y el criptoanálisis se le conoce como *criptología.*

En México todavía son pocos los usos de la criptografía, aunque existe una variedad de lugares donde es necesaria. Por ejemplo, los bancos, en los cuales la información sobre inversiones, transacciones, créditos, retiros, etc., debe estar asegurada en la medida de su importancia. La Bolsa de Valores, en donde la información necesaria para las diferentes operaciones financieras requiere de ser confidencial y de rápida transmisión, de tal modo que la criptografía debería ser usada para su protección. Las secretarías que tradicionalmente manejan información confidencial son la de Defensa Nacional, de Gobernación, de Relaciones Exteriores, de Hacienda y Crédito Público. Las Cámaras de Senadores y Diputados. Las Procuradurías estatales y federal.

Así como también Pemex, empresas de importación y exportación, hospitales, compañías de seguros, etcétera. En muchas de estas empresas aún no se usa un sistema de seguridad en la información, cosa que se irá dando a futuro o más concretamente tiene que ser adoptado conforme se vayan descubriendo sus beneficios.

De igual forma, en los medios de comunicación que son de fácil intercepción como son, el teléfono convencional, el teléfono celular, la radio, el telégrafo, la televisión, el correo electrónico, etc., no se tiene ninguna seguridad, ya que en nuestro país no existe ningún dispositivo que garantice la confidencialidad en la comunicación al usar todos estos medios; lo cual es diferente en países industrializados, por ejemplo, la compañía de televisión por cable Home Box Office (**HBO**) en los Estados Unidos de Norteamérica fue una de las primeras industrias que usó criptografía en su señal ([5.6]).

Aquí nos proponemos primeramente, describir algunos de los criptosistemas más conocidos ([5]), posteriormente, usar estas ideas para describir criptosistemas basados en el grupo de puntos racionales de una curva elíptica sobre un campo finito ([7]) haciendo énfasis en cuáles de estas curvas es más adecuado implementar criptosistemas.

Notas Históricas

Para resaltar la importancia que ha tenido la criptografía repasemos rápidamente su desarrollo desde los casos más antiguamente conocidos hasta los años 90. Los siguientes datos fueron tomados en su mayor parte de [5.13], y [14].

Uno de los primeros registros que se tienen de la criptografía data del año 400 antes de nuestra era. Los espartanos usaron un dispositivo llamado *Scytale*, el cual consistía de un bastón de cera, alrededor del cual se enrollaba una tira de pergamino el cual tenía un texto ordinario escrito y de esta forma lo encriptaba. Más tarde en Grecia, Polybius inventó un criptosistema que usaba sustituciones. Asimismo, Aeneas Tacticus escribió un trabajo titulado "Sobre la defensa de las Fortificaciones", en el que dedicó un capítulo entero

a la criptografía. Por otra parte, a los romanos se les acredita la invención del criptosistema que consiste en lo siguiente: primero se hace corresponder el alfabeto con los números del 0 al 25.

$$\begin{array}{cccccccccccc} A & B & C & D & E & F & \cdots & X & Y & Z \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & & \updownarrow & \updownarrow & \updownarrow \\ 0 & 1 & 2 & 3 & 4 & 5 & \cdots & 23 & 24 & 25 \end{array}$$

Para mandar un mensaje, por ejemplo "*ATACAR*", éste se convierte en su equivalente numérico $\mathbf{0, 19, 0, 2, 0, 17}$ y ahora se recorre el alfabeto, digamos cinco lugares a la derecha, que equivale a sumar cinco a cada número, obteniendo $\mathbf{5, 24, 5, 7, 5, 22}$ que corresponde a "*FYFHFW*" siendo éste el mensaje encriptado, y sólo quien conoce la llave, el número cinco, podrá recuperar el mensaje original. Mientras que Augusto Cesar usó el corrimiento de un lugar, Julio Cesar usó el número 3 como llave.

La criptología en Europa data de la edad media, en el año 1379 Gabriele de Lavinde de Parma escribió el primer manual sobre criptografía. En 1563 Giambattista della Porta crea un criptosistema con la particularidad de encriptar bloques de dos en dos letras. En 1586 Blaise de Vegenère, generalizó el criptosistema de Julio Cesar usando todos los posibles corrimientos.

En los años 1600, se comenzaron a dar soluciones a los criptosistemas existentes. En 1624 Augustus II, Duque Alemán, escribió el libro "Cryptomenytices et cryptographiae, libri IX", en el que se dedicaba a la solución de varios criptosistemas.

En 1663 en Roma, el jesuita Athanasius Kircher escribió el libro "Polygraphia nova et universalis", el que consiste en una colección de criptosistemas usados en la época.

Para los años 1700, siguieron los tratados dedicados al criptoanálisis, en 1781, a causa de un concurso en Viena, se descubrieron 15 llaves de los sistemas criptográficos de esa época.

A principios del siglo XIX Thomas Jefferson ([5.6]) inventó una máquina constituida por 10 cilindros que estaban montados en un eje de forma independiente, en donde se colocaba el alfabeto y al girar los cilindros, quedaba encriptado el mensaje.

En la Primera Guerra Mundial de 1914−1918 los encriptamientos todavía eran hechos por diferentes asociaciones del alfabeto (permutaciones) y los mensajes eran llevados por el hombre, usando medios de transporte muy lentos, de tal forma que había lugares a los cuales era imposible llevar el mensaje, como a barcos, aviones y submarinos, por lo que se comenzó a usar el teléfono, el telégrafo y la radio. Este último era fácil de transportar, lo que cambió radicalmente las comunicaciones; sin embargo, de este modo los mensajes eran también fácilmente interceptados. Esto justificó incrementar el uso de la criptografía.

Hasta 1918 los encriptamientos se hacían manualmente, lo que causaba muchos errores en el proceso de encriptar y desencriptar, de tal modo que los criptógrafos comenzaron a crear máquinas para tales fines. Por ejemplo, en los Estados Unidos de Norteamérica desde 1861 hasta 1980 se registraron 1769 patentes relacionadas con criptografía. A principios de los años 20 ya había un gran número de estas máquinas, dando gran seguridad en la transmisión de la información. Esta década fue la edad de oro para las máquinas de encriptamiento. Una de las más populares fue la **ENIGMA** creada por el ingeniero alemán Arthur Scherbius. En el Japón inventaron a **PURPLE,** en Norteamérica tenían a **SIGABA** y la versión inglesa se llamo **TYPEX**. De igual forma en 1922, Arvid Damm crea la compañía Aktiebolget Cryptograph, que llegó a ser una de las más grandes proveedoras de equipo criptográfico de la época, no sólo para la industria militar sino también para bancos e industrias comerciales y de servicios.

En 1926 la marina alemana decidió comprar la máquina **ENIGMA,** que fue patentada hasta 1928, fecha en que Scherbius murió. Irónicamente en 1929 su invento se vendió a gran escala en todo el mundo. A finales de la segunda gran guerra de 1939-1945, se habían producido alrededor de 30,000 máquinas **ENIGMAS.** No fue oficial, pero la fuerza aérea alemana era el más grande usuario con 20,000 del total de estas máquinas.

Entre 1943-1945 en **ENIGMA** se procesaban un promedio de 84.000 mensajes mensualmente. Sin embargo, la seguridad de los alemanes no sólo dependía de **ENIGMA.** En 1931 la firma Siemens-Halske patentó un dispositivo en telecomunicación llamado Geheimschreiber, que fue usado durante y después de la Segunda Guerra Mundial.

Después de la guerra se inició el desarrollo de la electrónica y las computadoras. Criptosistemas con algoritmos más sofisticados fueron implementados en la transmisión de la información, pero aún eran usadas máquinas del tipo **ENIGMA** como la M-209 Converter o C-36 inventada por Boris Hagelin, la cual fue usada hasta principio de los años 50 por la armada norteamericana. Como muchas otras actividades, la criptología pasó a ser dominada predominantemente por quienes ganaron la guerra. Así se inició la nueva era en la criptografía, "la electrónica". En la década de los años 50, el panorama mundial estaba dirigido a otra etapa política "la guerra fría". La hegemonía occidental se concentraba en los Estados Unidos de Norteamérica, su localización geográfica le permitió crecer económicamente, de tal modo que era un buen lugar para el desarrollo científico. Por ejemplo, un grupo de exoficiales de la marina crearon a **ERA** (Engineering Research Associates), con el propósito de desarrollar e investigar lo que se refiere a la seguridad. Los proyectos "DEMON" y "GOLDBERG" se dedicaron a hacer criptoanálisis en masa y a gran velocidad.

La necesidad política de penetrar los altos niveles soviéticos y del bloque del Este, hizo que los Estados Unidos adoptaran una mejor organización en el estudio de lo que llamaron Comunicación de Inteligencia (**COMINT**). Cuatro grupos de los Estados Unidos se dedicaban a tal tarea, en particular al Criptoanálisis: *The Army Security Agency* (**ASA**), *The Nacional Security Group* , *The Security Services of the Air Forces*, y *The Armed Forced Security Agency* (**AFSA**). Por razones de eficiencia el presidente H. Truman decidió centralizar los servicios de **COMINT**, creando el 4 de Noviembre de 1952 *la National Security Agency* (**NSA**), que se encargaría de todos los aspectos de "Comunicación de inteligencia".

En Europa otras organizaciones como la *North Atlantic Treaty Organiza-*

tion (**NATO**), desarrollaron tecnología para la seguridad en la información, con la finalidad de crear un dispositivo estándar, es decir, un equipo que sea utilizado por varios países, de esto resultó la KL-7 y KW-27.

Compañías como la International Business Machines Corporation (**IBM**) crearon a principios de los años 60 un sistema llamado **Harvest** que contaba con una unidad de criptoanálisis de alta velocidad; asimismo en 1976 aparece la **CRAY-1** (su inventor Seymour Cray trabajó en **ERA**), la cual es una de las máquinas más veloces hasta la fecha, ésta cuenta con más de 200,000 circuitos integrados. Una de éstas fue adquirida por la **NSA**, para ser utilizada en el criptoanálisis.

A principio de los años 70, la criptografía estaba por iniciar la época de los "circuitos integrados" y el desarrollo en los algoritmos, concretamente, el uso de las matemáticas modernas. Por ejemplo, en 1975 se publica la creación, de **IBM**, el criptosistema Data -Encryption-Standar (**DES**), que ha sido uno de los más usados hasta la fecha ([5.18]).

Un año importante para la criptografía fue el de 1976, cuando W.Diffie y M.Hellman crean el concepto de "**Criptosistema de llave pública**" ([5.14]), es decir, un criptosistema donde la llave de encriptamiento se puede encontrar en un directorio público de usuarios; sin embargo, la llave de desencriptamiento es diferente y no se obtiene fácilmente de la primera. En otras palabras, para encriptar se usa una función invertible f, que sea fácil de calcular, pero la inversa f^{-1} que se usa para desencriptar, debe de ser difícil de obtener a partir de f y de otra información relevante.

Poco más tarde, en 1978 se da a conocer el criptosistema de llave pública más seguro y usado hasta la fecha, el **RSA** ([6.1]). Sus inventores R.L. Rivest, A. Shamir y L. Adleman del **MIT** proponen la función de un sólo sentido que utiliza el exponente módulo un número entero n, producto de dos números primos y que tiene como seguridad la dificultad de factorizar a un número n, digamos de 150 dígitos. La necesidad de romper este criptosistema desarrolla la teoría para factorizar números grandes, cosa que después justifica la aparición de las curvas elípticas en criptografía.

Otro sistema que se ha mantenido hasta hoy, es el propuesto por ElGamal en 1984 ([15.9]), éste basa su seguridad en el problema del logaritmo discreto que aún no se ha podido resolver satisfactoriamente.

En la mayor parte del mundo existen centros de investigación en la seguridad de la información; por ejemplo, en 1988 se crea el **European Institute for System Security** ([5.8]), que entre sus objetivos está el desarrollar investigación en todos los campos que tengan que ver con la seguridad de la información, en particular con la criptografía. Varios de sus miembros son reconocidos matemáticos.

En los últimos 15 años muchas áreas de las matemáticas han podido ser usadas para crear criptosistemas. Como ya lo hemos hecho notar, entre otras se encuentran los campos finitos y factorización de números enteros. Otros ejemplos son: en 1970 R.J. McEliece ([15.18]) desarrolló un criptosistema de llave pública basado en códigos detectores-correctores de errores; en los años 80 V. Varadharajan ([15.5]) propuso distintas estructuras de anillos que pueden ser aplicadas en la generalización del sistema **RSA.** En 1984 Lidl y Müller ([2.31]) proponen polinomios de permutación; en 1988 J. Buchmann y H. Williams ([15.4]) proponen usar campos cuadráticos imaginarios; en 1995 R. Scheidler y H. Williams usan campos ciclotómicos, etcétera. Otro tipo de protocolo propuesto recientemente por el grupo de la **IBM** usa la teoría de incertidumbre y se le conoce como criptografía cuántica ([15.7]).

En 1985, de forma independiente V. Miller ([7.3]) y N. Koblitz ([7.2]) usan la teoría de curvas elípticas, para crear criptosistemas, lo cual es el objetivo principal a tratar. Estas curvas fueron propuestas por Lenstra ([12.1]), para factorizar números enteros. La ventaja tomada es la estructura de grupo abeliano que tienen los puntos racionales de una curva elíptica, y por lo tanto, pueden ser implementados criptosistemas usando ahora los puntos racionales en lugar de los elementos del grupo multiplicativo de un campo finito.

En 1988 Newbridge Microsystems Inc. ([7.1]) fabricó un "chip" para implementar varios criptosistemas basados en la aritmética del campo finito $GF(2^{593})$, donde la multiplicación de dos elementos del campo toma 1300 ciclos del reloj, mientras que calcular un inverso toma cerca de 50,000 ciclos

de reloj. El "chip" tiene una velocidad de reloj de 20Mhz, por lo tanto, la multiplicación y el inverso toma 0.065ms y 2.5ms respectivamente.

Recientemente dispositivos Very Large Scale Integration (**VLSI**) han sido construidos para operar la aritmética del campo finito $GF(2^{155})$ ([7.1]), en el cual una multiplicación toma 156 ciclos de reloj, mientras que un inverso toma 3800 ciclos. El "chip" tiene una velocidad de 40Mhz, por lo tanto, la multiplicación y el inverso toma 0.004ms y 0.095ms respectivamente. Estos dispositivos pueden ser usados para implementar criptosistemas usando curvas elípticas.

En 1992 Crandall ([7.1]) describe una implementación del criptosistema de Diffie y Hellman, usando curvas elípticas definidas sobre el campo $GF(p^k)$, donde p es de la forma $2^r - s$, con s pequeño. Crandall presenta un método para realizar operaciones en un campo finito que elimina las divisiones, este sistema fue llamado Fast Elliptic Encryption (**FEE**), adaptado por la compañía de computadoras **NeXT** para implementarlo en sus productos.

Hoy en día sería imposible mencionar el gran desarrollo que ha alcanzado la investigación y la comercialización de la criptografía. Más referencias con información documentada se pueden encontrar en el anexo III.

Por último diremos que entre la gran variedad de Universidades y compañías privadas en el mundo que investigan y desarrollan tecnología en criptografía están: The University of Warterloo, the Massachusetts Institute of Technology, University of California in Berkeley, Stanford, University of Wisconsin in Milwaukee, the Royal Holloway University of London, etc., y entre las compañías privadas estan AT&T (American Telegraph and Telephone), NTT (Nippon Telegraph and Telephone), RSA Data Security, IBM, Siemens, Matsushita, Certicom, Thompson, etcétera.

Las anteriores notas históricas sobre la criptología muestran, que como muchas áreas del conocimiento, ésta ha estado ligada al quehacer humano, desde los inicios de la humanidad.

Capítulo 1

Campos finitos

Introducción: El objetivo de este capítulo es recordar algunos resultados básicos sobre campos finitos (su existencia, construcción, aritmética, etcétera), y de esta forma proporcionar lo necesario sobre el tema que será utilizado en capítulos posteriores.

Para un estudio más profundo sobre los campos finitos se puede consultar [2.1], [2.2], [2.3], [2.4].

1.1 Existencia y construcción de campos finitos

DEFINICIÓN 1.1.1: Un anillo conmutativo $(K, +, \times)$, se dice que es un *campo* si $K^* = K - \{0\}$ es un grupo conmutativo bajo la operación producto " $\times$ ". El campo se dice finito si la cardinalidad $|K|$ de K es finita.

El ejemplo más sencillo de un campo finito son los enteros módulo un número primo p, $\mathbf{Z}_p$. Se verá más adelante que en base a estos campos se pueden construir todos los campos finitos. Por otro lado, si consideramos al conjunto $\mathbf{F}_p = \{0, 1, ..., p-1\}$ y a $\varphi : \mathbf{Z}_p \to \mathbf{F}_p$, $\varphi(\overline{a}) = a$, $a \in \{0, 1, ..., p-1\}$, podemos inducir estructura de campo a $\mathbf{F}_p$.

En los siguientes resultados se formalizará la construcción de campos finitos.

TEOREMA 1.1.2: Sea α un elemento algebraico sobre el campo K, de grado n y g el polinomio minimal de α sobre K. Entonces:

i) $K(\alpha)$ es isomorfo a $K[x]/(g)$.

ii) $[K(\alpha) : K] = n$ y $\{1, \alpha, \ldots, \alpha^{n-1}\}$ es una base de $K(\alpha)$ sobre K.

DEMOSTRACIÓN:

i) la función $\varphi : K[x] \to K(\alpha)$, definida por $\varphi(f) = f(\alpha)$ para $f \in K[x]$, es un homomorfismo de anillos con núcleo (g). Si S es la imagen de φ, S es isomorfo a $K[x]/(g)$, como g es irreducible, entonces éste es un campo y por lo tanto, S es un campo. Como $K \subseteq S \subseteq K(\alpha)$ y $\alpha \in S$, entonces $S = K(\alpha)$.

ii) Puesto que $S = K(\alpha)$, cualquier $\beta \in K(\alpha)$ puede ser escrito de la forma $\beta = f(\alpha)$ para algún $f(x) \in K[x]$. Por el algoritmo de la división $f = qg + r$ con $gr(r) < gr(g) = n$, entonces $\beta = f(\alpha) = q(\alpha)g(\alpha) + r(\alpha) = r(\alpha)$. Por lo tanto, β es una combinación lineal de $1, \alpha, \ldots, \alpha^{n-1}$ con coeficientes en K. Por otro lado si $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0$ para ciertos $a_i \in K$, el polinomio $h(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in K[x]$ tiene a α como raíz y es así un múltiplo de g. Como $gr(h) < n$, entonces la única posibilidad es que $h = 0$, es decir, $a_i = 0$ para toda i, de donde los elementos $1, \alpha, \ldots, \alpha^{n-1}$ son linealmente independientes sobre K.

El teorema anterior da un método para construir campos finitos, donde al campo K le llamaremos *campo base*. En gran parte de este trabajo el campo base será $\mathbb{F}_2$.

PROPOSICIÓN 1.1.3: Sea F un campo finito que contiene a un subcampo K con q elementos, entonces F tiene q^m elementos, donde $m = [F : K]$.

DEMOSTRACIÓN: Se sigue de que F es un espacio vectorial sobre K.

TEOREMA 1.1.4 (Fundamental de los campos finitos): Para cualquier primo p y cualquier entero positivo n existe un campo finito con p^n elementos. Cada campo finito con $q = p^n$ elementos es isomorfo al campo de descomposición F, del polinomio $x^q - x$ sobre $\mathbb{F}_p$, es decir, $F = \mathbb{F}_p(\alpha_1, \ldots, \alpha_n)$ para $\alpha_i \in F$, raíces de $x^q - x$.

DEMOSTRACIÓN: Si $q = p^n$ consideramos al polinomio $x^q - x \in \mathbb{F}_p[x]$ y sea F su campo de descomposición sobre $\mathbb{F}_p$. Este polinomio tiene q raíces distintas en F, ya que no puede tener raíces múltiples, puesto que su derivada es $qx^{q-1} - 1 = -1$ en $\mathbb{F}_p[x]$. El subconjunto $S = \{a \in F : a^q - a = 0\}$ es un subcampo de F. Como $x^q - x$ se debe de descomponer en S, ya que éste

contiene todas sus raíces, entonces $S = F$ que es el campo finito con q elementos.

Para ver la unicidad obsérvese que si F es un campo con $q = p^n$ elementos, entonces F tiene característica p, es decir, que F contiene a $\mathbf{F}_p$ como subcampo, así F es el campo de descomposición de $x^q - x$ sobre $\mathbf{F}_p$. Como consecuencia de la unicidad, salvo isomorfismos de campos de descomposición, tenemos la unicidad del campo finito.

A $\mathbf{F}_q$ también se le llama campo de Galois, denotado por $GF(q)$.

Ejemplos de campos finitos:

i) El anillo $\mathbf{Z}_p$, de las clases residuales módulo un número primo p.

ii) El campo más pequeño que no tiene orden un primo es $\mathbf{F}_{2^2}$ y este se construye de la siguiente manera:

Sea $\mathbf{F}_2 = \{0, 1\}$ el campo base y $f(x) = x^2 + x + 1 \in \mathbf{F}_2[x]$ un polinomio irreducible en $\mathbf{F}_2[x]$ (basta ver que f no tiene raíces en $\mathbf{F}_2$, ya que $gr(f) \leq 3$). Por el teorema 1.1.2, $\mathbf{F}_2[x]/(f)$ es un campo con 4 elementos. Por el mismo resultado $\mathbf{F}_2[x]/(f) \simeq \mathbf{F}_2(\alpha)$ donde α es una raíz del polinomio irreducible f, con $\{1, \alpha\}$ una base de $\mathbf{F}_2(\alpha)$ sobre $\mathbf{F}_2$ como espacio vectorial. Así $\mathbf{F}_{2^2} \simeq \mathbf{F}_2[x]/(f) \simeq \mathbf{F}_2(\alpha) = \{0, 1, \alpha, \alpha + 1\}$ donde $\alpha^2 = 1 + \alpha$.

Las operaciones en este campo para la suma, salvo las obvias, se obtienen como sigue:

$$\begin{array}{lcll} 1 & + & 1 & = 0 \\ 1 & + & \alpha & = 1 + \alpha \\ 1 & + & (1 + \alpha) & = \alpha \\ \alpha & + & \alpha & = 0 \\ \alpha & + & (1 + \alpha) & = 1 \\ 1 + \alpha & + & (1 + \alpha) & = 0 \end{array}$$

Para el producto tenemos:

$$\begin{array}{lcll} \alpha & \cdot & \alpha & = 1 + \alpha \\ \alpha & \cdot & (1 + \alpha) & = 1 \\ (1 + \alpha) & \cdot & (1 + \alpha) & = \alpha \end{array}$$

Obsérvese que $(\mathbf{F}_{2^2}^*, \cdot)$ resulta ser un grupo, el cual es cíclico generado por α, esto es: $\alpha^0 = 1, \alpha^1 = \alpha$, y $\alpha^2 = 1 + \alpha$.

Para la construcción de campos más grandes tenemos la necesidad de conocer polinomios irreducibles sobre el campo base. En la actualidad existen tablas de polinomios irreducibles que se pueden usar para varios casos (ver por ejemplo [2.16], [2.17], [2.18], [2.19], [2.20], [2.21], [2.22]). En nuestro caso tomaremos algunos de la lista que se encuentra en [1.10].

iii) En orden creciente obsérvese que no existe un campo con 6 elementos, ya que 6 no es potencia de algún número primo (teorema 1.1.4).

Ahora, construyamos al campo $\mathbf{F}_{2^3}$, es decir, un campo de 8 elementos. Como $8 = 2^3$ basta considerar al campo base $\mathbf{F}_2$ y añadir una raíz de un polinomio irreducible de grado 3, siendo éste $f(x) = x^3 + x + 1$. Entonces $\mathbf{F}_2[x]/(f)$ es un campo con 8 elementos isomorfo a $\mathbf{F}_2(\alpha)$ donde $\alpha^3 = \alpha + 1$. Los elementos de este campo son:

$$\mathbf{F}_{2^3} = \left\{0, 1, \alpha, \alpha^2, 1+\alpha, 1+\alpha^2, \alpha+\alpha^2, 1+\alpha+\alpha^2\right\}$$

La tabla de sumar es:

$$\begin{aligned}
1 + \alpha &= 1 + \alpha, \\
1 + \alpha^2 &= 1 + \alpha^2, \\
1 + (1+\alpha) &= \alpha, \\
1 + (1+\alpha^2) &= \alpha^2, \\
1 + (\alpha+\alpha^2) &= 1 + \alpha + \alpha^2, \\
1 + (1+\alpha+\alpha^2) &= \alpha + \alpha^2, \\
\alpha^2 + (1+\alpha) &= 1 + \alpha + \alpha^2, \\
\alpha^2 + (1+\alpha^2) &= 1, \\
\alpha^2 + (\alpha+\alpha^2) &= \alpha, \\
\alpha^2 + (1+\alpha+\alpha^2) &= 1 + \alpha, \\
(1+\alpha^2) + (\alpha+\alpha^2) &= 1 + \alpha, \\
(1+\alpha^2) + (1+\alpha+\alpha^2) &= \alpha,
\end{aligned}$$

$$\begin{aligned}
\alpha + \alpha^2 &= \alpha + \alpha^2, \\
\alpha + (1+\alpha) &= 1, \\
\alpha + (1+\alpha^2) &= 1 + \alpha + \alpha^2, \\
\alpha + (\alpha+\alpha^2) &= \alpha^2, \\
\alpha + (1+\alpha+\alpha^2) &= 1 + \alpha^2, \\
(1+\alpha) + (1+\alpha^2) &= \alpha + \alpha^2, \\
(1+\alpha) + (\alpha+\alpha^2) &= 1 + \alpha^2, \\
(1+\alpha) + (1+\alpha+\alpha^2) &= \alpha^2, \\
(\alpha+\alpha^2) + (1+\alpha+\alpha^2) &= 1
\end{aligned}$$

La tabla de multiplicar es:

$$\begin{aligned}
\alpha \cdot \alpha &= \alpha^2, \\
\alpha \cdot \alpha^2 &= 1+\alpha, \\
\alpha \cdot (1+\alpha) &= \alpha+\alpha^2, \\
\alpha \cdot (1+\alpha^2) &= 1, \\
\alpha \cdot (\alpha+\alpha^2) &= 1+\alpha+\alpha^2, \\
\alpha \cdot (1+\alpha+\alpha^2) &= 1+\alpha^2, \\
(1+\alpha) \cdot (1+\alpha) &= 1+\alpha^2, \\
(1+\alpha) \cdot (1+\alpha^2) &= \alpha^2, \\
(1+\alpha) \cdot (\alpha+\alpha^2) &= 1, \\
(1+\alpha) \cdot (1+\alpha+\alpha^2) &= \alpha, \\
(\alpha+\alpha^2) \cdot (\alpha+\alpha^2) &= \alpha, \\
(\alpha+\alpha^2) \cdot (1+\alpha+\alpha^2) &= \alpha^2,
\end{aligned}$$

$$\begin{aligned}
\alpha^2 \cdot \alpha^2 &= \alpha+\alpha^2, \\
\alpha^2 \cdot (1+\alpha) &= 1+\alpha+\alpha^2, \\
\alpha^2 \cdot (1+\alpha^2) &= \alpha, \\
\alpha^2 \cdot (\alpha+\alpha^2) &= 1+\alpha^2, \\
\alpha^2 \cdot (1+\alpha+\alpha^2) &= 1, \\
(1+\alpha^2) \cdot (1+\alpha^2) &= 1+\alpha+\alpha^2, \\
(1+\alpha^2) \cdot (\alpha+\alpha^2) &= 1+\alpha, \\
(1+\alpha^2) \cdot (1+\alpha+\alpha^2) &= \alpha+\alpha^2, \\
(1+\alpha+\alpha^2) \cdot (1+\alpha+\alpha^2) &= 1+\alpha,
\end{aligned}$$

En este caso tenemos que $\mathbf{F}_{2^3}^* = \{1, \alpha, \alpha^2, \ldots, \alpha^6\}$, es decir, α es un generador del grupo multiplicativo del campo $\mathbf{F}_{2^3}^*$.

iv) Para $n = 9$ tenemos que es necesario un polinomio irreducible f de grado 2 para que $\mathbf{F}_3[x]/(f)$ sea un campo con nueve elementos. Basta entonces considerar a $f(x) = x^2 - x - 1$. El proceso es similar al ejemplo anterior.

v) Para enteros como $10, 12, 14, 15, 18, 20, 21, 22, 24$ no existe un campo con tales elementos, ya que estos números no son potencia de un número primo. Para los enteros $11, 13, 17, 19, 23$ el campo es el correspondiente $\mathbf{Z}_{11}, \mathbf{Z}_{13}, \mathbf{Z}_{17}, \mathbf{Z}_{19}, \mathbf{Z}_{23}$.

Para terminar con este ejemplo diremos que para construir los campos con $16 = 2^4$ y $25 = 5^2$ elementos se pueden considerar a los polinomios $f_1(x) = x^4 + x + 1 \in \mathbf{F}_2[x]$ y $f_2(x) = x^2 - 2x - 2 \in \mathbf{F}_5[x]$, respectivamente.

1.2 Bases en un campo finito

Como F_{p^n} es un espacio vectorial sobre F_p, entonces existe una base, de ésta depende la representación de los elementos del campo finito, y también la manera de efectuar las operaciones. En el capítulo 5, veremos cuál de estas representaciones es más conveniente para usar en criptografía.

En esta sección solamente veremos los resultados principales respecto a las bases llamadas normales.

TEOREMA 1.2.1: Si F_q es un campo finito, entonces el grupo multiplicativo F_q^* es cíclico.

DEMOSTRACIÓN: Sea $q-1 = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$ la descomposición del orden del grupo F_q^* y $b_i = a_i^{(q-1)/p_i}$ donde a_i es un elemento no cero que no es raíz del polinomio $x^{(q-1)/p_i} - 1$. Se puede mostrar entonces que $b = b_1 \cdots b_m$ es un generador del grupo F_q^*.

Un generador del grupo cíclico F_q^* es llamado *elemento primitivo* de F_q.

DEFINICIÓN 1.2.2: Sea $K = \mathsf{F}_q$ y $F = \mathsf{F}_{q^m}$, una base de F sobre K que consiste de α y sus conjugados, es decir, el conjunto $\left\{\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}\right\}$ es llamada *base normal.* Si α es elemento primitivo, entonces la base se llama *base normal primitiva.*

TEOREMA 1.2.3: Para cualquier campo finito K y cualquier extensión finita F de K existe una base normal de F sobre K.

DEMOSTRACIÓN: Sea $K = \mathsf{F}_q$ y $F = \mathsf{F}_{q^m}$, $m \geq 2$, y los automorfismos de F sobre K dados por $I, \sigma, \sigma^2, \ldots, \sigma^{m-1}$, donde $\sigma(\alpha) = \alpha^q$ para $\alpha \in F$, σ, es el automorfismo de Frobenius. Estos automorfismos pueden ser considerados como operadores lineales del espacio vectorial F sobre K. Puesto que $\sigma^m = I$, el polinomio $x^m - 1 \in K[x]$ anula a σ. Como para $I, \sigma, \ldots, \sigma^{m-1}$ vistos como endomorfismos de F^* ningún polinomio no cero en $K[x]$ de grado menor que m anulan a σ. Entonces, $x^m - 1$ es el polinomio característico de σ. Luego, existe un elemento $\alpha \in F$ tal que $\alpha, \sigma(\alpha), \ldots, \sigma^{m-1}(\alpha)$ generan a

F y así forman una base de F sobre K. Como esta base consiste de α y sus conjugados con respecto a K, estos forman una base normal de F sobre K.

El siguiente resultado dice cuándo una colección de elementos es base.

El *discriminante* $\triangle_{F/K}(\alpha_1, ..., \alpha_m)$ de los elementos $\alpha_1, ..., \alpha_m \in F$ es el siguiente determinante $m \times m$.

$$\triangle_{F/K}(\alpha_1, ..., \alpha_m) = \left| \ tr_{F/K}(\alpha_i \alpha_j) \ \right|, \ 1 \leq i, j \leq m.$$

donde $tr_{F/K}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}}$, es la traza de α.

TEOREMA 1.2.4 ([2.1]): Sea K un campo finito, F una extensión de K de grado m, y $\alpha_1, \alpha_2, ..., \alpha_m \in F$. Entonces $\{\alpha_1, \alpha_2, ..., \alpha_m\}$ forman una base de F sobre K si y sólo si $\triangle_{F/K}(\alpha_1, \alpha_2, ..., \alpha_m) \neq 0$.

PROPOSICIÓN 1.2.5: Los elementos $\alpha_1, ..., \alpha_m$ de $\mathbf{F}_{q^m}$ forman una base de $\mathbf{F}_{q^m}$ sobre $\mathbf{F}_q$ si y sólo si

$$\begin{vmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_m \\ \alpha_1^q & \alpha_2^q & \cdots & \alpha_m^q \\ \vdots & \vdots & & \vdots \\ \alpha_1^{q^{m-1}} & \alpha_2^{q^{m-q}} & \cdots & \alpha_m^{q^{m-1}} \end{vmatrix} \neq 0$$

DEMOSTRACIÓN: Sea A la matriz $m \times m$ cuya entrada (i, j) es $\alpha_j^{q^{i-1}}$. Entonces $A^T A = B$, donde B es la matriz $m \times m$, con entradas (i, j) igual a $tr_{F/K}(\alpha_i \alpha_j)$. Por lo tanto, $\det(B) = \triangle_{F/K}(\alpha_1, \alpha_2, ..., \alpha_m) = \det(A)^2$, y así el resultado se sigue del teorema anterior.

A continuación tenemos un criterio relativamente simple para verificar si una base es normal.

TEOREMA 1.2.6 ([2.1]): Para $\alpha \in \mathbf{F}_{q^m}$, $\left\{\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}\right\}$ es una base normal de $\mathbf{F}_{q^m}$ sobre $\mathbf{F}_q$ si y sólo si los polinomios $x^m - 1$ y $\alpha x^{m-1} + \alpha^q x^{m-2} + \cdots + \alpha^{q^{m-2}} x + \alpha^{q^{m-1}}$ son primos relativos en $\mathbf{F}_{q^m}[x]$.

1.3 Introducción a los campos ciclotómicos

Un método para encontrar polinomios irreducibles, los cuales pueden ser utilizados para la construcción de campos finitos, usa polinomios ciclotómicos y se reduce a factorizar dichos polinomios. Algunos algoritmos de factorización de polinomios se pueden encontrar en [2.23], [2.24], [2.28], [2.29].

Sea K un campo y n un entero positivo, el *$n-$ésimo campo ciclotómico* sobre K denotado por $K^{(n)}$ es el campo de descomposición del polinomio $x^n - 1$. Las raíces de $x^n - 1$ en $K^{(n)}$ son llamadas las raíces $n-$ésimas de la unidad sobre K y el conjunto de estas raíces será denotado por $E^{(n)}$.

Un generador del grupo cíclico $E^{(n)}$ se llama *raíz $n-$ésima primitiva de la unidad* sobre K. No es difícil ver que existen $\phi(n)$ diferentes raíces $n-$ésimas primitivas de la unidad, donde ϕ es la función de Euler ([2.1]). Si ζ es una de ellas, entonces ζ^s es otra, donde s es primo relativo con n.

DEFINICIÓN 1.3.1: Sea K un campo de característica p, n un entero no divisible por p, y ζ una raíz primitiva $n-$ésima de la unidad sobre K. Entonces el polinomio

$$Q_n(x) = \prod_s (x - \zeta^s)$$

con $mcd(s, n) = 1$, se llama el *$n-$ésimo polinomio ciclotómico* sobre K.

El polinomio $Q_n(x)$ es independiente de la elección de ζ por definición, y su grado es $\phi(n)$.

Por ejemplo, si p es un número primo entonces tenemos que $Q_p(x) = 1 + x + x^2 + \cdots + x^{p-1}$.

Veamos un resultado sobre campos ciclotómicos que nos será útil en la construcción de campos finitos.

TEOREMA 1.3.2: El campo ciclotómico $K^{(n)}$ es una extensión algebraica simple de K. Si $K = \mathsf{F}_q$ con $mcd(q, n) = 1$, entonces Q_n se factoriza en $\frac{\varphi(n)}{d}$ distintos polinomios mónicos irreducibles en $K[x]$ de grado d, $K^{(n)}$ es el campo de descomposición de cualquier factor irreducible sobre K y $\left[K^{(n)} : K\right] = d$, donde d es el menor entero positivo tal que $q^d \equiv 1 \ mod \ n$.

DEMOSTRACIÓN:

Si existe una raíz $n-$ésima primitiva de la unidad ζ sobre K, entonces $K^{(n)} = K(\zeta)$. Además $\zeta \in \mathsf{F}_{q^k}$ si y sólo si $\zeta^{q^k} = \zeta$ equivalente a $q^k \equiv 1 \ mod \ n$. El mínimo entero para lo cual es válido es, $k = d$, y por lo tanto $\zeta \in \mathsf{F}_{q^d}$, así el polinomio minimal de ζ sobre F_q tiene grado d y puesto que ζ es una raíz arbitraria de Q_n se obtiene lo deseado.

Veamos ahora cómo se puede usar el resultado anterior para representar los elementos de un campo finito F_q con $q = p^n$, donde p es la característica de F_q.

Sea F_q, con $q = p^n$ consideremos al $(q-1)-$polinomio ciclotómico sobre F_p, $Q_{q-1}(x) \in \mathsf{F}_p[x]$. Este polinomio se puede factorizar en elementos irreducibles de $\mathsf{F}_p[x]$, cada uno de ellos del mismo grado (teorema 1.3.2). Por lo tanto, una raíz de cualquiera de estos factores es una raíz $(q-1)-$ésima primitiva de la unidad sobre F_p y así un elemento primitivo de F_q.

Ejemplos:

i) Para construir a F_9, notemos que $\mathsf{F}_9 = \mathsf{F}_3^{(8)}$, esto es el 8-campo ciclotómico sobre F_3, como $Q_8(x) = 1 + x^4 \in \mathsf{F}_3[x]$, entonces factorizando este polinomio tenemos

$$Q_8(x) = \left(2 + x + x^2\right)\left(2 + 2x + x^2\right)$$

ii) Se puede encontrar una forma explícita para calcular a Q_n ([2.1]), sin embargo para n un primo ya la tenemos. Como ejemplo tenemos a $\mathsf{F}_{2^5} = \mathsf{F}_{32} = \mathsf{F}_2^{(31)}$, en este caso 31 es primo y consideramos a:

$$Q_{31}(x) = 1 + x + x^2 + x^3 + \cdots + x^{30} \in \mathsf{F}_2[x]$$

al factorizar obtenemos

$$\begin{aligned} Q_{31}(x) &= (1+x^2+x^5)(1+x^3+x^5)(1+x+x^2+x^3+x^5) \\ &\quad (1+x+x^2+x^4+x^5)(1+x+x^3+x^4+x^5) \\ &\quad (1+x^2+x^3+x^4+x^5) \end{aligned}$$

Si ζ es una raíz de, digamos $(1+x^2+x^5)$, entonces ζ genera al campo finito $\mathsf{F}_{32} = \mathsf{F}_2(\zeta)$.

iii) Como otro ejemplo tenemos al campo $\mathsf{F}_{2^7} = \mathsf{F}_{128} = \mathsf{F}_2^{(127)}$, en este caso también 127 es primo y tenemos:

$$Q_{127}(x) = 1 + x + x^2 + \cdots + x^{126}$$

cuya factorización es

$$\begin{aligned} Q_{127}(x) &= (1+x+x^7)(1+x^3+x^7)(1+x+x^2+x^3+x^7) \\ &\quad (1+x^4+x^7)(1+x^2+x^3+x^4+x^7) \\ &\quad (1+x+x^2+x^5+x^7)(1+x+x^3+x^5+x^7) \\ &\quad (1+x^3+x^4+x^5+x^7)(1+x+x^2+x^3+x^4+x^5+x^7) \\ &\quad (1+x^6+x^7)(1+x+x^3+x^6+x^7) \\ &\quad (1+x+x^4+x^6+x^7)(1+x^2+x^4+x^6+x^7) \\ &\quad (1+x^2+x^5+x^6+x^7)(1+x+x^2+x^3+x^5+x^6+x^7) \\ &\quad (1+x^4+x^5+x^6+x^7)(1+x+x^2+x^4+x^5+x^6+x^7) \\ &\quad (1+x^2+x^3+x^4+x^5+x^6+x^7) \end{aligned}$$

De forma silmilar, si ζ es una raíz de $(1+x+x^7)$, entonces ζ es un generador de $\mathsf{F}_{2^7} = \mathsf{F}_2(\zeta)$.

Sea $f(x) \in \mathsf{F}_q[x]$ un polinomio no cero. Si $f(0) \neq 0$, entonces el menor entero positivo e, tal que f divide a $x^e - 1$, es llamado el *orden* de f denotado por $ord(f)$. Si $f(0) = 0$, entonces $f(x) = x^k g(x)$, y el orden de f es el orden de g.

PROPOSICIÓN 1.3.3: El número de polinomios mónicos irreducibles sobre F_q de grado m y orden e es igual a $\frac{\varphi(e)}{m}$, donde $e \geq 2$ y m es el orden de q en el anillo $\mathbb{Z}_e$. Es 2 si $m = e = 1$, e igual a 0 en los demás casos. En particular el grado de un polinomio irreducible en $\mathsf{F}_q[x]$ de orden e es igual al orden de q módulo e.

DEMOSTRACIÓN: Sea $f(x) \in \mathsf{F}_q[x]$ irreducible con $f(0) \neq 0$, por lo tanto, $ord(f) = e$, si y sólo si, todas las raíces de f son raíces $e-$ésimas primitivas de la unidad en F_q. En otras palabras, tenemos que $ord(f) = e$, si y sólo si, f divide al polinomio ciclotómico Q_e. Entonces cualquier factor irreducible de Q_e tiene el mismo grado m, el menor entero positivo tal que $q^m \equiv 1 \ mod \ e$ y el número de tales factores está dado por $\frac{\varphi(e)}{m}$. Para $m = e = 1$, tenemos que tomar en cuenta el polinomio irreducible mónico $f(x) = x$.

Ejemplos:

i) Consideremos a $\mathsf{F}_2[x]$. Para construir un campo de $2^2 = 4$ elementos necesitamos un polinomio primitivo de grado 2, en este caso tenemos que hay $\frac{\varphi(2^2-1)}{2} = 1$ polinomios irreducibles primitivos.

ii) Para construir un campo de $2^3 = 8$ elementos tenemos a $\frac{\varphi(2^3-1)}{3} = 2$ polinomios primitivos de grado 3.

iii) Para un campo de 2^{50} elementos tendriamos $\frac{\varphi(2^{50}-1)}{50} = 13122000000000$ elecciones de un polinomio primitivo.

iv) Para el campo de 2^{155} elementos, tenemos

$$\frac{\phi(2^{155}-1)}{155} = 28420696843897870538598254345347913444 \times 10^7$$

posibilidades de elegir un polinomio primitivo.

Los siguientes son algunos ejemplos de polinomios ciclotómicos expresados como productos de factores irreducibles, los cuales se pueden usar para la construcción de campos finitos que son extensiones de F_2.

i) $Q_7(x) = (1 + x + x^3)(1 + x^2 + x^3)$

Por lo tanto, estos son los polinomios primitivos que además vemos que en efecto sólo son 2, esto es, $\frac{\phi(2^3-1)}{3} = 2$.

ii) $Q_{15}(x) = (1 + x + x^4)(1 + x^3 + x^4)$

De forma análoga, estos son los dos únicos polinomios primitivos de grado 4.

iii)

$$\begin{aligned} Q_{63} &= (1+x+x^6)(1+x+x^3+x^4+x^6)(1+x^5+x^6) \\ &\quad (1+x+x^2+x^5+x^6)(1+x^2+x^3+x^5+x^6) \\ &\quad (1+x+x^4+x^5+x^6) \end{aligned}$$

Estos son los polinomios primitivos de grado 6 que se utilizan para construir un campo de 64 elementos.

iv) Conforme el grado sea mayor, el número de polinomios primitivos crece según $\frac{\phi(2^n-1)}{n}$, lo cual es muy rápido. Por ejemplo, para grado 7 tenemos 18 polinomios primitivos.

En la siguente tabla (se obtuvo con *Mathematica*) se da el grado del polinomio, el número de polinomios primitivos que hay de ese grado, y sólo un ejemplo de ellos.

Grado	*Número*	*Ejemplo*
9	48	x^9+x^4+1
10	60	$x^{10}+x^3+1$
11	176	$x^{11}+x^2+1$
15	1800	$x^{15}+x+1$
20	24000	$x^{20}+x^3+1$
25	1296000	$x^{20}+x^3+1$
30	17820000	$x^{30}+x^6+x^4+x+1$
35	929275200	$x^{35}+x^2+1$
40	11842560000	$x^{40}+x^5+x^4+x^3+1$
49	11398311767808	$x^{49}+x^6+x^5+x^4+1$
50	13122000000000	$x^{50}+x^4+x^3+x^2+1$
53	1699179983040000	$x^{53}+x^6+x^2+x+1$
61	37800705069076950	$x^{61}+x^5+x^2+x+1$
67	2202596295934991760	$x^{67}+x^5+x^2+x+1$
73	129085132425950929920	$x^{73}+x^4+x^3+x^2+1$
79	7648581626983221210888	$x^{79}+x^4+x^3+x^2+1$
85	4404402020209996649718000	$x^{85}+x^8+x^2+x+1$
100	570767634×10^{19}	$x^{100}+x^8+x^7+x^2+1$.

Capítulo 2

Criptografía

En este capítulo damos las definiciones básicas para entender lo que es un criptosistema ([5]). También se plantea el problema del logaritmo discreto (PLD) sobre campos finitos ([3]), y su estado actual. Posteriormente se describen los criptosistemas de Rivest, Shamir y Adleman (RSA) y el de ElGamal; los cuales representan dos de las principales corrientes de la mayoría de criptosistemas de llave pública: la primera basa su seguridad en la dificultad de factorizar un número entero y la segunda en la dificultad de resolver el PLD. Un importante motivo por el cual se debe de entender el sistema de ElGamal es, que tal criptosistema se usa en los capítulos siguientes, usando en lugar del grupo multiplicativo de un campo finito F_q, al grupo de puntos racionales de una curva elíptica sobre un campo finito. Finalmente se comentan otros criptosistemas que permiten ver qué tan amplio es el uso de las matemáticas modernas en esta área.

2.1 Criptosistemas

Comenzaremos haciendo el siguiente planteamiento: un usuario **A** desea enviar un mensaje m a otro usuario **B**, por medio de una línea de transmisión **L** que se supone insegura y donde un enemigo **E** puede interceptar el mensaje. En este caso existen varios problemas: (1) cómo hacer para que a pesar de que **E** intercepte el mensaje, éste no pueda saber su verdadero contenido, es decir, se pueda "esconder" el mensaje; (2) una vez que el usario **B** haya recibido el mensaje, cómo puede estar seguro de que se lo envió el usuario **A**; (3) al ser recibido el mensaje, cómo estar seguro de que no ha sido modificado. A estos problemas se les conoce como *privacidad, autenticidad e integridad* de la información respectivamente. Al conjunto de técnicas que sirven para resolver este tipo de problemas se le conoce como *Criptografía* ([5.13]).

En lo siguiente se dará una definición más formal de un sistema criptográfico o criptosistema.

Al conjunto finito $\mathcal{A}$, usado en algún lenguaje, lo llamaremos *alfabeto* y a sus elementos, letras o caracteres. Como ejemplos de alfabeto, tenemos al conjunto $\mathcal{A}=\{A, B, C, \ldots, Z, \_\}$.

El siguiente elemento a considerar es un conjunto G con estructura algebraica, que en general será un grupo o un anillo. El identificar a los elementos del alfabeto $\mathcal{A}$ con los elementos del conjunto G le llamaremos *encajamiento* de $\mathcal{A}$ en G, es decir, si existe una función $g : \mathcal{A} \to G$ inyectiva, y lo representamos por $\mathcal{A} \hookrightarrow G$.

Por motivos prácticos podemos suponer que un mensaje m, es una sucesión finita de elementos de $\mathcal{A}$, luego entonces, la podemos dividir en partes iguales de longitud k. Las partes del mensaje resultante se llamarán *mensajes elementales*. Un mensaje m, que utiliza el alfabeto $\mathcal{A}$ visto en G, se llamará *texto ordinario*. Donde no haya confusión, texto ordinario tendrá el mismo significado que mensaje, gracias a la función g.

Ejemplo: si m="ESTE ES EL PRIMER EJEMPLO", entonces podemos verlo como $m=(m_1, m_2, m_3, m_4, m_5)$, donde m_1 = "ESTE_", m_2 = "ES_EL",..., m_5 = "EMPLO". En este caso los mensajes elementales tienen longitud $k = 5$.

Como paso siguiente, para construir un criptosistema se considera una función f que transforma los textos ordinarios a "textos escondidos" y que llamaremos *función de encriptamiento*. Formalmente esta función tiene dominio y contradominio a G, biyectiva en su imagen, así existe su inversa f^{-1} que llamaremos *función de desencriptamiento*. A la imagen $f(m)$ de m, se le llama *texto encriptado*.

Por el momento un criptosistema lo tomaremos como el arreglo (G, F, F^{-1}) donde G es un grupo, F el conjunto de funciones de encriptamiento y F^{-1} el conjunto de funciones de desencriptamiento.

Como podemos observar, la seguridad de un criptosistema depende en gran medida de la función $f \in F$. Si se conoce f se puede encriptar, y si se

conoce $f^{-1} \in F^{-1}$ se puede desencriptar el mensaje.

Sin embargo, aunque se conozca la forma general de f, esto es, cualquier elemento de F para conocer explícitamente a una f_α, en particular falta por conocer otros parámetros: a estos parámetros les llamaremos *llaves de encriptamiento* que denotaremos como $L = \{l_\alpha\}$ y de forma similar los que son para conocer explícitamente a la función f_α^{-1} se llaman *llaves de desencriptamiento* que denotamos por $L^{-1} = \{l_\alpha^{-1}\}$. Por ejemplo si $F = \{f_{a,b}(x) = ax + b\}$, para $f_{2,3}(x) = 2x + 3$, la llave de encriptamiento es $(2, 3)$, y la de desencriptamiento $\left(\frac{1}{2}, -\frac{3}{2}\right)$.

DEFINICIÓN 2.1.1:

i) Si existe un algoritmo subexponencial que tenga como salida la función f^{-1}, y como entrada a f, se denominará criptosistema de *llave privada*, denotado por $F \approx F^{-1}$ o $L \approx L^{-1}$.

ii) Por otro lado, si todavía no se ha encontrado tal algoritmo, el que obtiene a f^{-1} a partir de f, lo denominaremos criptosistema de *llave pública* y se representará por $F \not\approx F^{-1}$ o $L \not\approx L^{-1}$.

Así la representación de un criptosistema queda como:

$$CpS = \{\mathcal{A} \hookrightarrow G, F = \{f_\alpha\}, F^{-1} = \{f_\alpha^{-1}\}\}$$
$$L = \{l_\alpha\}$$
$$L^{-1} = \{l_\alpha^{-1}\}$$

2.2 Criptosistemas de llave privada

Por definición, un criptosistema de llave privada mantiene a sus llaves de encriptamiento y desencriptamiento en secreto, ya que de ello depende el cómo desencriptar un mensaje. En la actualidad los criptosistemas de llave privada son muy usados principalmente por su fácil implementación y su rapidez de transmisión. Aunque aún existen problemas no resueltos, como la distribución de llaves, cosa que da, de algún modo, origen a los sistemas de llave pública.

Ahora describiremos brevemente algunos sistemas de llave privada y finalmente, detallamos un poco uno de ellos con el fin de identificar los elementos antes definidos.

El criptosistema de llave privada, quizá el más conocido en la actualidad es Data Encryption Standard, **DES** ([15.16]). **DES** fue desarrollado en el periodo 1973-1974 por la **IBM**; entre sus inventores se encuentran Horst Feistel, quien diseñó a "Lucifer", sistema que antecedió a **DES**; Alan Konheim, Bryamt Tuckerman, Edna Grossman y Don Coppersmith.

La estructura básica de **DES** es tomada de Lucifer, con el tamaño de las llaves de 56 bits. Recibe como entrada un texto ordinario de 64 bits, que transforma a un texto encriptado de la misma longitud. La entrada se divide en dos partes, cada una se somete a 16 aplicaciones entre permutaciones y transposiciones hasta obtener el texto encriptado. Como **DES** está basado en operaciones sobre bits, esto le permite una fácil implementación tanto en "software" como en "hardware". La seguridad de este sistema está garantizada por las 2^{56} llaves posibles, cosa que aún es imposible verificar cada una; sin embargo, hay quien afirma que con la tecnología en paralelo puede ser posible romper el sistema en poco tiempo; en tal caso es posible aplicarlo varias veces, digamos 3, para así obtener $(2^{56})^3$ posibles llaves.

Otro sistema de llave privada es el llamado International Data Encryption Algorithm **IDEA** ([15.23]), éste trata de cubrir la relativa pequeñes de las llaves en **DES**; inventado por Xuejia Lai y James Massey. **IDEA** es un sistema que encripta bloques de 64 bits con llaves de 128 bits. La idea general es ver al conjunto de bits con diferente estructura algebraica, con la operación lógica XOR, la suma módulo 2^{16} y la multiplicación módulo $2^{16}+1$; estas operaciones son aplicadas a bloques de 16 bits.

Algunas implementaciones de **IDEA** llegan a ser hasta 2 veces más rápidas que **DES**. La seguridad de **IDEA** es sobre entendida por el tamaño de sus llaves, además de ser dotado con algoritmos inmunes a los ataques conocidos, incluso el criptoanálisis lineal y diferencial que son de gran popularidad en **DES**.

En la misma dirección que **DES** e **IDEA** está el sistema **GOST** ([15.24]), el cual fue desarrollado por la parte soviética y conserva la misma estructura básica. Algunas de las diferencias con **DES** es que **GOST** tiene formas más simples de generar llaves, y éstas tienen una longitud de 256 bits; además

de incluir a una S-caja (una permutación usada en **DES**) como información secreta, por lo tanto **GOST** cuenta con 610 bits de este tipo de información. Ambos sistemas usan 8 S-cajas, excepto que una S-caja del soviético es 25% la medida de una S-caja de **DES**, éste efectúa 16 aplicaciones en el encriptamiento, a lo que **GOST** hace 32.

Sobre la seguridad de **GOST**, podemos mencionar que en principio es superior a la de **DES**, viendo el tamaño de las llaves, así como la confidencialidad de una de las S-cajas. Como los ataques conocidos dependen del número de aplicaciones que se realizan en el encriptamiento, entonces aumenta la seguridad del sistema.

Como último ejemplo de sistemas de llave privada, tenemos al reciente **RC-5** ([15.22]), creado por R. Rivest del **MIT**. Este sistema está caracterizado por la flexibilidad que representan sus parámetros. El sistema es designado por **RC5**-$w/r/b$; donde w es el tamaño de una palabra; el valor estándar es de 32 bits, sin embargo, también se permiten valores de 16 y 64 bits; el número r es la cantidad de aplicaciones que recibe un bloque para ser encriptado, los valores permitidos están entre 0 y 255; b, es el tamaño de la llave secreta en bytes, sus valores permitidos están entre 0 y 277. Por ejemplo **RC5**-*32/16/7* es un algoritmo con los mismos parámetros que **DES**; el algoritmo usa 3 tipos de operaciones: la suma módulo 2^w, la operación lógica OR y la rotación de palabras por la izquierda. Debido a la variabilidad de sus parámetros, el sistema permite optimizar tanto su velocidad como su seguridad.

En seguida veamos el ejemplo de un sistema sencillo de llave privada que nos ayudará a identificar las definiciones anteriormente descritas.

En este y en sucesivos ejemplos consideraremos a el alfabeto $\mathcal{A}=\{A, B, ..., Z, \_\}$, como $|\mathcal{A}| = 27$; para mensajes elementales de tamaño uno se tomará al grupo G como el de los enteros módulo 27, $\mathbf{Z}_{27}$, con el encajamiento siguiente:

$$\begin{array}{ccccccc} A & B & C & \ldots & Z & \_ \\ \updownarrow & \updownarrow & \updownarrow & & \updownarrow & \updownarrow \\ 0 & 1 & 2 & \ldots & 25 & 26 \end{array}$$

representado como $\mathcal{A}^1 \hookrightarrow \mathbb{Z}_{27}$ (el superíndice en $\mathcal{A}$ denota el tamaño de los mensajes elementales).

Para el primer ejemplo de una función de encriptamiento sea $a_0 = 5 \in \mathbb{Z}_{27}$ fijo y f definida como:

$$\begin{aligned} f: \ & \mathbb{Z}_{27} \to \mathbb{Z}_{27} \\ & m \ \mapsto m + 5 \ (mod \ 27) \end{aligned}$$

Si el mensaje ordinario es m="SEGUNDO EJEMPLO", entonces:

$M =$	S	E	G	U	N	D	O	$\_$	E	J	E	M	P	L	O
	$\updownarrow$	$\updownarrow$	$\cdots$											$\cdots$	$\updownarrow$
$m =$	18	4	6	20	13	3	14	26	4	9	4	12	15	11	14
	$\updownarrow$	$\updownarrow$	$\cdots$											$\cdots$	$\updownarrow$
$f(m) =$	23	9	11	25	18	8	19	4	9	14	9	17	20	16	19
	$\updownarrow$	$\updownarrow$	$\cdots$											$\cdots$	$\updownarrow$
$c =$	X	J	L	Z	S	I	T	E	J	O	J	R	U	Q	T

Así el mensaje encriptado es c="XJLZSITEJOJRUQT". En este caso la llave de encriptamiento es $L = (5, 27)$ y la de desencriptamiento $L^{-1} = (-5, 27)$. El sistema es de llave privada $L \approx L^{-1}$, ya que $-a_0$ se puede obtener fácilmente a partir de a_0.

Como podemos abservar el criptosistema anterior se puede representar como:

$$\begin{gathered} CpS = \{\mathcal{A}^1 \hookrightarrow \mathbb{Z}_{27}, \{m + 5\,(mod\,27)\}, \{c - 5\,(mod\ 27)\}\} \\ L = (5, 27) \\ L^{-1} = (-5, 27) \\ L \approx L^{-1} \end{gathered}$$

En un caso más general al anterior, tenemos a $f : \mathbb{Z}_n \to \mathbb{Z}_n$, $f(m) = a_1 m + a_0 \ (mod\ n)$, donde $a_0, a_1 \in \mathbb{Z}_n$ son fijos. La función de desencriptamiento se obtiene despejando a m, esto es, $f^{-1}(c) = a_1^{-1}c - a_1^{-1}a_0 \ (mod\ n)$, donde ahora es necesario que $a_1 \in \mathbb{Z}_n^*$, es decir, $mcd(a_1, n) = 1$.

Obsérvese que en este ejemplo $f(m)$ es un polinomio de primer grado en m. En general se pueden considerar polinomios $p(n)$ sobre $\mathbf{Z}_n$ que sean permutaciones. De forma natural tales polinomios se pueden usar como funciones de encriptamiento.

Para una información general respecto a los polinomios permutación se puede consultar [2.1], [2.30], [2.31] y [2.32].

Una generalización del ejemplo anterior es el siguiente; consideremos matrices con entradas en $\mathbf{Z}_n$ y mensajes unidad de tamaño 2 encajados en $(\mathbf{Z}_n)^2$. Por lo tanto, el texto ordinario tiene la forma $m = \begin{pmatrix} x \\ y \end{pmatrix}$, donde $x, y \in \mathbf{Z}_n$, el cual podemos resumir en:

$$CpS = \left\{\mathcal{A}^2 \hookrightarrow \mathbb{Z}_n^2, \{A_1 m + A_0 \,(mod\ n)\}, \left\{A_1^{-1} c - A_1^{-1} A_0 \,(mod\ n)\right\}\right\}$$
$$L = (A_1, A_0, n)$$
$$L^{-1} = \left(A_1^{-1}, -A_1^{-1} A_0, n\right)$$
$$L \approx L^{-1}$$

2.3 Problema del logaritmo discreto

Esta sección está dedicada a entender un problema muy importante y estudiado en criptografía, el Problema del Logaritmo Discreto (PLD). De la dificultad de solucionar este problema depende la seguridad de varios criptosistemas; por lo que es conveniente al menos entenderlo y repasar algunos métodos propuestos para su solución.

Sea G un grupo finito. El problema del logaritmo discreto para G, es el siguiente: si $\langle\alpha\rangle$ es el subgrupo cíclico generado por $\alpha \in G$, y $y \in \langle\alpha\rangle$, entonces el logaritmo discreto para y, es el entero x, tal que

$$\alpha^x = y.$$

Si existe el entero x se denota por $\log_\alpha y = x$.

De particular importancia es el caso cuando G es el grupo multiplicativo de un campo finito $\mathbf{F}_q$ con $q = p^n$ elementos.

Desde que se planteó este problema, ha sido objeto de intensa investigación, por ejemplo, en 1978 M. Hellman y S. Pohlig ([3.15]) proporcionan un algoritmo para la solución del PLD en $\mathbf{Z}_p$, para aquellos primos p que en la factorización de $\left|\mathbf{Z}_p^*\right|$ tienen números primos "pequeños". Posteriormente en 1979 L. Adleman ([3.13]) generaliza el método a campos finitos $\mathbf{F}_q$, en donde la solución al problema depende de encontrar polinomios en cuya factorización haya polinomios de grado "pequeño". Como caso particular, en 1984 D. Coppersmith ([3.13]) publicó el algoritmo de Adleman aplicado al PLD sobre campos de la forma F_{2^n}. Novedosos resultados han sido obtenidos al introducir la criba cuadrática, usada en el problema de factorizar números enteros, así como también la criba de campos numéricos ([3.3]). Recientemente L. Adleman ([3.2]) generaliza los métodos anteriores, proponiendo una criba en el campo de funciones.

Antes de mencionar los métodos que resuelven el PLD, revisemos una importante definición de la teoría de complejidad.

Un algoritmo subexponencial ([3.6]), es aquel que crece a tiempo $L[x, c, \alpha]$, donde

$$L[x, c, \alpha] = O\left(\exp\left((c + o(1))(\ln x)^{\alpha}(\ln \ln x)^{1-\alpha}\right)\right)$$

aquí c es constante, $0 < \alpha < 1$ y x es el "tamaño" del espacio donde se efectúa el algoritmo. Por ejemplo si se trabaja en $\mathbf{F}_{2^n}$, $x = 2^n$.

Esta función nos permite conocer qué tan rápido se efectúa un algoritmo, en este caso para resolver el PLD. Si $\alpha \to 0$, entonces $L[x, c, \alpha]$ se transforma en un polinomio, por otro lado, si $\alpha \to 1$ la función es una exponencial. Es decir, nos interesará encontrar algoritmos donde α esté cerca de 0, x sea grande y c una constante cerca de 1.

Cuando se entienda en qué espacio se está trabajando, la notación $L[x, c, \alpha]$ se podrá reducir en $L[c, \alpha]$. En la mayor parte de este trabajo $x = 2^n$.

A continuación se describe la solución al PLD en algunos casos interesantes.

1) El problema del logaritmo discreto para $G = \mathbf{F}_p^*$ con p primo y $p = 2^n + 1$, fue resuelto en 1976 por S. Pohlig y M. Hellman ([3.15]) de la siguiente manera: dado α y $y \in \mathbf{F}_p^*$ determinar un entero x tal que $y = \alpha^x \ mod\ p$, donde podemos suponer que $0 \leq x \leq p-2$, ya que $\left|\mathbf{Z}_p^*\right| = p-1$ y $\alpha^{p-1} = 1$.

Para encontrar tal entero x, primeramente lo escribimos en su expansión binaria: $x = \sum_{i=0}^{n-1} b_i 2^i$, ya que $x < p-1 = 2^n$ y donde se elige a α como un elemento primitivo de $\mathbf{Z}_p$. Para encontrar a $\{b_0, b_1, ..., b_{n-1}\}$ se procede de la siguiente forma:

i) Como $y = \alpha^x$ y conocemos a α, elevamos a y a la potencia $\frac{p-1}{2} = 2^{n-1}$, como α es primitivo, $\alpha^{\frac{p-1}{2}} \equiv \pm 1 \ mod\ p$ y además $\frac{p-1}{2} < p-1$, entonces $\alpha^{\frac{p-1}{2}} \equiv -1 \ mod\ p$, y así

$$y^{\frac{p-1}{2}} = (\alpha^x)^{\frac{p-1}{2}} \equiv (-1)^x \ mod\ p$$

por lo tanto

$$y^{\frac{p-1}{2}} \equiv \begin{cases} 1 \ mod\ p & \Leftrightarrow b_0 = 0 \\ -1 \ mod\ p & \Leftrightarrow b_0 = 1 \end{cases}$$

de esta manera hemos determinado el primer "bit" b_0 de x.

ii) Los restantes "bits" de x se determinan en forma inductiva, esto es, si estamos en el $i-$ésimo paso tenemos: $m = \frac{p-1}{2^{i+1}}$ y $z = \alpha^{x_i}$, con $x_i = \sum_{j=i}^{n-1} b_j 2^j$, así elevando a z a la potencia m :

$$z^m = \alpha^{x_i m} = \alpha^{\left(b_i 2^i + b_{i+1} 2^{i+1} + \cdots + b_{n-1} 2^{n-1}\right)\frac{p-1}{2^{i+1}}}$$

en este caso $\frac{p-1}{2^{i+1}} = 2^{n-i-1}$, por lo tanto

$$\begin{aligned} z^m &= \alpha^{b_i 2^{n-1} + b_{i+1} 2^n + b_{i+2} 2^{n+1} + \cdots + b_{n-1} 2^{2n-i-1}} \\ &= \alpha^{b_i 2^{n-1}} = \left(\alpha^{\frac{p-1}{2}}\right)^{b_i} \qquad \equiv \pm 1 \ mod\ p \end{aligned}$$

y de forma análoga

$$z^m \equiv \begin{cases} 1 \mod p & \Leftrightarrow b_i = 0 \\ -1 \mod p & \Leftrightarrow b_i = 1 \end{cases}$$

teniendo así al $i-$ésimo "bit" de x.

Ejemplo:

Tomemos al campo $\mathbf{Z}_{17}$, esto es cuando $p = 2^4+1 = 17$. $\mathbf{Z}_{17}^* = \{1, 2, 3, ..., 16\}$. Sea $\alpha = 3$ y $y = 12$. Procedamos a encontrar un x tal que $3^x = 12$. En este caso x tiene la forma $x = b_0 + b_1 2 + b_2 2^2 + b_3 2^3$.

Para encontrar a b_0, tenemos que $\frac{p-1}{2} = 8$, luego

$$y^{\frac{p-1}{2}} = 12^8 \equiv -1 \mod 17$$

por lo tanto $b_0 = 1$.

Para encontar a b_1, tenemos que $m = \frac{17-1}{4} = 4$, entonces

$$\begin{aligned} z^m = (\alpha^{x_1})^m = (y\alpha^{-b_0})^m &= (12 \cdot 3^{-1})^4 \\ &\equiv 1 \mod 17, \quad \Rightarrow b_1 = 0 \end{aligned}$$

Para b_2 tenemos que $m = \frac{17-1}{8} = 2$, entonces

$$\begin{aligned} z^m = (\alpha^{x_2})^m = (y\alpha^{-b_0-b_1 2})^m &= (12 \cdot 3^{-1})^2 \\ &\equiv -1 \mod 17 \quad \Rightarrow b_2 = 1. \end{aligned}$$

Finalmente para encontrar a b_3, tenemos que $m = \frac{17-1}{2^4} = 1$, entonces

$$\begin{aligned} z^m = (\alpha^{x_3})^m = (y\alpha^{-b_0-b_1 2-b_2 2^2})^m &= (12 \cdot 3^{-1-0-4})^1 \\ &\equiv -1 \mod 17 \qquad \Rightarrow b_3 = 1. \end{aligned}$$

Por lo tanto $x = 1 + 0 \cdot 2 + 1 \cdot 2^2 + 1 \cdot 2^3 = 13$, esto es

$$\alpha^x = 3^{13} = 1594323 \equiv 12 \mod 17.$$

2) Ahora veamos la solución del logaritmo discreto en el campo finito $\mathbf{F}_q$ donde los factores primos de $q-1$ son "pequeños" ([5.1]).

Para resolver el problema del logatirmo discreto de un elemento y, tal que $y = \alpha^x$, donde $\alpha \in \mathbb{F}_q^*$, se procede de la siguiente manera:

i) Como $q-1 = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$, para cada p_k calculemos las p_k–ésimas raíces de la unidad $r_{p_k,j} = \alpha^{j(q-1)/p_k}$, $j = 0, 1, \ldots, p-1$, $k = 1, \ldots, n$ usando el método de cuadrados repetidos ([5.1]); por lo que obtenemos

$$\begin{array}{ccccc} r_{p_1,0} & r_{p_1,1} & r_{p_1,2} & \cdots & r_{p_1,p_1-1} \\ r_{p_2,0} & r_{p_2,1} & r_{p_2,2} & \cdots & r_{p_2,p_2-1} \\ \vdots & \vdots & \vdots & & \vdots \\ r_{p_n,0} & r_{p_n,1} & r_{p_n,2} & \cdots & r_{p_n,p_n-1} \end{array}$$

que la denotaremos como $\{r_{p_k j}\}$.

ii) Lo que queremos encontrar es un $x, 0 \leq x < q-1$, tal que $\alpha^x = y$. Como $q-1 = \prod_{k=1}^{n} p_k^{a_k}$, es suficiente encontrar $x_k \ mod\ p_k^{a_k}$ para cada k, así x está únicamente determinado por el teorema Chino del Residuo. Por lo tanto, fijemos un p_k que llamaremos p, para encontrar un x_k, que llamaremos x, tal que $\alpha^x = y \ mod\ p^a$.

iii) Para obtener a x, sea $x \equiv x_0 + x_1 p + \cdots + x_{a-1} p^{a-1} mod\ p^a$ con $0 \leq x_i < p$. Para determinar x_0, calculemos a $y^{(q-1)/p}$ que es una raíz p–ésima de la unidad, ya que $y^{q-1} = 1$, como $y = \alpha^x$ entonces

$$y^{(q-1)/p} = \alpha^{x(q-1)/p} = \alpha^{x_0(q-1)/p} = r_{p,x_0}$$

por lo tanto, hay que comparar $y^{(q-1)/p}$ con algún $\{r_{p,j}\}_{0 \leq j < p}$, y así $x_0 = j$, tal que $y^{(q-1)/p} = r_{p,j}$.

iv) Para calcular los restantes x_i procedemos inductivamente. En el paso i–ésimo tenemos que $y_i = \frac{y}{\alpha^{x_0 + x_1 p + \cdots + x_{i-1} p^{i-1}}}$ cuyo logaritmo módulo p^a es $x_i p^i + \cdots x_{a-1} p^{a-1}$, además $y_i^{(q-1)/p^i} = 1$, por lo tanto

$$\begin{aligned} y_i^{(q-1)/p^{i+1}} &= \alpha^{\left(x_i + x_{i+1} p + \cdots + x_{a-1} p^{a-1-i}\right)(q-1)/p} \\ &= \alpha^{x_i (q-1)/p} \qquad\qquad = r_{p,x_i} \end{aligned}$$

comparando nuevamente a $y_i^{(q-1)/p^{i+1}}$ con $\{r_{p,j}\}_{0 \leq j < p}$, tomamos a $x_i = j$, tal que $y_i^{(q-1)/p^{i+1}} = r_{p,j}$.

v) Por último, se efectúan los pasos anteriores para cada p divisor de $q-1$ y usando el Teorema Chino del Residuo obtenemos el valor de x.

3) En 1979, L. Adleman ([3.11], [3.13]) dio un algoritmo (método del índice), tratando de resolver el problema de logaritmo discreto en un campo finito arbitrario $\mathbf{F}_q$, en particular podemos suponer que tenemos el campo $\mathbf{F}_{2^n}$; este algoritmo se basa en la siguiente definición: se dice que un polinomio $A(x)$ es suave respecto a un entero b, si $A(x)$ es producto de polinomios irreducibles de grado a lo más b.

El procedimiento de Adleman es el siguiente:

i) Seleccionamos la cota b y a c una constante pequeña, digamos $c = 1$, seleccionemos aleatoriamente un entero m, tal que $0 \leq m \leq 2^n - 2$, entonces definamos al polinomio $A(x) = x^n mod\ p(x)$, donde $p(x) \in \mathbf{F}_{2^n}$ es un polinomio primitivo, así $A(x)$ es un polinomio aleatorio de grado a lo más $n-1$. El primer paso es probar la suavidad de $A(x)$, esto es, que al factorizar a $A(x)$ sea producto de polinomios irreducibles $q_j(x) \in \mathbf{F}_{2^n}[x]$ de grado a lo más b, o sea que $A(x) = x^m = \prod_j q_j(x)^{e_j}\ mod\ p(x)$. Si éste es el caso entonces tenemos la siguiente relación logarítmica base x : $m = \sum_j e_j \log_x q_j(x)$, en el anillo $\mathbf{Z}_{2^n-1}$, en caso contrario se elige otro m.

ii) Al realizar lo anterior, tantas veces como sea necesario hasta tener al menos más ecuaciones que polinomios irreducibles, se tendrá un sistema de ecuaciones de la forma:

$$m_i = \sum_j e_{ij} \log_x q_{ij}(x)$$

que al resolverlos se tendrán los logaritmos de todos los polinomios irreducibles $q_j(x)$ de grado a lo más b.

iii) Si se tiene un elemento arbitrario $B(x) \in \mathbf{F}_q[x]$, para calcular su logaritmo primero se toma un entero m' aleatoriamente y calculamos a $A(x) \equiv B(x)\, x^{m'} mod\ p(x)$, intentando tantos m' como sea necesario hasta que $A(x)$ sea suave, esto es, $B(x)\, x^{m'} \equiv \prod_j q_j(x)^{e_j}\ mod\ p(x)$, con $e_j \leq b$ entonces de ii) ya conocemos los logaritmos de estos $q_j(x)$, por lo tanto

$$\log_x B(x) + m' \equiv \sum_j e_j \log_x q_j(x) \mod p(x).$$

Obsérvese que el método anterior se realiza en tres etapas independientes (en lo que se refiere a su programación en computadoras). La primera es generar las ecuaciones logarítmicas para polinomios suaves, esta etapa es la que consume la mayor cantidad de tiempo. La segunda es el resolver los sistemas de ecuaciones, que en general, ya existen métodos para su solución ([3.20], [3.21], [3.22]). La última es calcular los logaritmos pedidos, ésta es quizá la que consuma la menor cantidad de tiempo de las tres, dependiendo del algoritmo usado.

Este metódo (del indíce) corre a un tiempo acotado por $L[c, 1/2]$.

Ejemplo ([3.13]): en el caso del campo $\mathbf{F}_{2^{127}}$, si seleccionamos a $b = 23$, tendremos a 766 150 polinomios irreducibles de grado a lo más 23, además requerimos para cada polinomio un promedio de 7692 intentos para verificar la suavidad y de alrededor 5 549 000 000 pruebas de suavidad. Si cada una de estas pruebas se realiza en 250 microsegundos, entonces requerimos de alrededor 400 horas, para tener los logaritmos de polinomios de grado menor a 23.

En 1983 Blake, Fuji-Hara, R. Mullin y S. Vanstone ([3.13]) mejoran el algoritmo anterior, observando que éste depende principalmente de la probabilidad de que un polinomio sea suave, sin embargo, Adleman utiliza polinomios de grado a lo más n, lo que se propone ahora es disminuir el grado de los polinomios, a los cuales hay que probar su suavidad usando el algoritmo extendido de Euclides para construir polinomios $C(x), D(x)$ de grado a lo más $\frac{n}{2}$, tales que $A(x) D(x) \equiv C(x) \mod p(x)$ de donde tenemos las ecuaciones

$$m + \sum_j e_j \log_x q_j(x) \equiv \sum_k f_k \log_x q_k(x) \mod p(x)$$

que son usadas de la misma forma como en el método de Adleman. Por ejemplo ([3.13]) para $\mathbf{F}_{2^{127}}$, con $b = 27$ existen 16510 polinomios irreducibles de grado a lo más 27, de donde si se eligen los polinomios $D(x), C(x)$ de grado a lo más 63, y primos relativos entre sí, se tendrán que hacer alrededor

de 120 000 000 pruebas de suavidad, lo que lleva un tiempo estimado de 9 horas.

4) En Noviembre de 1983 Don Coppersmith ([3.13]) publicó el método simplificado y mejorado para el caso de un campo de característica 2, corre a un tiempo $L[c, 1/3]$, donde $c = 1.5874...$ La ventaja se toma al considerar la linealidad de la función exponencial a un número potencia de 2.

5) En 1992, en su tesis doctoral R. Lovorn ([3.6]) determinó un algoritmo subexponencial para el PLD en $\mathbf{F}_{p^n}$ con p primo y $n = 2$ ó $\log p < n^{0.98}$, que corre a un tiempo de $L[c, 1/2]$ donde $c = \sqrt{2} + o(1)$.

6) En 1993 L. Adleman y J. Demarrais ([3.5]) dieron un algoritmo subexponencial para campos $\mathbf{F}_{p^n}$, que corre a un tiempo acotado por $L[c, 1/2]$.

7) Existe una gran relación entre el PLD y el problema de factorización de números enteros ([3.4], [3.9]), y paralelamente se han usado las mismas técnicas para resolver ambos problemas. Recientemente D. Gordon ([3.3]) ha usado la criba de campos numéricos para resolver el PLD, a un tiempo $L[c, 1/2]$, donde $c = 2.0800$.

8) En 1995 L. Adleman ([3.2]) generalizó el método anterior a la criba de campo de funciones, a un tiempo $L[c, 1/3]$. Además de plantear los siguientes problemas abiertos hasta esta fecha:

a) ¿Son los problemas de factorización y PLD equivalentes sobre campos finitos en general?

b) ¿Se podrá encontrar un algoritmo $L[x, c, 1/3]$, para el PLD en todos los campos finitos?

c) ¿Es posible dar una optimización de la criba de campo de funciones para el caso particular de $\mathbf{F}_{2^n}$, que corra por lo menos al mismo tiempo que el algoritmo de Coppersmith?

2.4 Criptosistemas de llave pública

Recordemos que un criptosistema de llave pública se puede resumir en el siguiente esquema:

$$CpS = \{\mathcal{A} \hookrightarrow G, \{f_\alpha\}, \{f_\alpha^{-1}\}\}$$
$$L = (l_\alpha)$$
$$L^{-1} = (l_\alpha^{-1})$$
$$L \not\approx L^{-1}$$

donde la principal característica es que la llave privada no puede ser obtenida eficientemente a partir de la llave pública.

En esta sección se muestran dos de estos criptosistemas, donde la función de encriptamiento f es fácil de calcular, una vez que la llave de encriptamiento l se conoce, pero es muy difícil calcular la función inversa f^{-1} (no existe aún un algoritmo eficiente). Desde un punto de vista computacional, la función f no es invertible (sin la información adicional de la llave l^{-1} de desencriptamiento), tales funciones son llamadas de "un-sentido". La definición de un criptosistema de llave pública y función de "un-sentido" no es rigurosa desde el punto de vista matemático, ya que depende de los avances tecnológicos en computadoras y el descubrimiento de nuevos algoritmos.

El nombre de "llave pública" se debe a que la información necesaria para enviar un mensaje (la llave de encriptamiento l) es información pública.

Alguien que desea enviar un mensaje, sólo tiene que buscar la llave de encriptamiento en un archivo público y usar el algoritmo general de encriptamiento con los parámetros correspondientes del destinatario quien es el único que tiene la llave necesaria para desencriptar y poder leer el mensaje.

En los últimos años es frecuente que se tenga una gran cantidad de usuarios, por lo que para los sistemas de llave privada es un problema la distribución de las llaves; los sistemas de llave pública lo soluciona en buena medida.

La llave pública proporciona también una solución al problema de autenticidad de la siguiente forma: la firma de una persona es una señal escrita difícil de duplicar y así permite al receptor del mensaje saber si realmente es de la persona que escribió ahí su nombre. En una comunicación electrónica, donde no es fácil tener firmas físicas, se tiene que usar otro método. En criptografía de llave pública hay una manera fácil de identificación, de tal forma que no se pueda suplantar a otra persona. Por ejemplo, si **A** y **B** son dos usuarios del sistema con f_A, f_B las correspondientes funciones de encriptamiento y M es la firma de **A**, entonces **A** enviará la firma a **B** como $f_B f_A^{-1}(M)$. **B** puede desencriptar todo el mensaje aplicando f_B^{-1}, exepto a

$f_A^{-1}(M)$ que solamente puede ser desencriptado con la llave pública de **A**, es decir, se identifica a **A**.

En los años 70, W. Diffie y M. Hellman ([5.14]) introducen la primera función de un "solo sentido" como la función potencia en $\mathbb{F}_p$. Este sistema funciona de la siguiente manera:

i) Cada usuario U_i genera un número aleatorio x_i independientemente de $\mathbb{F}_p^*$. Se guarda en secreto a x_i y se calcula $y_i = \alpha^{x_i} mod\ p$, el cual se hace público con el nombre del usuario y otros datos, donde α es un elemento primitivo de $\mathbb{F}_p^*$ fijo. Por ejemplo:

Usuario	*Datos*	*Clave del Usuario*
U_1	ABC	y_1
U_2	CDE	y_2
$\vdots$	$\vdots$	$\vdots$
U_k	FGH	y_k

ii) Cuando los usuarios U_i y U_j quieran comunicarse confidencialmente usan la llave $K_{ij} = \alpha^{x_i x_j} mod\ p$. Cada uno puede calcular esta llave elevando la correspondiente clave y a la potencia secreta

$$\begin{aligned} K_{ij} &= y_j^{x_i} mod\ p \\ &= \alpha^{x_j x_i} mod\ p \end{aligned}$$

Para que algún intruso pueda saber la llave tendrá que calcular

$$K_{ij} = y_i^{(\log y_j)} mod\ p$$

es decir, si conocemos los logaritmos módulo p, entonces es fácil romper el sistema.

Cabe mencionar que aún no se ha probado que el sistema sea seguro si los logaritmos son difíciles de calcular.

2.5 Criptosistema de ElGamal

En 1984 Taher ElGamal ([15.9]) propuso un criptosistema que basa su seguridad en la "imposibilidad" de resolver el problema del logaritmo discreto en campos finitos. En próximos capítulos este criptosistema será usado junto con el grupo de puntos racionales de una curva elíptica sobre campos finitos. Por lo tanto, es necesario detallar más a fondo cómo funciona, además de dar ejemplos prácticos que permitan entender su funcionamiento.

El sistema de ElGamal se describe de la siguiente manera:

Primero fijemos un campo finito de la forma F_{2^n}, considerablemante grande, esto significa para casos prácticos, $n > 500$ y un elemento $\alpha \in \mathsf{F}_q^*$, $q = 2^n$, preferentemente primitivo. Supongamos que ya hemos encajado al alfabeto en el campo finito, entonces:

i) Cada usuario $\mathbf{U}_j$ elige aleatoriamente un entero x_j, tal que $0 < x_j < q-1$, el cual queda en secreto. La llave pública será el elemento α^{x_j}, esto es, la clave con la cual puede recibir información de cualquier usuario.

ii) Para enviar el mensaje $m = (m_1, m_2, ..., m_l)$ al usuario $\mathbf{A}$, por cada m_i se envía el par de elementos $\left(\alpha^k, m_i \alpha^{x_A k}\right)$, donde k es un entero que se elige aleatoriamente, y donde el segundo término se puede calcular, ya que α^{x_A} es público.

iii) Ahora el usuario $\mathbf{A}$ puede leer el mensaje m_i, elevando el primer elemento de la pareja a la potencia x_A, que $\mathbf{A}$ guarda en secreto, entonces recobra a m_i, dividiendo la segunda pareja por $\alpha^{k x_A}$, o elevando a α^k a la potencia $(q-1-x_A)$ y multiplicándolo por la segunda pareja, es decir, $\left(\alpha^k\right)^{(q-1-x_A)} m_i \alpha^{x_A k} = m_i$.

El criptosistema de ElGamal tiene el siguiente esquema

$$CpS = \left\{\mathcal{A} \hookrightarrow \mathsf{F}_q, \left\{c = \left(\alpha^k, m_i \cdot \alpha^{x_j k}\right)\right\}, \left\{c_1^{(q-1-x_j)} c_2\right\}\right\}$$
$$L = (k, \alpha^{x_j})$$
$$L^{-1} = (x_j)$$
$$L \not\approx L^{-1}$$

Ejemplos:

1) En este ejemplo tomemos un campo pequeño para observar claramente los pasos a seguir.

Sea $\mathsf{F}_q = \mathbb{Z}_{29}$, entonces $\mathbf{Z}_{29}^* = \{1, 2, 3, ..., 28\}$, $\alpha = 2$, además considerese el siguiente encajamiento:

$$\begin{array}{cccccccccc} A & B & C & D & \cdots & Y & Z & \_ & . \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & & \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ 1 & 2 & 3 & 4 & \cdots & 25 & 26 & 27 & 28 \end{array}$$

y el siguiente archivo de usuarios

Campo $\mathbf{Z}_{29}$	*Llave privada*	*Llave pública*
U_1	$x_1 = 7$	$12 \ mod\ 29$
U_2	$x_2 = 17$	$21 \ mod\ 29$
U_3	$x_3 = 10$	$9 \ mod\ 29$

Se desea enviar el mensaje m = "ADIOS", al usuario $\mathbf{U}_1$, en este caso se tiene $m = (1, 4, 9, 15, 19) = (m_1, m_2, m_3, m_4, m_5)$ y así el mensaje encriptado tiene la forma de cinco parejas, en este ejemplo tomemos $k = 5$, y así obtenemos

$$\begin{aligned} (2^5, 1 \cdot 12^5) &\equiv (3, 12) \\ (2^5, 4 \cdot 12^5) &\equiv (3, 19) \\ (2^5, 9 \cdot 12^5) &\equiv (3, 21) \\ (2^5, 15 \cdot 12^5) &\equiv (3, 6) \\ (2^5, 19 \cdot 15^5) &\equiv (3, 25) \end{aligned}$$

las cuales se transmiten al usuario $\mathbf{U}_1$.

Cuando el mensaje llega a su destino, éste se desencripta de la siguiente manera:

$$(c_1, c_2) \sim \ c_1^{(q-1-x_A)} \cdot c_2 \ \equiv m_i$$

$$\begin{aligned} (3, 12) &\sim \ 3^{(29-1-7)} \cdot 12 \ \equiv 17 \cdot 12 \ \equiv 204 \ \equiv 1 \\ (3, 19) &\sim \ 3^{(29-1-7)} \cdot 19 \ \equiv 17 \cdot 19 \ \equiv 323 \ \equiv 4 \\ (3, 21) &\sim \ 3^{(29-1-7)} \cdot 21 \ \equiv 17 \cdot 21 \ \equiv 357 \ \equiv 9 \\ (3, 6) &\sim \ 3^{(29-1-7)} \cdot 6 \ \equiv 17 \cdot 6 \ \equiv 102 \ \equiv 15 \\ (3, 25) &\sim \ 3^{(29-1-7)} \cdot 25 \ \equiv 17 \cdot 25 \ \equiv 425 \ \equiv 19 \end{aligned}$$

Donde $\sim$ indica el proceso de desencriptamiento, recuperando el mensaje original.

2) En este caso veamos cómo se utiliza este criptosistema en el campo finito $\mathbf{F}_{2^5}$ con 32 elementos, el cual no es de la forma $\mathbf{Z}_p$. De acuerdo con el capítulo anterior $\mathbf{F}_{2^5} \cong \mathbf{F}_2[x]/(f)$, donde $f(x) = x^5 + x^2 + 1 \in \mathbf{Z}_2[x]$ es irreducible y primitivo. Como f es primitivo cualquiera de sus raíces genera cíclicamente al grupo $\mathbf{F}_{2^5}^*$; vemos a continuación una lista, sin incluir al 0, 1, usando la relación $\alpha^5 = \alpha^2 + 1$.

α^1	$= \alpha$	α^{11}	$= \alpha^2 + \alpha + 1$	α^{21}	$= \alpha^4 + \alpha^3$
α^2	$= \alpha^2$	α^{12}	$= \alpha^3 + \alpha^2 + \alpha$	α^{22}	$= \alpha^4 + \alpha^2 + 1$
α^3	$= \alpha^3$	α^{13}	$= \alpha^4 + \alpha^3 + \alpha^2$	α^{23}	$= \alpha^3 + \alpha^2 + \alpha + 1$
α^4	$= \alpha^4$	α^{14}	$= \alpha^4 + \alpha^3 + \alpha^2 + 1$	α^{24}	$= \alpha^4 + \alpha^3 + \alpha^2 + \alpha$
α^5	$= \alpha^2 + 1$	α^{15}	$= \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$	α^{25}	$= \alpha^4 + \alpha^3 + 1$
α^6	$= \alpha^3 + \alpha$	α^{16}	$= \alpha^4 + \alpha^3 + \alpha + 1$	α^{26}	$= \alpha^4 + \alpha^2 + \alpha + 1$
α^7	$= \alpha^4 + \alpha^2$	α^{17}	$= \alpha^4 + \alpha + 1$	α^{27}	$= \alpha^3 + \alpha + 1$
α^8	$= \alpha^3 + \alpha^2 + 1$	α^{18}	$= \alpha + 1$	α^{28}	$= \alpha^4 + \alpha^2 + \alpha$
α^9	$= \alpha^4 + \alpha^3 + \alpha$	α^{19}	$= \alpha^2 + \alpha$	α^{29}	$= \alpha^3 + 1$
α^{10}	$= \alpha^4 + 1$	α^{20}	$= \alpha^3 + \alpha^2$	α^{30}	$= \alpha^4 + \alpha$

En seguida damos un encajamiento del alfabeto en este campo:

A	B	C	$\cdots$	X	Y	Z	$\_$	.	1	2	3
$\updownarrow$	$\updownarrow$	$\updownarrow$	$\cdots$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$
0	1	2	$\cdots$	23	24	25	26	27	28	29	30
$\updownarrow$	$\updownarrow$	$\updownarrow$	$\cdots$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$
α^0	α^1	α^2	$\cdots$	α^{23}	α^{24}	α^{25}	α^{26}	α^{27}	α^{28}	α^{29}	α^{30}

Supóngase además que tenemos el siguiente directorio de usuarios

Usuario	*llave privada* x_j	*llave pública*
U_1	$x_1 = 2$	α^2
U_2	$x_2 = 10$	$\alpha^4 + 1$
U_3	$x_3 = 13$	$\alpha^4 + \alpha^3 + \alpha^2$

El mensaje a encriptar es el siguiente $m = (m_1, ..., m_{12})$ = "IR EN 3 DIAS", por lo que tenemos el siguiente encajamiento

$$\begin{array}{llll} m_1 \hookrightarrow & \alpha^8 & = \alpha^3+\alpha^2+1 & m_7 \hookrightarrow \quad \alpha^{30} = \alpha^4+\alpha \\ m_2 \hookrightarrow & \alpha^{17} & = \alpha^4+\alpha+1 & m_8 \hookrightarrow \quad \alpha^{26} = \alpha^4+\alpha^2+\alpha+1 \\ m_3 \hookrightarrow & \alpha^{26} & = \alpha^4+\alpha^2+\alpha+1 & m_9 \hookrightarrow \quad \alpha^3 = \alpha^3 \\ m_4 \hookrightarrow & \alpha^4 & = \alpha^4 & m_{10} \hookrightarrow \quad \alpha^8 = \alpha^3+\alpha^2+1 \\ m_5 \hookrightarrow & \alpha^{13} & = \alpha^4+\alpha^3+\alpha^2 & m_{11} \hookrightarrow \quad \alpha^0 = 1 \\ m_6 \hookrightarrow & \alpha^{26} & = \alpha^4+\alpha^2+\alpha+1 & m_{12} \hookrightarrow \quad \alpha^{18} = \alpha+1 \end{array}$$

y se desea enviarlo al usuario $\mathbf{U}_2$. La llave pública de este usuario $\mathbf{U}_2$ es α^4+1, de esta forma si $k = 2$, para obtener el encriptamiento de m_1, procedemos de la siguiente manera:

$$\begin{aligned} m_1 = \alpha^3+\alpha^2+1 \hookrightarrow \quad & \left(\alpha^2, (\alpha^3+\alpha^2+1)(\alpha^4+1)^2\right) \\ = \quad & (\alpha^2, (\alpha^3+\alpha^2+1)(\alpha^8+1)) \\ = \quad & (\alpha^2, \alpha^4+\alpha^2+\alpha) \end{aligned}$$

Por lo tanto, $(\alpha^2, \alpha^4+\alpha^2+\alpha)$ es la información transmitida al usuario $\mathbf{U}_2$. Obsérvese que esta pareja puede transmitirse como una colección de bits, esto es, de ceros y unos. Esto permite que este tipo de campos sean muy usados en la transmisión de, en general, cualquier tipo de información. Por ejemplo, el dato $(\alpha^2, \alpha+\alpha^2+\alpha^4)$ corresponde a la siguiente pareja de cadenas de bits $(00100, 01101)$.

De forma similar se encriptan los otros mensajes elementales, obteniendo:

$$\begin{array}{ll} m_1 \mapsto & (\alpha^2, \alpha^4+\alpha^2+\alpha) \\ m_2 \mapsto & (\alpha^2, \alpha^3+\alpha) \\ m_3 \mapsto & (\alpha^2, \alpha^4+\alpha^3+\alpha^2+\alpha+1) \\ m_4 \mapsto & (\alpha^2, \alpha^4+\alpha^3+\alpha^2+\alpha) \\ m_5 \mapsto & (\alpha^2, \alpha^2) \\ m_6 \mapsto & (\alpha^2, \alpha^4+\alpha^3+\alpha^2+\alpha) \end{array} \qquad \begin{array}{ll} m_7 \mapsto & (\alpha^2, \alpha^2+\alpha) \\ m_8 \mapsto & (\alpha^2, \alpha^4+\alpha^3+\alpha^2+\alpha) \\ m_9 \mapsto & (\alpha^2, \alpha^3+\alpha^2+\alpha+1) \\ m_{10} \mapsto & (\alpha^2, \alpha^4+\alpha^2+\alpha) \\ m_{11} \mapsto & (\alpha^2, \alpha^3+\alpha^2) \\ m_{12} \mapsto & (\alpha^2, \alpha^4+\alpha^2) \end{array}$$

Al llegar el mensaje al usuario $\mathbf{U}_2$, este procede a su desencriptamiento, de la manera antes mencionada, esto es, si se recibe $C = (c_1, c_2)$, entonces

$m = c_1^{(q-1-x_2)} c_2$. Este procedimiento evita el tener que calcular elementos inversos en el campo, por ejemplo para m_1, tenemos:
$(\alpha^2)^{(32-1-10)} = (\alpha^2)^{21} = \alpha^{31} \cdot \alpha^{11} = \alpha^2 + \alpha + 1$, entonces

$$\begin{aligned} c_1^{(q-1-x_{10})} c_2 &= (\alpha^2 + \alpha + 1)(\alpha^4 + \alpha^2 + \alpha) \\ &= \alpha^3 + \alpha^2 + 1 \end{aligned}$$

que en efecto, es el mensaje elemental m_1. De forma análoga se recuperan los restantes mensajes transmitidos.

2.6 Criptosistema RSA

En 1978, R.L.Rivest, A.Shamir, y L.Adleman ([6.1]) proponen una nueva idea para implementar un criptosistema de llave pública. Apoyando su seguridad en la dificultad de la factorización completa de un número entero muy "grande" crearon el sistema RSA, es quizá, el sistema de llave pública más usado en nuestros días, y han sido muchas las publicaciones sobre su implementación; algunas de ellas se encuentran en [6.8], [6.10], [6.13], [6.14], [6.16]. Su principal aportación ha sido el impulsar la investigación sobre la factorización de números enteros ([11]), que es utilizada para tratar de romper el sistema RSA.

En esta sección se describe su funcionamiento, y se plantean algunos de los problemas que se tienen en su implementación.

Describamos cómo trabaja el sistema RSA:

i) Cada usuario **A** elige dos números primos p_A, q_A extremadamente grandes, de alrededor de 200 dígitos cada uno, y se toma $n_A = p_A q_A$. Como en este caso se conoce la factorización de n_A es fácil calcular $\varphi(n_A) = (p_A - 1)(q_A - 1) = n_A + 1 - p_A - q_A$, donde φ es la función de Euler. Ahora el usuario **A** elige aleatoriamente un entero e_A entre 1 y $\varphi(n_A)$, con la propiedad de que sea primo relativo a $\varphi(n_A)$, o sea, $mcd(e_A, \varphi(n_A)) = 1$.

ii) Se procede a calcular el inverso multiplicativo de e_A módulo $\varphi(n_A)$: $d_A = e_A^{-1} \ mod \ \varphi(n_A)$.

iii) El usuario hace pública la llave de encriptamiento $K_{E,A} = (n_A, e_A)$, y oculta la llave de desencriptamiento $K_{D,A} = (n_A, d_A)$. La transformación de encriptamiento es el mapeo $f : \mathbf{Z}_{n_A} \rightarrow \mathbf{Z}_{n_A}$ que está definido por $f(m) = m^{e_A} \ mod \ n_A$. La transformación de desencriptamiento está dada por $f^{-1}(C) = C^{d_A} \ mod \ n_A$.

El resumen lo tenemos en el siguiente esquema:

$$CpS = \left\{ \mathcal{A}^k \hookrightarrow \mathbf{Z}_n, (f(m) = m^e \ mod \ n), \left(c^d \ mod \ n\right) \right\}$$
$$L = (n, e)$$
$$L^{-1} = (n, d)$$
$$L \not\approx L^{-1}$$

Ahora verifiquemos que las funciones anteriores son inversas una de la otra:

$f^{-1}(f(P)) \equiv f^{-1}(P^{e_A}) \equiv (P^{e_A})^{d_A} \equiv P^{k\varphi(n_A)+1} \equiv \left(P^{\varphi(n_A)}\right)^k P \equiv$
$\equiv P \ mod \ n_A$

Esto sucede si $mcd(P, n_A) = 1$, en este caso $P^{\varphi(n_A)} \equiv 1 \ mod \ n_A$, además como $e_A d_A \equiv 1 \ mod \ \varphi(n_A)$ tenemos que $e_A d_A = k\varphi(n_A) + 1$ para algún k.

Para el caso donde $mcd(P, n_A) \neq 1$ también se cumple la congruencia, aunque la probabilidad de que esto ocurra para primos grandes es muy pequeña.

Si $(P, n_A) > 1$, el resultado se sigue de la siguiente proposición:

PROPOSICIÓN 2.6.1: Sea n un entero libre de cuadrado, producto de primos distintos y d, e tales que $de - 1$ es divisible por $p - 1$, para todo primo p que divide a n, entonces $a^{de} \equiv a \ mod \ n$, para todo a.

DEMOSTRACIÓN: Es suficiente probar que $a^{de} \equiv a \ mod \ p$ para todo a y para cada $p \mid n$, ya que si

$$a^{de} \equiv a \ mod \ p_1$$
$$a^{de} \equiv a \ mod \ p_2$$
$$\vdots$$
$$a^{de} \equiv a \ mod \ p_k$$

donde $n = p_1 p_2 \cdots p_k$, entonces como $p_1 \mid \left(a^{de} - a\right) \ldots . , p_k \mid \left(a^{de} - a\right)$, tenemos que $a^{de} - a = p_1 r_1$, como n es libre de cuadrado y $p_2 \mid \left(a^{de} - a\right)$ se sigue que $a^{de} - a = p_1 p_2 r_2$, de igual forma para p_i $1 \leq i \leq k$, por lo tanto, $a^{de} - a = p_1 p_2 \cdots p_k r_k$, es decir $a^{de} \equiv a \ mod \ n$.

En particular $d_A e_A \equiv 1 \ mod \ \varphi(n_A)$, como $\varphi(n_A) = (p_A - 1)(q_A - 1)$.

i) Si $p \mid a$, entonces también $p \mid a^{de}$, $p \mid a^{de} - a$, o sea $a^{de} \equiv a \ mod \ p$.

ii) Si p no divide a a entonces por el teorema pequeño de Fermat $a^p \equiv a \ mod \ p$, o sea $a^{p-1} \equiv 1 \ mod \ p$ y como $p - 1 \mid de - 1$, entonces $a^{de-1} \equiv 1 \ mod \ p$, y así $a^{de} \equiv a \ mod \ p$.

En la práctica suponemos que el alfabeto tiene N letras, entonces sean $k < l$ enteros positivos tales que, por ejemplo, N^k, N^l, tengan aproximadamente 150 dígitos decimales, mismo múmero de dígitos del producto de los primos. Entonces tomamos como mensajes unidad del texto-ordinario bloques de $k-$letras, que se pueden ver como enteros de $k-$dígitos en base N, es decir, se les asigna un equivalente numérico entre 0 y N^k. Similarmente se toma a los mensajes unidad del texto-encriptado como bloques de $l-$letras en nuestro alfabeto de N letras, así cada usuario A debe elegir sus primos suficientemente grandes p_A, q_A tales que $n_A = p_A q_A$ satisfaga $N^k < n_A < N^l$; $N^k, N^l < n$ por lo que a cualquier mensaje unidad del texto ordinario, es decir, un entero menor que N^k, le corresponde un elemento de $\mathbf{Z}_{n_A}$, y puesto que $n_A < N^l$ la imagen $f(m) \in \mathbf{Z}_{n_A}$ puede escribirse únicamente como un bloque de $l-$letras.

Ejemplos:

Consideremos el siguiente directorio de usuarios, donde $p_1 = 11$, $q_1 = 23$, por lo tanto $n_1 = 253$.

Usuario	n_i	e_i
U_1	253	21
U_2	3800099	77

1) En el primer caso supongamos que deseamos mandar un mensaje al usuario $\mathbf{U}_1$, entonces, como $\varphi(253) = \varphi(11)\varphi(23) = 10 \cdot 22 = 220$ tenemos

primero que e_1 está bien elegido, ya que $220 = 2^2 \cdot 5 \cdot 11$, y $21 = 7 \cdot 3$, entonces, $mcd(21, \varphi(253)) = 1$, supóngase además que se tiene el siguiente encajamiento

$$\begin{array}{cccccccc} A & B & C & \cdots & X & Y & Z \\ \updownarrow & \updownarrow & \updownarrow & \cdots & \updownarrow & \updownarrow & \updownarrow \\ 0 & 1 & 2 & \cdots & 23 & 24 & 25 \end{array}$$

esto es $A^1 \hookrightarrow \mathbb{Z}_{26}$ si consideramos a los mensajes unidad de longitud uno, cada letra se ve como un número módulo 26.

Si el mesaje por enviar es m = "HOY", dividámoslo en mensajes unidad de longitud uno, entonces

$$\begin{aligned} m_1 &= 7 \\ m_2 &= 12 \\ m_3 &= 24 \end{aligned}$$

aplicando la función de encriptamiento $f(m) = m^{e_1} \ mod \ n_1$, tenemos

$$\begin{aligned} 7^{21} \quad mod\ 253 &= 194 \\ 12^{21} \quad mod\ 253 &= 232 \\ 24^{21} \quad mod\ 253 &= 24 \end{aligned}$$

por lo tanto, como cada $m^{e_1} \ mod \ 253 < 26^2$ podemos considerar a cada mensaje encriptado como un mensaje elemental de longitud 2, es decir $194 = 12 + 7 \cdot 26^1$, entonces $f(m_1)$ = "MH", $232 = 24 + 8 \cdot 26^1$, $f(m_2)$ = "YI", $24 = 24 + 0 \cdot 26^1$, $f(m_3)$ = "YA".

Finalmente el mensaje encriptado es $f(m)$ = "MHYIYA".

Para poder desencriptar el mensaje, el usuario $\mathbf{U}_1$ calcula $e_1^{-1} = d_1 \ mod \ \varphi(n_1)$, que en este caso, aplicando el algoritmo de Euclides a 220 y 21 tenemos:

$$1 \ = \ 21 \cdot 21 - 2 \cdot 220$$

lo que nos lleva a $d_1 = 21$, es decir, para recuperar el mensaje ordinario tenemos que elevar el mensaje encriptado a la potencia 21 y reducirlo módulo 253. En este caso tenemos el proceso inverso así:

"MH" = 194,

$(194)^{21} = 1106206812041788448522055539242403262499697721344$
que al reducirlo obtenemos, $194^{21} \equiv 7 \ mod\ 253$.
"YI" =232,
$(232)^{21} = 4734211790606615780573276812110340668809473636 1232$
que al reducirlo obtenemos, $232^{21} \equiv 12 \ mod\ 253$.
"YA"=24
$(24)^{21} = 964797292281744881690597 13024$
que al reducirlo obtenemos, $24^{21} \equiv 24$.

Observemos que al elevar a la potencia 21 en el encriptamiento y, en este caso, también en el desencriptamiento, el resultado obtenido resulta ser un número demasiado grande. He aquí uno de los principales problemas a resolver en la implementación del RSA. Por ejemplo, si m y e tienen 256 "bits" cada uno, necesitaríamos

$$\log_2(m^e) = e \cdot \log_2(m) \approx 2^{256} \cdot 256 = 2^{264} \approx 10^{80}$$

"bits", que sería imposible de almacenar, ¡esto es aproximadamente el número de partículas en el universo! Por otro lado, si suponemos que hubiera 512 millones de computadoras, cada una con 512 MBytes de memoria, el número total de "bits" disponible sería de

$$512 \cdot 2^{20} \cdot 512 \cdot 2^{20} \cdot 8 = 2^{61} \approx 10^{18}$$

que es sólo suficiente para almacenar a m^e, cuando m, e fueran de 55 "bits" ([6.4]).

Lo anterior muestra que es necesario buscar algoritmos que efectúen operaciones módulo un entero, con números "grandes", de tal modo que requieran el mínimo de almacenamiento en memoria. Una serie de estos algoritmos se pueden encontrar en [6.4].

2.7 Otros Criptosistemas

Esta última sección la dedicaremos a mencionar otros criptosistemas, los cuales no se detallarán como los anteriores, pero sin embargo son de gran importancia, ya que en ellos tenemos varias direcciones de la matemática aplicada a la criptografía.

2.7.1 Criptosistema usando campos ciclotómicos

El criptosistema RSA se puede romper si se conoce la factorización del módulo n; sin embargo, no se conoce que el sistema sea seguro si no se resuelve la factorización. Este criptosistema ([15.1]), presenta un ejemplo donde la seguridad es equivalente a la dificultad de factorizar un entero.

2.7.2 Sistema de intercambio de llaves usando campos cuadráticos reales

Este esquema ([15.2], [15.3]), es una generalización del sistema de Diffie y Hellman, basado en la exponenciación del grupo multiplicaitvo $\mathbb{Z}_p^*$. La generalización se hace con un subconjunto de un campo cuadrático real.

2.7.3 Sistema de intercambio de llaves basado en el campo cuadrático imaginario

Este sistema ([15.4]), está basado también en las ideas de Diffie y Hellman, y parece ser más seguro. Se basa en la aritmética de un campo cuadrático imaginario.

2.7.4 Sistema de distribución de llaves usando el anillo de matrices

Este sistema ([15.5]), generaliza el sistema de Diffie y Hellman vía anillos de matrices no singulares sobre $\mathbb{Z}_p$, y matrices triangulares superiores, con elementos invertibles en la diagonal principal sobre $\mathbb{Z}_p$.

2.7.5 Criptosistema de llave pública basado en ecuaciones diofantinas

Este criptosistema ([15.6]), tiene como particularidad que las llaves son fácilmente generadas y los procesos de encriptamiento y desencriptamiento son simples. Para encriptar se efectúa un producto vectorial del mensaje con la llave de encriptamiento. Para desencriptar se realizan varias multiplicaciones y operaciones modulares.

2.7.6 Criptografia cuántica

En los últimos años se ha propuesto un nuevo tipo de computadoras, las computadoras cuánticas. Éstas se basan en las similitudes con las leyes de la macánica cuántica. Por lo tanto, la criptografia cuántica también ha sido desarrollada, así como también el PLD y la factorización en computación cuántica ([15.7]).

2.7.7 Sistema basado en la congruencia de operaciones polinomiales

Un nuevo esquema para autentificar firmas se propone en [15.8], mucho más corto que el esquema RSA y de fácil implementación. Este nuevo esquema está basado en la congruencia de operaciones con polinomios cuyo grado es mayor a 3. La llave secreta consiste de dos números primos p, q "grandes", y la llave pública es el producto $n = p^2q$. La seguridad del esquema depende de factorizar a n.

2.7.8 Sistema "Knapsack" de Merkle y Hellman

En 1978 R.C. Merkle y M.E. Hellman ([5.30]), propusieron el criptosistema conocido como "knapsack", basado en la dificultad de una solución a $\sum x_i a_i = s$, aún cuando se sabe que la solución existe. En donde el mensaje es el vector $m = (x_0, ..., x_{n-1})$, y a_i, s son enteros no negativos ([5.31], [5.32], [5.33], [5.34]).

2.7.9 Criptosistema usando anillo de polinomios

Es un criptosistema ([15.10]) que toma el mismo problema que el sistema de Merkle y Hellman en el anillo de polinomios $K[x]$ donde K es un campo finito.

2.7.10 Criptosistema de Chor-Rivest

Este criptosistema ([5.12]) se basa en el problema de Merkle y Hellman trabajado con elementos de un campo finito $\mathbb{F}_q$.

2.7.11 Digital Signature Algorithm (DSA)

Este sistema ([15.13]) ha combinado el PLD en $\mathbb{Z}_n$ con el uso de funciones "hash". Se ha propuesto por el gobierno de los Estados Unidos para uso estándar, sin embargo, ha recibido varias críticas al pretender tal propósito.

2.7.12 Funciones Hash

En varias ocaciones son usadas las funciones $f : \{0,1\}^x \rightarrow \{0,1\}^t$ de un solo sentido que mapean cadenas de "bits" de longitud arbitraria a una cadena de longitud fija, a estas funciones se les conoce como funciones "hash". Algunos algoritmos como el Message-Digest Algorithms (MD) se encuentran en [15.17].

Capítulo 3

Curvas Elípticas

Introducción: En este capítulo se enuncian algunos resultados básicos sobre curvas elípticas ([9.2]); comenzamos con el concepto de curva elíptica usando la función $\wp$ de Weierstrass sobre los números complejos ([9.6]). Posteriormente se desarrollan las principales propiedades de las curvas elípticas, en particular se ve que los puntos racionales de una curva elíptica forman un grupo abeliano; damos la operación con la que estos puntos forman un grupo, hecho de primordial importancia, ya que éste grupo hará el papel del grupo F_q^* en la construcción de algunos criptosistemas. Finalmente como parte importante en este trabajo, se clasifican a las curvas elípticas sobre campos finitos de acuerdo a las propiedades más usadas en criptografía.

3.1 Introducción a las curvas elípticas sobre $\mathbb{C}$

En esta sección definimos las propiedades elementales de la función $\wp$ de Weierstrass. Esto tiene por objeto, demostrar la relación que hay entre esta función y las curvas elípticas, como forma clásica de abordar tales curvas ([9.6], [9.10]).

Sean e_1, e_2 dos números complejos linealmente independientes sobre los números reales. El conjunto de vectores de la forma $n_1e_1 + n_2e_2$ donde n_1, n_2 son números enteros forman un subgrupo Ω del grupo aditivo del campo de los números complejos $\mathbb{C}$.

DEFINICIÓN 3.1.1: Decimos que una función $f : \mathbb{C} \to \mathbb{C}$ tiene a Ω como grupo de periodos si $f(z + n_1e_1 + n_2e_2) = f(z)$ para todo $z \in \mathbb{C}$ y para todos los enteros n_1, n_2.

PROPOSICIÓN 3.1.2: Dado un subgrupo Ω definido como antes, entonces la serie

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Omega - \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

es normalmente convergente sobre subconjuntos compactos de $\mathbb{C}$.

DEMOSTRACIÓN: Como la convergencia se pide para subconjuntos compactos de $\mathbb{C}$, basta hacerlo para círculos de radio r. Sea entonces $|z| \leq r$, un círculo de radio r; como $|\omega| \geq 2r$ para $\omega \in \Omega$, salvo un número finito de puntos, se tiene que

$$\left| \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right| = \frac{|z| \left| 2 - \frac{z}{\omega} \right|}{|\omega|^3 \left| 1 - \frac{z}{\omega} \right|^2}$$

además $|z| \leq r$ y $|\omega| \geq 2r$, entonces $\frac{1}{2r} \geq \frac{1}{|\omega|}$; usando la desigualdad del triángulo llegamos a

$$\frac{|z| \left| 2 - \frac{z}{\omega} \right|}{|\omega|^3 \left| 1 - \frac{z}{\omega} \right|^2} \leq \frac{\frac{3}{2} r}{|\omega|^3 \frac{1}{4}}$$

por lo tanto

$$\left| \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right| \leq \frac{10r}{|\omega|^3}$$

finalmente se sigue que la serie converge normalmente en el disco $|z| \leq r$, ya que la serie $\sum_{\omega \in \Omega - \{0\}} \frac{1}{|\omega|^3}$ converge ([9.10]).

DEFINICIÓN 3.1.3: La función $\wp(z)$ de Weierstrass es la función meromorfa que define la serie de la proposición 3.1.2. Esta función depende del subgrupo Ω.

En seguida veamos algunas propiedes de la función $\wp$ de Weierstrass.

a) Los polos de $\wp$ son exactamente los puntos $\omega \in \Omega$, y éstos son polos dobles con residuo cero; en una vecindad de $z = \omega$ tenemos

$$\wp(z) = \frac{1}{(z-\omega)^2} + g(z)$$

donde $g(z)$ es holomorfa en esa vecindad.

b) La función $\wp$ es una función par, ya que

$$\wp(-z) = \frac{1}{z^2} + \sum_{\omega \in \Omega - \{0\}} \left(\frac{1}{(z+\omega)^2} + \frac{1}{\omega^2} \right)$$

al sustituir $-\omega$ por ω obtenemos que $\wp(-z) = \wp(z)$.

c) Al considerar la derivada $\wp'$ de $\wp$ y expresarla como serie, derivando término a término ésta también es normalmente convergente en subconjuntos compactos.

Como

$$\wp'(z) = -\frac{2}{z^3} + \sum_{\omega \neq 0} \frac{-2}{(z-\omega)^3} = -2 \sum_{\omega \in \Omega} \frac{1}{(z-\omega)^3}$$

y

$$\wp'(z+\omega_0) = -2 \sum_{\omega \in \Omega} \frac{1}{(z+\omega_0-\omega)^3} = -2 \sum_{\omega \in \Omega} \frac{1}{(z-\omega)^3} = \wp'(z)$$

se cumple para todo $\omega_0 \in \Omega$, entonces $\wp'$ es periódica. Además $\wp'(-z) = -\wp'(z)$.

d) La función $\wp$ es periódica, con grupo de periodos Ω. Es suficiente demostrar que $\wp(z+e_i) = \wp(z)$, $i = 1, 2$.

En resumen, la función $\wp$ de Weierstrass es una función meromorfa con los puntos de Ω como periodos, sus polos son los puntos de Ω, además cada polo tiene orden 2 y parte principal $\frac{1}{(z-\omega)^2}$.

Veamos ahora la expansión de Laurent de $\wp(z)$; dado que $\wp$ es una función par, la expansión de Laurent de $\wp$ en una vecindad del origen es:

$$\wp(z) = \frac{1}{z^2} + a_2 z^2 + a_4 z^4 + \cdots$$

Por otro lado, la función holomorfa $g(z)$ dada en la propiedad a) de la función $\wp$, toma la forma

$$g(z) = \wp(z) - \frac{1}{z^2} = \sum_{\omega \neq 0} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

en una vecindad del cero, además $g(0) = 0$. Para encontrar los coeficientes $a_2, a_4, \ldots$, de la expansión de Laurent en términos del subgrupo Ω, derivamos la serie $g(z)$ término a término; ya que $a_n = \frac{1}{n!} g^{(n)}(0)$, entonces:

$$a_2 = \frac{1}{2} \sum_{\omega \neq 0} \frac{6}{(0-\omega)^4} = 3 \sum_{\omega \neq 0} \frac{1}{\omega^4}$$

y además,

$$a_4 = \frac{(-2)(-3)(-4)}{4!} \sum_{\omega \neq 0} \frac{(-5)}{\omega^6} = \sum_{\omega \neq 0} \frac{5}{\omega^6}$$

Ahora obtengamos una relación importante entre $\wp$ y $\wp'$.

Como $\wp(z) = \frac{1}{z^2} + a_2 z^2 + a_4 z^4 + \cdots$, derivando término a término y elevando al cuadrado tenemos

$$\wp'(z) = \frac{-2}{z^3} + 2a_2 z + 4a_4 z^3 + \cdots$$

$$(\wp'(z))^2 = \frac{4}{z^6} - \frac{8a_2}{z^2} - 16a_4 + \cdots$$

por otro lado, elevando al cubo a $\wp(z)$

$$(\wp(z))^3 = \frac{1}{z^6} + 3(a_2 z^2)\left(\frac{1}{z^4}\right) + 3a_4 z^4 \left(\frac{1}{z^4}\right) = \frac{1}{z^6} + \frac{3a_2}{z^2} + 3a_4 + \cdots$$

por lo tanto,

$$\begin{aligned} \wp'^2 - 4\wp^3 &= \left(\tfrac{4}{z^6} - \tfrac{8a_2}{z^2} - 16a_4 + \cdots\right) - 4\left(\tfrac{1}{z^6} + \tfrac{3a_2}{z^2} + 3a_4 + \cdots\right) \\ &= -20\tfrac{a_2}{z^2} - 28a_4 + z^2(\ldots) \end{aligned}$$

como sabemos que $\frac{1}{z^2} = \wp(z) - a_2 z^2 - a_4 z^4 - \cdots$, entonces,

$$\begin{aligned} \wp'^2 - 4\wp^3 + 20a_2\left(\tfrac{1}{z^2}\right) + 28a_4 &= z^2(\ldots) \\ \wp'^2 - 4\wp^3 + 20a_2\wp + 28a_4 &= z^2(\ldots) \end{aligned}$$

Así, la función $\wp'^2 - 4\wp^3 + 20a_2\wp + 28a_4$ es holomorfa en una vecindad del origen en donde se anula y tiene a Ω como su grupo de periodos, es decir, la función es holomorfa en alguna vecindad de cada punto de Ω; como esta función no tiene polos fuera de Ω, la función es holomorfa en todo el plano, es decir, es entera y puesto que está acotada en cualquier subconjunto compacto, su periodicidad implica que está acotada en $\mathbb{C}$. Como es cero en el origen por el teorema de Liouville, es cero en todo $\mathbb{C}$, o sea:

$$\wp'^2 - 4\wp^3 + 20a_2\wp + 28a_4 = 0$$

Esta relación juega un papel importante, ya que a partir de ésta podemos definir a una curva elíptica sobre $\mathbb{C}$.

DEFINICIÓN 3.1.4: Una curva elíptica afín E sobre el campo de los números complejos es el conjunto algebraico afín definido por el polinomio

$$f(x,y) = y^2 - 4x^3 + g_2x + g_4$$

con $f(x,y) \in \mathbb{C}[x,y]$, $x = \wp(z)$, $y = \wp'(z)$, $g_2 = 20a_2$ y $g_4 = 28a_4$; unión un elemento denotado por $\mathcal{O}$, que en breve justificará su presencia.

La anterior definición de curva elíptica puede ser también vista en el espacio proyectivo $\mathbb{P}^2(\mathbb{C})$, como el conjunto algebraico proyectivo $\tilde{E}$, definido por el polinomio:

$$F(X,Y,Z) = Y^2Z - 4X^3 + g_2XZ^2 + g_4Z^3$$

que con el cambio de variable $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$ regresamos al plano afín $\mathbb{C} \times \mathbb{C}$. En este caso la única clase en $\mathbb{P}^2(\mathbb{C})$, tal que $Z = 0$, es la clase que tiene como representante al punto $(0,1,0)$ que llamaremos punto al infinito $\mathcal{O}$.

Para terminar con esta sección, observemos que lo anterior nos sugiere la existencia de una relación entre el toro complejo $\mathbb{C}/\Omega$ y una curva elíptica

E sobre $\mathbb{C}$. En efecto, existe una fuerte relación entre los toros $\mathbb{C}/\Omega$ y las curvas elípticas E. Además como se verá después, la operación natural de grupo en $\mathbb{C}/\Omega$ es transladada a E mediante $\wp$. Más aún, para cada curva elíptica E sobre $\mathbb{C}$ existen números complejos $g_2(\Omega)$, $g_4(\Omega)$ tales que son los coeficientes de E. Esto lo podemos formalizar en los siguientes hechos: dada Ω, sean $z_1 = \frac{e_1}{2}, z_2 = \frac{e_2}{2}$ y $z_3 = \frac{e_1+e_2}{2}$, entonces todo punto $z \in \mathbb{C}$ tal que $2z \in \Omega$ y $z \notin \Omega$ es congruente a sólo uno de estos puntos. Como $\wp'$ tiene un único polo triple en cada paralelogramo $\Omega(n_1, n_2)$, entonces $\wp'$ tiene a lo más 3 ceros distintos, que son exactamente z_1, z_2 y z_3. De forma análoga $\wp$ toma un valor $\wp(z_0)$ a lo más 2 veces, son exactamente 2 si $2z_0 \notin \Omega$, las raíces z_0 y $-z_0$ de $\wp(z) - \wp(z_0) = 0$. Si $2z_0 \in \Omega$, $z_0 \notin \Omega$, entonces $\wp(z) - \wp(z_0) = 0$ tiene una raíz doble, es decir $\wp'(z_0) = 0$. Por lo tanto, $\wp(z_1), \wp(z_2)$ y $\wp(z_3)$ son tomadas exactamente una vez en cada paralelogramo Ω y además son raíces de la ecuación $4x^3 - g_2x - g_4 = 0$. Como las raíces de $4x^3 - g_2x - g_4$ son diferentes su discriminante $\triangle = g_2^3 - 27g_4^2$ es diferente de cero.
En la siguiente sección veremos cómo un tipo especial de curvas cúbicas con discriminante diferente de cero sobre cualquier campo es llamada curva elíptica.

TEOREMA 3.1.6: El mapeo φ de $\mathbb{C}/\Omega$ en $\mathbb{P}^2(\mathbb{C})$ dado por:

$$z \mapsto \begin{cases} (\wp(z), \wp'(z), 1) & z \notin \Omega \\ (0,1,0) & z \in \Omega \end{cases}$$

es holomorfo y manda a $\mathbb{C}/\Omega$ en una correspondencia uno a uno sobre la curva elíptica proyectiva $\tilde{E} : Y^2Z = 4X^3 - g_2X^2Z - g_4Z^3$.

DEMOSTRACIÓN: φ es holomorfo ya que lo es en cada entrada. Para $z \in \Omega$ consideramos a $\varphi(z) = (z^3\wp(z), z^3\wp'(z), z^3)$ que es holomorfo en $\bar{0} \in \mathbb{C}/\Omega$.

Veamos que φ es sobre: de la definición de curva elíptica, es claro que $\varphi(\mathbb{C}/\Omega) \subseteq \tilde{E} \subset \mathbb{P}^2(\mathbb{C})$. Sea $(x, y, 1) \in \tilde{E}$, como $\wp$ tiene orden 2 existen $z, z^* \neq 0 \in \mathbb{C}$ tal que, ya sea: $\wp(z) = x$ en tal caso $y = \wp'(z)$ y $z \mapsto (x, y, 1)$ ó $\wp(z^*) = x$, en este caso $y = -\wp'(z)$ y $z^* \mapsto (x, y, 1)$, donde z^* es el simétrico de $-z$.

La función φ es uno a uno: supongamos que φ mapea dos puntos distintos no cero $z_1, z_2 \in \mathbb{C}/\Omega$ al mismo punto. Entonces $\wp(z_1) = \wp(z_2)$, como $\wp$ tiene orden 2, $z_2 = z_1^*$ y así $\wp'(z_2) = -\wp'(z_1)$, entonces $\wp'(z_2) = \wp'(z_1) = 0$, por lo

que z_1, z_2 son algunos de los puntos $\left\{\frac{e_1}{2}, \frac{e_2}{2}, \frac{e_1+e_2}{2}\right\}$ por lo tanto $z_1^* = z_1, z_2^* = z_2$ y ya que $z_2 = z_1^*$ obtenemos la contradicción $z_1 = z_2$.

Veamos ahora cómo la estructura de grupo en $\mathbb{C}/\Omega$ puede ser trasladada a $\tilde{E}$, bajo la misma φ.

Primero observemos qué sucede con los puntos de intersección de la recta $y = mx + b$ con la curva afín E. La función $f(z) = \wp'(z) - (m\wp(z) + b)$, tiene un polo de orden 3 en Ω, luego existen 3 ceros z_1, z_2 y z_3 de $f(z)$ tales que $z_1 + z_2 + z_3 \in \Omega$. Es decir, que φ manda a $z_1 + z_2 + z_3 = \bar{0}$ en $\mathbb{C}/\Omega$ a los tres puntos de intersección de la recta $y = mx + b$ con E. Así de forma natural φ debe de mandar respectivamente los tres puntos anteriores a tres puntos $P, Q, R \in E$, tales que $P + Q + R = \mathcal{O}$ (el cero en E); es decir, que $P + Q = -R$. Ahora derivemos a partir de esto, las fórmulas de suma en E. Como $\wp'(z_i) = m\wp(z_i) + b$, para $i = 1, 2, 3$ la ecuación

$$4x^3 - (mx + b)^2 - g_2x - g_4 = 0$$

tiene tres raíces $\wp(z_1), \wp(z_2)$ y $\wp(z_3)$ con suma igual a $\frac{m^2}{4}$, además $z_3 = -(z_1 + z_2)$ y si $\wp(z_1) \neq \wp(z_2)$, tenemos que $\wp'(z_1) - \wp'(z_2) = m(\wp(z_1) - \wp(z_2))$, restando la ecuación de la recta para z_1 y z_2. Como $\wp$ es función par, tenemos que

$$\wp(z_1 + z_2) = \frac{m^2}{4} - \wp(z_1) - \wp(z_2)$$

sustituyendo a m, tenemos:

$$\wp(z_1 + z_2) = -\wp(z_1) - \wp(z_2) + \frac{1}{4}\left(\frac{\wp'(z_1) - \wp'(z_2)}{\wp(z_1) - \wp(z_2)}\right)^2$$

y de forma análoga

$$\wp(2z) = -2\wp(z) + \frac{1}{4}\left(\frac{\wp''(z)}{\wp'(z)}\right)^2$$

Estas operaciones trasladan la estructura de grupo abeliano a la curva elíptica y como veremos después podremos mantener esto para cualquier

campo, ya que las operaciones se obtendrán como función racional de las coordenadas de los puntos.

3.2 Propiedades de las curvas elípticas

En esta sección describiremos brevemente algunas propiedades básicas de las curvas elípticas definidas sobre un campo arbitrario K.

Primero diremos qué se entenderá por una curva elíptica sobre un campo K.

Sea K un campo arbitrario. Una curva cúbica $\tilde{E}$ en su forma normal de Weierstrass en el plano proyectivo $\mathbf{P}^2$, es el conjunto algebraico determinado por el polinomio:

$$F(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$$

donde $a_i \in K$ y $F(X,Y,Z) \in K[X,Y,Z]$. A este conjunto se le conoce comunmente como el conjunto de puntos racionales de la curva cúbica proyectiva $\tilde{E}$.

Aquí también la clase tal que $Z = 0$, es la que tiene como representante al punto $\mathcal{O} = (0,1,0)$, es decir, el punto al infinito.

Con el cambio de variable $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$ obtenemos la curva cúbica E en coordenadas afines, que podemos representar por la relación:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

que llamaremos simplemente forma normal de Weierstrass.

DEFINICIÓN 3.2.1: Una curva elíptica sobre un campo K, es una curva cúbica no-singular en su forma normal de Weierstrass. Es decir una curva cúbica que no tenga puntos singulares, unión el punto al infinito $\mathcal{O}$.

Obsérvese que para el caso complejo la definición coincide, ya que las curvas obtenidas con la función de Weierstrass son no-singulares.

Ahora daremos algunos parámetros de las curvas elípticas, los cuales nos ayudarán a dar una clasificación de éstas.

A partir de la forma normal de Weierstrass:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

definimos los siguientes coeficientes: $b_2 = a_1^2 + 4a_2$, $b_4 = a_1a_3 + 2a_4$, $b_6 = a_3^2 + 4a_6$, $b_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2$, $c_4 = b_2^2 - 24b_4$ y $c_6 = -b_2^3 + 36b_2b_4 - 216b_6$.

Al parámetro $\triangle = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$ se la llama el discriminante de la forma normal de Weierstrass.

Si $\triangle \neq 0$, el $j-$invariante de la forma normal de Weierstrass, se define como $j = \frac{c_4^3}{\triangle}$.

Ahora demos la definición de equivalencia entre dos curvas cúbicas en la forma normal de Weierstrass utilizando los parámetros anteriores y tomando como motivación el caso de curvas elípticas sobre los números complejos.

En el siguiente teorema se hace uso de la igualdad $1728\triangle = c_4^3 - c_6^2$, que se puede obtener fácilmente haciendo las sustituciones requeridas.

DEFINICIÓN 3.2.2: Diremos que las curvas cúbicas E_1, E_2, definidas sobre K:

$$E_1 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

y

$$E_2 : y'^2 + a_1'x'y' + a_3'y' = x'^3 + a_2'x'^2 + a_4'x' + a_6'$$

son equivalentes ($E_1 \sim E_2$) si existe un cambio de variable de la forma $(x, y) \mapsto (u^2x' + r, u^3y' + u^2sx' + t)$, donde $u, r, s, t \in K$, $u \neq 0$ que transforma E_1 en E_2.

Observemos que la relación anterior, es de equivalencia con el cambio de variable inverso $(x', y') \mapsto (u^{-2}(x-r), u^{-3}(y-sx-t+rs))$.

PROPOSICIÓN 3.2.3: Si dos curvas cúbicas son equivalentes, entonces se cumplen las siguientes relaciones entre sus parámetros.

$$\begin{aligned}
ua_1 &= a_1 + 2s \\
u^2a_2' &= a_2 - sa_1 + 3r - s^2 \\
u^3a_3' &= a_3 + ra_1 + 2t \\
u^4a_4' &= a_4 - sa_3 + 2ra_2 - (t+rs)a_1 + 3r^2 - 2st \\
u^6a_6' &= a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1 \\
u^2b_2' &= b_2 + 12r \\
u^4b_4' &= b_4 + rb_2 + 6r^2 \\
u^6b_6' &= b_6 + 2rb_4 + r^2b_2 + 4r^3 \\
u^8b_8' &= b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4 \\
u^4c_4' &= c_4 \\
u^6c_6' &= c_6 \\
u^{12}\triangle' &= \triangle \\
j' &= j
\end{aligned}$$

DEMOSTRACIÓN: Las igualdades anteriores se obtienen haciendo las sustituciones pertinentes.

Primero para los a_i.

i) De la ecuación: $y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$ haciendo $x = u^2x' + r$, y $y = u^3y' + u^2sx' + t$, tenemos lo siguiente:

$(u^3y' + u^2sx' + t)^2 + a_1(u^2x' + r)(u^3y' + u^2sx't) +$
$+a_3(u^3y' + u^2sx't) - (u^2x' + r)^3 - a_2(u^2x' + r)^2 - a_4(u^2x' + r) - a_6 = 0$

ii) Ahora, haciendo los siguientes cálculos:

$(u^3y' + u^2sx' + t)^2 = u^6y'^2 + 2u^5sy'x' + 2u^3y't + u^4s^2x'^2 + 2u^2sx't + t^2$
$(u^2x' + r)(u^3y' + u^2sx' + t) = u^5x'y' + u^4sx'^2 + u^3y'r + u^2rsx' + u^2x't + rt$
$(u^2x' + r)^3 = u^6x'^3 + 3u^4x'^2r + 3u^2x'r + r^3$
$(u^2x' + r)^2 = u^4x'^2 + 2u^2x'r + r^2$

iii) Finalmente asociando términos semejantes obtenemos la curva E_2 :

$$\begin{aligned} u^6y'^2 + (u^52s + a_1u^5)x'y' + (2u^3t + a_1u^3r + a_3u^3)y' - u^6x'^3 - \\ (-u^4s^2 - a_1u^4s + 3u^4r + a_2u^4)x'^2 - \\ (-u^2sa_3 + a_4u^2 - 2u^2st - u^2a_1rs - a_1u^2t + a_2 2u^2r + 3u^2r)x' - \\ (-t^2 - a_1rt - ta_3 + r^3 + a_2r^2 + ra_2 + a_6) \quad = 0 \end{aligned}$$

De donde las relaciones requeridas se siguen de inmediato.

Al verificar las relaciones para los b'_i, se hace uso de las anteriores relaciones para los a'_i

$$\begin{aligned} u^2b'_2 &= (a_1 + 2s)^2 + 4(a_2 - sa_1 + 3r - s^2) \\ &= b_2 + 12r \\ u^4b'_4 &= 2(a_4 - sa_3 + 2ra_2 - ta_1 - rsa_1 + 3r^2 - 2st) + (a_1 + 2s)(a_3 + ra_1 + 2t) \\ &= b_4 + rb_2 + 6r^2 \\ u^6b'_6 &= (a_3 + ra_1 + 2t)^2 + 4(a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1) \\ &= b_6 + 2rb_4 + r^2b_2 + 4r^3 \\ u^8b'_8 &= (a_1 + 2s)^2(a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1) + \\ &\quad +4(a_2 - sa_1 + 3r - s^2)(a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1) - \\ &\quad -(a_1 + 2s)(a_3 + ra_1 + 2t)(a_4 - sa_3 + 2ra_2 - ta_1 - rsa_1 + 3r^2 - 2st) + \\ &\quad +(a_2 - sa_1 + 3r - s^2)(a_3 + ra_1 + 2t)^2 - \\ &\quad -(a_4 - sa_3 + 2ra_2 - ta_1 - rsa_1 + 3r^2 - 2st)^2 \\ &= b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4 \end{aligned}$$

Para las siguientes igualdades se procede de forma similar:

$$\begin{aligned} u^4c'_4 &= b'^2_2 - 24b'_4 \\ &= c_4 \\ u^6c'_6 &= -(b_2 + 12r)^3 + 36(b_2 + 12r)(b_4 + rb_2 + 6r^2) - \\ &\quad -216(b_6 + 36b_2b_4 + r^2b_2 + 4r^3) \\ &= c_6 \\ u^{12}\triangle' &= \frac{c'^3_4 - c'^2_6}{12^3} = \frac{c^3_4 - c^2_6}{12^3} = \triangle \\ j' &= \frac{c'^3_4}{\triangle'} = \left(\frac{c^3_4}{u^{12}}\right) / \left(\frac{\triangle}{u^{12}}\right) = \frac{c^3_4}{\triangle} = j \end{aligned}$$

El siguiente teorema será útil para identificar cuáles de las curvas cúbicas en su forma normal de Weierstrass son curvas elípticas, es decir, no-singulares.

TEOREMA 3.2.4: Sea K un campo tal que $car(K) \neq 2$, y E una curva cúbica en su forma normal de Weierstrass. Entonces E es no singular si y sólo si $\triangle \neq 0$.

DEMOSTRACIÓN: Veamos primero que el punto al infinito $\mathcal{O}$ no puede ser singular. Al considerar a

$F(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$ la forma normal en coordenadas proyectivas tenemos que: $\frac{\partial F}{\partial Z}(\mathcal{O}) = 1$, de donde se sigue el resultado.

Ahora supóngase que E es singular en el punto $p = (x_0, y_0)$; como la traslación $x = x' + x_0$, $y = y' + y_0$ deja a $\triangle$ y a c_4 invariantes, se puede suponer que el punto singular es $(0,0)$ y así

$a_6 = f(0,0) = a_4 = \frac{\partial f}{\partial x}(0,0) = a_3 = \frac{\partial f}{\partial y}(0,0) = 0$; entonces la ecuación toma la forma $f(x,y) = y^2 + a_1xy - a_2x^2 - x^3 = 0$, la cual tiene asociada los parámetros $c_4 = (a_1^2 + 4a_2)^2$ y $\triangle = 0$.

Para terminar basta ver que si f es no singular, entonces $\triangle \neq 0$. Si suponemos que $car(K) \neq 2$, como veremos en breve, la forma normal de Weierstrass se reduce a $y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$. En este caso f es singular si y sólo si existe un punto $(x_0, y_0) \in E$ raíz de las derivadas parciales de f; es decir, que $2y_0 = 12x_0^2 + 2b_2x_0 + 2b_4 = 0$, equivalentemente los puntos singulares son de la forma $(x_0, 0)$ con x_0 raíz doble de $4x^3 + b_2x^2 + 2b_4x + b_6 = 0$, si y sólo si el discriminante $16\triangle$ se anula, obteniendo el resultado.

Enseguida veremos cómo la forma normal de Weierstrass puede ser transformada a formas más simples dependiendo de la característica del campo K, dando los parámetros antes definidos para cada caso.

Considerando la forma normal de Weierstrass de una curva cúbica y un campo tal que $car(K) \neq 2$, al completar cuadrados, tenemos:

$$\left(y + \frac{(a_1x + a_3)}{2}\right)^2 = x^3 + a_2x^2 + a_4x + a_6 + \frac{(a_1x + a_3)^2}{4}$$

haciendo el cambio de variable $y = y - \frac{(a_1x + a_3)}{2}$ se tiene:

$$\begin{aligned} y^2 &= x^3 + a_2x^2 + a_4x + a_6 + \frac{a_1^2x^2 + 2a_1a_3x + a_3^2}{4} \\ &= 4x^3 + (a_1^2 + 4a_2)x^2 + 2(2a_4 + a_1a_3)x + a_3^2 + 4a_6 \end{aligned}$$

la cual finalmente toma la forma

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

donde $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1a_3$ y $b_6 = a_3^2 + 4a_6$

Si ahora $car(K) \neq 2, 3$ con el cambio de variable $(x, y) \mapsto \left(\frac{x-12b_2}{36}, \frac{y}{216}\right)$, se elimina el término cuadrático y así tenemos que la curvas cúbicas tienen la forma:

$$y^2 = x^3 + a_4x + a_6$$

donde $c_4 = -48a_4$, $c_6 = -864a_6$, $\triangle = -16(4a_4^3 + 27a_6^2)$ y $j = 12^3 \frac{4a_4^3}{4a_4^3 + 27a_6^2}$.

En este caso dos curvas son equivalentes si existen las siguientes relaciones entre sus parámetros: $a_4 = u^4a_4'$ y $a_6 = u^6a_6'$.

Otra caracterización sobre curvas cúbicas la tenemos en la siguiente proposición

PROPOSICIÓN 3.2.5: Dos curvas cúbicas sobre K, $car(K) \neq 2, 3$ son equivalentes si y sólo si tienen el mismo j-invariante.

DEMOSTRACIÓN: Como $car(K) \neq 2, 3$, podemos reducir la ecuación de la curva a la forma $y^2 = x^3 + ax + b$; ahora si consideramos a otra curva $y'^2 = x'^3 + a'x' + b$, con el mismo j-invariante, entonces $\frac{4a^3}{(4a^3+27b^2)} = \frac{4a'^3}{(4a'^3+27b'^2)}$, equivalentemente $a^3b'^2 = a'^3b^2$. Para mostrar que las curvas son equivalentes hay que dar un cambio de variable de la forma $(x, y) = (u^2x', u^3y')$. Si $a = 0$, entonces $j = 0$ y $u = \left(\frac{b}{b'}\right)^{\frac{1}{6}}$; si $b = 0$, entonces $j = 1728$, $a \neq 0$ y $b' = 0$, en este caso $u = \left(\frac{a}{a'}\right)^{\frac{1}{4}}$. Para el caso de que $ab \neq 0$ el cambio de variable es cualquiera de los anteriores.

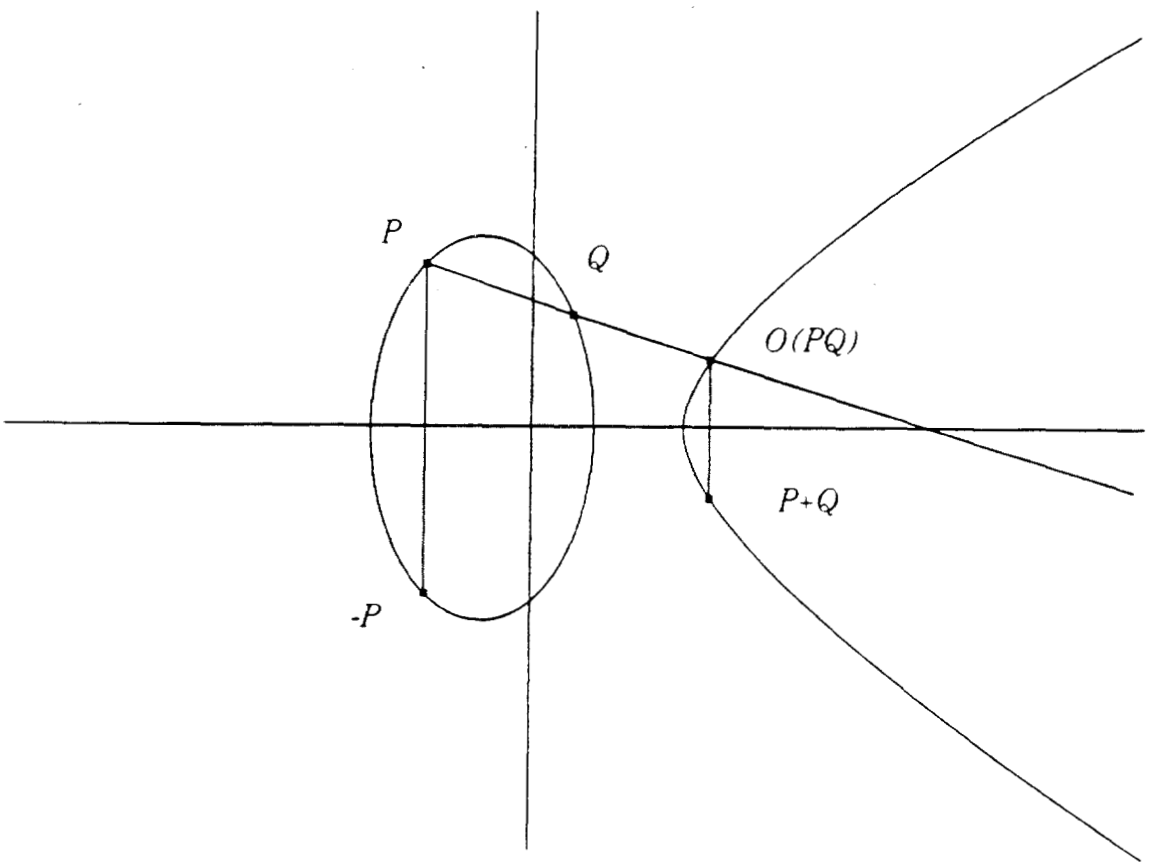
3.2.1 Estructura de grupo en una curva elíptica

En esta subsección daremos las reglas de suma de $P + Q \in E(K)$ en función de las coordenadas de los puntos racionales P, Q, éstas dan estructura de grupo abeliano a una curva elíptica E sobre un campo K y su definición se inspira en el caso complejo.

En 1835, en su trabajo "De usu Theoriae Integralium Ellipticorum et Integralium Abelianorum in Analysis Diophantea", K. Jacobi fue quien primeramente sugirió el uso de la ley de grupo en una curva elíptica. Más tarde en 1921 L.J. Mordell estableció que tal grupo es un grupo abeliano finitamente generado ([9.3]).

La idea geométrica para obtener las reglas de suma es la siguiente: la suma de dos puntos racionales $P, Q \in E(K)$ se define como $P + Q = -O(PQ)$, donde $O(PQ)$ es el tercer punto de intersección entre la curva y la recta determinada por los puntos P, Q; el inverso $-P$ es el punto simétrico a P.

Todo esto lo podemos observar en la siguiente figura:



Tenemos que si el punto $\mathcal{O}$ es el tercer punto de intersección de la curva con cualquier recta vertical, entonces con la idea anterior, $\mathcal{O}$ es la identidad del grupo.

Procedamos primero a encontrar el inverso $-P$ de un punto P.

Cualquier recta que pasa por $\mathcal{O}$ es de la forma $x = x_0$ (las rectas paralelas al eje y), además intersecta a E en los puntos $(x_0, y_1), (x_0, y_2)$ donde y_1, y_2 son raíces de la ecuación

$$y^2 + (a_1 x_0 + a_3)\, y - \left(x_0^3 + a_2 x_0^2 + a_4 x_0 + a_6\right) = 0$$

Ahora si $P = (x, y) \in E$, entonces $-P = (x, y^*)$ donde $y + y^* = -a_1 x - a_3$, ya que la suma de las raíces es igual al negativo del coeficiente de y en la ecuación cuadrática anterior, en otras palabras $-P = (x, -y - a_1 x - a_3)$.

Para obtener las coordenadas del punto $P + Q$ tomemos un par de puntos $P = (x_1, y_1)$, $Q = (x_2, y_2)$; sabemos ahora que $P + Q = -O(PQ)$, donde $O(PQ)$ es el tercer punto de intersección de la recta que pasa por P, Q y la curva E. Resta encontrar el punto $-O(PQ)$ en términos de las coordenadas de P, Q para lo que tenemos los siguientes casos:

i) Si $x_1 \neq x_2$, entonces $P \neq Q$ y la línea determinada por P, Q tiene una ecuación de la forma $y = mx + b$, donde $m = \frac{y_1 - y_2}{x_1 - x_2}$.
ii) Si $x_1 = x_2$, pero $P \neq Q$, entonces la línea determinada por P, Q es $x = x_1$ y en este caso tenemos $Q = -P$.
iii) Si $P = Q$, entonces la línea considerada es la tangente a P.

Considerando ahora la relación:

$$y^2 + a_1 xy + a_3 y = f(x) = x^3 + a_2 x^2 + a_4 x + a_6$$

al derivar tenemos

$$(2y + a_1 x + a_3)\, y' = f'(x) - a_1 y$$

por lo tanto

$$m = y' = \frac{f'(x_1) - a_1 y_1}{2y_1 + a_1 x_1 + a_3}$$

Para encontrar las coordenadas de $P + Q = (x_3, y_3)$ se sustituye a $y = mx + b$ en la ecuación de Weierstrass.

$$(mx + b)^2 + a_1 x (mx + b) + a_3 (mx + b) = x^3 + a_2 x^2 + a_4 x + a_6$$

ordenando términos como un polinomio en x, se tiene:

$$x^3 + \left(a_2 - m^2 - m a_1\right) x^2 + (a_4 - 2mb - a_1 b - m a_3)\, x + \left(a_6 - b^2 - a_3 b\right) = 0$$

Esta ecuación tiene a lo más tres raíces en K, dos de ellas son x_1, x_2 y la tercera es x_3. Ahora como la suma de las raíces es igual al negativo del coeficiente de x^2, y además como $y_3 = mx_3 + b$ tenemos para el primer caso

$$x_3 = m^2 + m a_1 - a_2 - x_1 - x_2$$

así

$$P + Q = (x_3, y_3) = (x_3, -y_3 - a_1 x_3 - a_3)$$

que en términos de valores conocidos, queda sólo saber quién es y_3. Como $-y_3 = -(mx_3 + b)$ y $b = y_1 - m x_1$, entonces

$$\begin{aligned} y_3^* &= -y_3 - a_1 x_3 - a_3 \\ &= -(m x_3 + y_1 - m x_1) - a_1 x_3 - a_3 \end{aligned}$$

de donde llegamos finalmente a las relaciones:

$$\boxed{P + Q = \begin{pmatrix} x_3 \\ y_3 \end{pmatrix} = \begin{pmatrix} m^2 + m a_1 - a_2 - x_1 - x_2 \\ m(x_1 - x_3) - y_1 - a_1 x_3 - a_3 \end{pmatrix}}$$

Para el tercer caso, de forma análoga que el anterior se obtienen las relaciones:

$$\boxed{2P = \begin{pmatrix} x_3 \\ y_3 \end{pmatrix} = \begin{pmatrix} m^2 + m a_1 - a_2 - 2x_1 \\ m(x_1 - x_3) - y_1 - a_1 x_3 - a_3 \end{pmatrix}}$$

Las fórmulas anteriores dan estructura de grupo abeliano a E.

Por construcción $P+Q \in E(K)$, la identidad del grupo es el punto $\mathcal{O}$; para cada punto P, se ha definido el inverso $-P$; además como $y_1 - mx_1 = y_2 - mx_2$, vemos que la operación es conmutativa. Por último, aunque más tedioso, se puede demostrar que la operación definida en $E(K)$ es asociativa.

Obsérvese primero que las coordenadas de $P+Q$ se obtienen al combinar las coordenadas de P y Q, utilizando la suma y el producto del campo K, es decir, estas mismas operaciones pueden ser efectuadas en principio en cualquier campo, considerando la característica del campo en cada caso.

Como un ejemplo, para el caso en que $car(K) \neq 2, 3$, al usar

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

con el cambio de variable $(x, y) \mapsto \left(\frac{x-3b_2}{6^2}, \frac{y}{108}\right)$ transforma la ecuación anterior en

$$y^2 = x^3 + 27\left(-b_2^2 + 24b_4\right) + 54\left(-b_2^3 + 36b_2b_4 - 216b_6\right)$$

que finalmente podemos ver como

$$y^2 = x^3 - 27c_4x - 54c_6$$

Siendo esta relación de la forma $y^2 = x^3 + a_4x + a_6$, donde $a_4 = -27c_4$, $a_6 = -54c_6$.

En este caso las fórmulas de suma en $E(K)$, quedan como

$$\boxed{\begin{pmatrix} x_3 \\ y_3 \end{pmatrix} = \begin{pmatrix} m^2 - x_1 - x_2 \\ m(x_1 - x_3) - y_1 \end{pmatrix}}$$

donde $m = \begin{cases} \frac{y_2-y_1}{x_2-x_1} & si\ P \neq Q \\ \frac{3x_1^2+a_4}{2y_1} & si\ P = Q \end{cases}$

3.3 Curvas elípticas sobre campos finitos de característica 2

En esta sección damos algunos resultados de curvas elípticas definidas sobre campos finitos de característica 2. Estos resultados se usan en la siguiente sección para estudiar la estructura de los puntos racionales, la mayoría de éstos se pueden encontrar en [10]. Lo relevante en nuestro caso es encontrar aquellas curvas que sean más útiles en criptografía.

3.3.1 Clases de equivalencia de curvas elípticas sobre $\mathbb{F}_{2^m}$

Aquí damos la clasificación de las curvas elípticas definidas sobre el campo finito $\mathbb{F}_{2^m}$.

Partimos de la forma normal de Weierstrass:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Como $j(E) = \frac{c_4^3}{\Delta}$, $c_4 = b_2^2 - 24b_4 = b_2^2$, y $b_2 = a_1^2 + 4a_2 = a_1^2$, (véase sección 3.2), entonces $j(E) = \frac{a_1^{12}}{\Delta}$. Una clasificación de estas curva de acuerdo a su $j-$invariante es la siguiente:

a) Si $j(E) = 0$, es decir, $a_1 = 0$. Al hacer el cambio de variable

$$(x, y) \mapsto (x + a_2, y)$$

tenemos:

$$y^2 + a_3y = x^3 + \left(3a_2^2 + a_4\right)x + a_4a_2 + a_6$$

por lo tanto, al renombrar y simplificar la ecuación toma la forma:

$$E : y^2 + a_3y = x^3 + a_4x + a_6$$

donde $j(E) = 0$, y como $b_2 = b_4 = 0$, y $b_6 = a_3^2$, se tiene $\Delta = a_3^4$.

A este tipo de curvas elípticas se les da el nombre de *supersingulares*.

b) Si $j(E) \neq 0$, entonces $a_1 \neq 0$. Haciendo el cambio de variable

$$(x, y) \mapsto \left(a_1^2 x + \frac{a_3}{a_1}, a_1^3 y + \frac{a_1^2 a_4 + a_3^2}{a_1^3} \right)$$

obtenemos

$a_1^6 y^2 + a_1 yx + x(a_1^2 a_4 + a_3^2) + \frac{a_1^4 a_4^2 + a_3^4}{a_1^6} =$

$a_1^6 x^3 + x^2(3a_1^3 a_3 + a_1^4 a_2) + x(3a_3^2 + a_4 a_1^2) + \frac{a_3^3}{a_1^3} + \frac{a_2 a_3^2}{a_1^2} + \frac{a_4 a_3}{a_1} + a_6$

Simplificando

$$a_1^6 y^2 + a_1^6 yx = a_1^6 x^3 + x^2 \left(3a_1^3 a_3 + a_1^4 a_2 \right) + a_6 a_1^6$$

que al dividir por a_1^6, la forma normal de Weierstrass se transforma en:

$$E : y^2 + xy = x^3 + a_2 x^2 + a_6$$

donde al hacer las sustituciones tenemos $\triangle = a_6$ y $j = \frac{1}{a_6}$. Este otro tipo de curvas elípticas se conocen como $no - supersingulares$.

Ahora veamos cómo son las clases de equivalencia que tenemos en estos dos tipos de curvas elípticas, con la relación definida en la sección 3.2.

La respuesta la tenemos con el siguiente teorema.

TEOREMA 3.3.1.1: Las curvas elípticas sobre $\mathbb{F}_{2^m}$, se clasifican de la siguiente forma:

i) Si $j \neq 0$, entonces hay $2(2^m - 1)$, clases de equivalencia de curvas elípticas $no - supersingulares$.

ii) Si $j = 0$, y m es impar, hay 3 clases de equivalencia.

iii) Si $j = 0$, y m es par, hay 7 clases de equivalencia.

DEMOSTRACIÓN:

i) De 3.3.1 b) una curva elíptica con $j \neq 0$, tiene la forma:

$$E : y^2 + xy = x^3 + a_2 x^2 + a_6$$

con $a_6 \neq 0$. Por el teorema 3.2.3 una curva E' es equivalente a E cuando se cumplen las siguientes relaciones:

$$\begin{aligned} ua_1' &= a_1 + 2s \\ u^2a_2' &= a_2 - sa_1 + 3r - s^2 \\ u^3a_3' &= a_3 + ra_1 + 2t \\ u^4a_4' &= a_4 - sa_3 + 2ra_2 - (t + rs)\,a_1 + 3r^2 - 2st \\ u^6a_6' &= a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1 \end{aligned}$$

donde $u, r, s, t \in \mathbb{F}_{2^m}$, $u \neq 0$. Al considerar las condiciones para este caso, es decir, $a_1 = a_1' = 1$, $a_3 = a_3' = a_4 = a_4' = 0$, las relaciones anteriores se reducen a:

$$a_6' = a_6, \quad a_2' = a_2 + s + s^2$$

Entonces, dos curvas con $j \neq 0$, son equivalentes si y sólo si $a_6' = a_6$ y $tr\,(a_2') = tr\,(a_2)$.

Sea γ un elemento en $\mathbb{F}_{2^m}$, tal que $tr\,(\gamma) = 1$ (si m es impar se puede tomar $\gamma = 1$), entonces las clases de equivalencia las podemos representar como

$$\left\{ y^2 + xy = x^3 + a_2x^2 + a_6 \mid a_6 \in \mathbb{F}_{2^m}^*,\ a_2 = 0,\ \gamma \right\}$$

Por lo tanto, hay $2\,(2^m - 1)$ clases de equivalencia. Una curva equivalente a E, es entonces $y^2 + xy = x^3 + \alpha x^2 + a_6$, donde α es cualquiera de los $q/2$ elementos de $\mathbb{F}_{2^m}$, $q = 2^m$ tales que $tr\,(\alpha) = tr\,(a_2)$ y el cambio de variable está dado por $f : (x, y) \mapsto (x, y + sx)$ donde $s^2 + s = a_2 + a_2'$.

ii) Para este caso obsérvese que el mapeo $f : x \mapsto x^3$ es inyectivo si m es impar, en $\mathbb{F}_{2^m}$, más aún, es un polinomio permutación ([2.1]). Ahora si

$$E' : y^2 + a_3'y = x^3 + a_4'x + a_6'$$

es una curva elíptica con $j = 0$, y $a_3' \neq 0$. Entonces haciendo el cambio de variable $(x, y) \mapsto (r^2x, r^3y)$, con $r = (a_3')^{\frac{1}{3}}$, y aplicándolo a E', se tiene:

$$\begin{aligned} r^6y^2 + a_3'r^3y &= r^6x^3 + a_4'r^2x + a_6' \\ &= r^6x^3 + a_4'r^2x + a_6' \\ y^2 + y &= x^3 + a_4x + a_6 \end{aligned}$$

Por lo tanto, podemos suponer que una curva elíptica sobre $\mathbb{F}_{2^m}$ con $j = 0$, tiene la forma:

$$E : y^2 + y = x^3 + a_4 x + a_6$$

y como $a_4, a_6 \in \mathbb{F}_{2^m}$, tenemos 2^{2m} curvas.

Ahora procedamos a encontrar exactamente quiénes son las clases de equivalencia entre estas curvas, dando a uno de sus representantes.

Si $E' \sim E$ (son equivalentes), en este caso $a_1 = a_2 = 0$ y $a_3 = 1$, de las relaciones de la proposición 3.2.3 llegamos a las ecuaciones

$$\begin{aligned} s^4 + s + a_4 + a_4' &= 0 \\ t^2 + t + s^6 + a_4 s^2 + a_6 + a_6' &= 0 \end{aligned}$$

$r, s, t \in \mathbb{F}_{2^m}$; y el cambio de variable es $(x, y) \mapsto (x + s^2, y + sx + t)$.

Considerando a la curva

$$E_1 : y^2 + y = x^3$$

y si $E \sim E_1$, existen $s, t \in \mathbb{F}_{2^m}$ que satisfacen las relaciones

$$\begin{aligned} s^4 + s + a_4 &= 0 \\ t^2 + t + s^6 + a_6 &= 0 \end{aligned}$$

Puesto que m es impar del anexo en [10.8], $s^4 + s + a_4 = 0$ tiene exactamente dos soluciones en $\mathbb{F}_{2^m}$, si s_0 es una de ellas $s_0 + 1$ es la otra; para la segunda ecuación también tenemos a t_0 y a $t_0 + 1$ como soluciones; pero si $tr(s_0^6 + a_6) = 0$, entonces $tr\left((s_0 + 1)^6 + a_6\right) = tr((s_0^4 + 1)(s_0^2 + 1) + a_6) = 1$, por lo que, sólo (t_0, s_0) y $(t_0 + 1, s_0)$ son soluciones de ambas ecuaciones. Es decir, que para cada par de soluciones tenemos una curva equivalente a E_1 y como hay q^2 posibles curvas, tenemos $\frac{q^2}{2}$ curvas isomorfas a E_1.

Ahora, consideremos a la curva

$$E_2 : y^2 + y = x^3 + x$$

Claramente se observa que $E_1 \not\sim E_2$, ya que sus coeficientes no cumplen las condiciones de equivalencia. Por otra parte, si $E \sim E_2$, entonces existen $s, t \in \mathbb{F}_{2^m}$ que satisfacen las ecuaciones

$$\begin{aligned} s^4 + s + 1 + a_4 &= 0 \\ t^2 + t + s^6 + s^2 + a_6 &= 0 \end{aligned}$$

En este caso tenemos las 4 soluciones $(s_0, t_0), (s_0, t_0 + 1), (s_0 + 1, t_0)$ y $(s_0 + 1, t_0 + 1)$; por lo que existen $\frac{q^2}{4}$ curvas isomorfas a E_2.

Finalmente consideremos a la curva

$$E_3 : y^2 + y = x^3 + x + 1$$

y a las ecuaciones

$$\begin{aligned} s^4 + s + 1 + a_4 &= 0 \\ t^2 + t + s^6 + s^2 + 1 + a_6 &= 0 \end{aligned}$$

Es fácil también ver que $E_1 \not\sim E_3$ y $E_2 \not\sim E_3$; además, de forma similar que el caso anterior, existen $\frac{q^2}{4}$ curvas equivalentes a E_3.

Para concluir esta parte del teorema diremos que una curva elíptica sobre el campo $\mathbb{F}_{2^m}$ con j-invariante cero y m impar es equivalente a una de las siguientes tres curvas:

$$\begin{aligned} E_1 &: y^2 + y = x^3 \\ E_2 &: y^2 + y = x^3 + x \\ E_3 &: y^2 + y = x^3 + x + 1 \end{aligned}$$

iii) En este caso existen 7 clases de equivalencia y para su obtención se procede de forma similar que el caso anterior ([10.8]).

Por ejemplo, si consideramos el campo $\mathbb{F}_{2^2} = \{0, 1, \alpha, 1+\alpha\}$ entonces, tenemos 6 clases de equivalencia y como $tr(\alpha) = \alpha + \alpha^2 = 1$, los 6 representantes de las clases de equivalencia son:

$$\begin{array}{ll} y^2 + xy = x^3 + 1 & y^2 + xy = x^3 + \alpha x^2 + 1 \\ y^2 + xy = x^3 + \alpha & y^2 + xy = x^3 + \alpha x^2 + \alpha \\ y^2 + xy = x^3 + \alpha + 1 & y^2 + xy = x^3 + \alpha x^2 + \alpha + 1 \end{array}$$

3.3.2 Ley de grupo sobre $E(\mathbb{F}_{2^m})$

En esta subsección damos explícitamente la ley de grupo sobre los puntos racionales de una curva elíptica sobre campos de característica 2. Estas operaciones se realizan en el campo finito $\mathbb{F}_{2^m}$, y de su realización depende en mucho la rapidez de un criptosistema que usa curvas elípticas. Es decir, nos interesa que estas operaciones se realicen en el menor tiempo posible.

De acuerdo con el teorema 3.3.1.1, y las fórmulas de la sección 3.2.1 consideramos los siguientes casos:

a) Caso *supersingular*, esto es si $j = 0$, donde

$$E : y^2 + a_3 y = x^3 + a_4 x + a_6$$

Si $P = (x_1, y_1)$ y $Q = (x_2, y_2)$, entonces $-P = (x_1, -y_1 - a_1 x_1 - a_3)$; como $a_1 = a_2 = 0$ tenemos que $-P = (x_1, y_1 + a_3)$.

Ahora si $Q \neq \pm P$, $P + Q = (x_3, y_3)$ donde

$$\begin{aligned} x_3 &= m^2 + m a_1 - a_2 - x_1 - x_2 \\ &= m^2 + x_1 + x_2 \end{aligned}$$

$m = \frac{y_1 + y_2}{x_1 + x_2}$, y

$$\begin{aligned} y_3 &= m(x_1 - x_3) - y_1 - a_1 x_3 - a_3 \\ &= m(x_1 + x_3) + y_1 + a_3 \end{aligned}$$

Para el caso donde $P = Q$,

$$x_3 = m^2$$

donde $m = \frac{x_1^2 + a_4}{a_3}$ para la segunda coordenada

$$\begin{aligned} y_3 &= m(x_1 - x_3) - y_1 - a_1 x_3 - a_3 \\ &= m(x_1 + x_3) + y_1 + a_3 \end{aligned}$$

Lo anterior lo podemos resumir en las siguientes relaciones:

$$\begin{pmatrix} x_3 \\ y_3 \end{pmatrix} = \begin{pmatrix} \left(\frac{y_1+y_2}{x_1+x_2}\right)^2 + x_1 + x_2 \\ \left(\frac{y_1+y_2}{x_1+x_2}\right)(x_1 + x_3) + y_1 + a_3 \end{pmatrix}, \; si \; P \neq Q$$

y

$$\begin{pmatrix} x_3 \\ y_3 \end{pmatrix} = \begin{pmatrix} \frac{x_1^4 + a_4^2}{a_3^2} \\ \left(\frac{x_1^2 + a_4}{a_3}\right)(x_1 + x_3) + y_1 + a_3 \end{pmatrix}, \; si \; P = Q$$

b) Caso *no-supersingular* ($j \neq 0$).

$$E : y^2 + xy = x^3 + a_2 x^2 + a_6$$

En este caso $a_1 = 1$ y $a_3 = a_4 = 0$, entonces $-P = (x_1, y_1 + x_1)$.
Si $P \neq \pm Q$, entonces $P + Q = (x_3, y_3)$ donde

$$x_3 = m^2 + m + x_1 + x_2 + a_2$$

$m = \frac{y_1+y_2}{x_1+x_2}$, y

$$y_3 = m(x_1 + x_3) + y_1 + x_3$$

Ahora si $P = Q$,

$$x_3 = m^2 + m + a_2$$

donde $m = \frac{3x_1^2 + 2a_2 x_1 - a_1 y_1}{2y_1 + a_1 x_1 + a_3} = x_1 + \frac{y_1}{x_1}$.

Lo que podemos resumir en:

$$\begin{pmatrix} x_3 \\ y_3 \end{pmatrix} = \begin{pmatrix} \left(\frac{y_1+y_2}{x_1+x_2}\right)^2 + \frac{y_1+y_2}{x_1+x_2} + x_1 + x_2 + a_2 \\ \left(\frac{y_1+y_2}{x_1+x_2}\right)(x_1+x_3) + x_3 + y_1 \end{pmatrix}, \; si \; P \neq Q$$

y

$$\begin{pmatrix} x_3 \\ y_3 \end{pmatrix} = \begin{pmatrix} x_1^2 + \frac{a_6}{x_1^2} \\ x_1^2 + \left(x_1 + \frac{y_1}{x_1}\right) x_3 + x_3 \end{pmatrix}, \; si \; P = Q$$

3.3.3 El grupo de puntos racionales $E(\mathbb{F}_{2^m})$

Por último, describimos la clasificación de los grupos que se obtienen al considerar los puntos racionales de una curva elíptica sobre un campo finito de característica 2 ([10.6], [10.7]).

Como ya se ha mencionado, una de las características más importantes de las curvas elípticas, es que sus puntos racionales forman un grupo abeliano finitamente generado. En esta sección enunciamos los resultados básicos de este hecho.

Nosotros basamos nuestra atención en clasificar el grupo $E(K)$ para los casos de nuestro interés y hablaremos principalmente del tipo de grupo que obtengamos y el número de elementos que tiene el grupo.

Si suponemos que K es un campo finito con $q = p^n$ elementos, E una curva elíptica y $E(K)$ el grupo de sus puntos racionales, entonces tenemos el siguiente resultado conjeturado por E. Artin en su tesis y probado en los años 30 por Hasse.

TEOREMA 3.3.3.3 ([9.1], [10.5]): Sea E una curva elíptica sobre un campo finito K con q elementos, entonces

$$|\#(E(K)) - q - 1| \leq 2\sqrt{q}$$

Mas concretamente tenemos lo siguiente:

TEOREMA 3.3.3.4: Sea E una curva elíptica sobre el campo finito K con $q = p^n$ elementos y $a = \#E(K)$ dado por $a = 1 + q - b$, donde b es un entero tal que $|b| \leq 2\sqrt{q}$. Entonces todos los valores de a posibles satisfacen las siguientes condiciones:

i) Si n es par: $b = \pm 2\sqrt{q}$,

ii) Si n es par y $p \not\equiv 1 \ mod\ 3 : b = \pm\sqrt{q}$,

iii) Si n es impar y $p = 2$ ó 3: $b = \pm p^{(n+1)/2}$,

iv) Si $p \not\equiv 1 \ mod\ 4 : b = 0$,

v) $mcd(b, p) = mcd(b, q) = 1$.

La demostración de este teorema se puede encontrar en [10.4].

Veamos algunos ejemplos en cada caso.

i) Si $n = 10$, $p = 2$, entonces $\#E(\mathbb{F}_{2^{10}}) = 1 + 2^{10} \pm 2^5$.

ii) Si $n = 5$, $p = 2$, entonces $\#E(\mathbb{F}_{2^5}) = 1 + 2^5 \pm 2^3$.

iii) Si $n = 155$, $p = 2$, entonces $\#E(\mathbb{F}_{2^{155}}) = 1 + 2^{155} \pm 2^{78}$, esto es, en el mejor de los casos tenemos un grupo con

45671926166590716193865453253838748021541568513 elementos

iv) Si $n = 100$, $p = 7$, entonces $\#E(\mathbb{F}_{7^{100}}) = 1 + 7^{100}$.

v) Si $n = 100$, $p = 11$, entonces $\#E(\mathbb{F}_{11^{100}}) = 1 + 11^{100}$.

La estructura de grupo de los puntos racionales de una curva elíptica sobre un campo finito se describe en seguida.

TEOREMA 3.3.3.5: Con las mismas condiciones del teorema anterior, tenemos los siguientes casos para el grupo $E(K)$.

a) Para el caso i) del teorema anterior, el grupo $E(K)$ es $\left(\mathbb{Z}_{q^{1/2}\pm 1}\right)^2$.

b) Para el caso ii) y iii) el grupo $E(K)$ es cíclico.

c) Para iv) el grupo $E(K)$ es $\mathbb{Z}_2 \oplus \mathbb{Z}_{(q+1)/2}$ ó cíclico si $q \equiv 3 \ mod\ 4$; y cíclico en cualquier otro caso.

d) Para el caso v) el grupo es de la forma

$$\mathbb{Z}_{p^{h_p}} \oplus \prod_{l \neq p} \left(\mathbb{Z}_{l^{a_l}} \oplus \mathbb{Z}_{l^{h_l - a_l}}\right)$$

donde $h = \prod_l l^{h_l}$ es el orden del grupo, y $0 \leq a_l \leq h_l$.

La demostración se puede consultar en [10.6], [10.7].

Como podemos ver ahora, en muchos casos la estructura de grupo de los puntos $K-$racionales de una curva elíptica sobre un campo finito, tiene una forma simple, y en general, como veremos en el capítulo siguiente, algo de nuestro interés es que el grupo sea cíclico o "casi" cíclico. Esto hace al conjunto $E(K)$ mejor para ser usado en criptografía.

Para finalizar damos los resultados para algunos casos de característica 2. Primero, veamos la conjetura de Weil que nos ayudará para tal fin.

Si una curva elíptica está definida sobre $\mathbb{F}_q$ con $q = p^n$ elementos, ésta también se puede considerar definida sobre $\mathbb{F}_{q^m}$, $m \geq 1$ por lo que tiene sentido hablar de los $\mathbb{F}_{q^m}-$puntos racionales de la curva . Si N_m es el número de puntos racionales de E sobre $\mathbb{F}_{q^m}$, tenemos la siguiente definición:

Sea E una curva elíptica sobre $\mathbb{F}_q$, entonces la función zeta de E, con indeterminada T es:

$$Z\left(T, E\mid_{\mathbb{F}_q}\right) = exp(\sum_{m=1}^{\infty} N_m T^m/m)$$

TEOREMA 3.3.3.6 ([9.1]): La función zeta de una curva elíptica sobre $\mathbb{F}_q$, es una función racional de T y tiene la forma:

$$Z(T) = \frac{1 - aT + qT^2}{(1-T)(1-qT)}$$

done a depende de E y $N_1 = q + 1 - a$. El discriminante del polinomio cuadrático del numerador es negativo, es decir, $a^2 < 4q$. Luego este polinomio tiene dos raíces conjugadas complejas α, β con norma $\sqrt{q}$.

Este resultado lo podemos usar para calcular el número de puntos racionales de una curva elíptica definida en extensiones del campo $\mathbb{F}_2$. Para cualquier curva algebraica definida sobre $\mathbb{F}_q$, veamos que la siguiente relación es válida.

$$N_m = q^m + 1 - \alpha^m - \beta^m$$

Ésta se deduce fácilmente, partiendo de la relación:

$$\sum_{m=1}^{\infty} N_m T^m/m = \log\left(\frac{(1-T)(1-qT)}{(1-\alpha T)(1-\beta T)}\right)$$

del lado izquierdo tenemos una serie convergente, entonces cada coeficiente puede ser obtenido por $a_m = \frac{1}{m!} f^{(m)}(0)$, donde $a_m = N_m/m$ y $f(T)$ es el lado derecho de la ecuación anterior, por lo tanto:

$$f'(T) = \frac{-\alpha - \beta + 2T\alpha\beta}{(1-\alpha T)(1-\beta T)} - \frac{-q - 1 + 2qT}{(1-T)(1-qT)}$$

$f'(0) = -\alpha - \beta + q + 1$, entonces $N_1 = -\alpha - \beta + q + 1$.

Para el caso $m = 2$, tenemos

$$\begin{aligned} f''(T) &= \frac{(1-\alpha T)(1-\beta T)2\alpha\beta - (-\alpha - \beta + 2\alpha\beta T)^2}{(1-\alpha T)^2(1-\beta T)^2} - \\ &\quad - \frac{(1-T)(1-qT)2q - (-q-1+2qT)^2}{(1-T)^2(1-qT)^2} \end{aligned}$$

con $N_2 = 2f''(0)/2$ tenemos que

$N_2 = 2\alpha\beta - (-\alpha - \beta)^2 - 2q + (q+1)^2 = -\alpha^2 - \beta^2 + q^2 + 1$, y en forma inductiva tenemos el resultado requerido.

Para finalizar damos una lista de los tipos de grupo que corresponden a las curvas elípticas supersingulares. Para su obtención procedemos como en el siguiente ejemplo:

Sea la curva $y^2 + y = x^3$ sobre el campo $\mathbb{F}_{2^m}$, con m impar. Entonces por el teorema 3.3.3.5 el grupo $E(\mathbb{F}_2)$ es cíclico y $\#E(\mathbb{F}_2) = q + 1 - b$. Para obtener el número de elementos de este grupo, advertimos primero que E sobre $\mathbb{F}_2$, tiene a $\{(0,0),(0,1),(1,0)\}$ como puntos racionales finitos, es decir, $N_1 = q + 1 - a = 3$, lo que implica que $a = 0$. Por lo tanto, la función zeta toma la forma $Z(T) = \frac{(1+2T^2)}{(1-T)(1-2T)}$; las raíces del numerador son $r_1 = \frac{i}{\sqrt{2}}$ y $r_2 = -\frac{i}{\sqrt{2}}$. Entonces $\alpha = i\sqrt{2}$ y $\beta = -i\sqrt{2}$, por lo tanto, $N_m = 2^m + 1 - \left(i\sqrt{2}\right)^m - \left(-i\sqrt{2}\right)^m = 2^m + 1$, cuando m es impar.

De forma análoga podemos clasificar los grupos de puntos racionales para los representantes de las 3 clases de equivalencia de curvas elípticas supersingulares definidas sobre $\mathbb{F}_{2^m}$, con m impar y $j = 0$, (véase parte ii del teorema 3.3.1.1) resumidos en la siguiente tabla:

Curva	m	Orden	Tipo de grupo
$y^2 + y = x^3$	*impar*	$q+1$	*cíclico*
$y^2 + y = x^3 + x$	$m \equiv 1,7 \ mod\ 8$	$q+1+\sqrt{2q}$	„
	$m \equiv 3,5 \ mod\ 8$	$q+1-\sqrt{2q}$	
$y^2 + y = x^3 + x + 1$	$m \equiv 1,7 \ mod\ 8$	$q+1-\sqrt{2q}$	„
	$m \equiv 3,5 \ mod\ 8$	$q+1+\sqrt{2q}$	

El grupo de puntos racionales de una curva elíptica definida sobre un campo de la forma $\mathbb{F}_{2^m}$ será utilizado en capítulos posteriores para describir algunos criptosistemas.

Capítulo 4

Criptosistemas sobre $E(\mathbb{Z}_p)$

Introducción: En este capítulo damos los elementos básicos para construir criptosistemas usando el grupo $E(\mathbb{Z}_p)$, que forman los puntos racionales de una curva elíptica sobre el campo finito $\mathbb{Z}_p$, con p un número primo mayor que 3. Esto como introducción al próximo capítulo donde estudiaremos criptosistemas usando campos finitos de característica 2.

La mayor parte de lo que trataremos aquí gira alrededor de dos conceptos importantes en criptografía: la seguridad y la implementación.

4.1 Curvas elípticas sobre $\mathbb{Z}_p$

El caso de curvas elípticas definidas sobre un campo finito $\mathbb{F}_q$, de característica mayor a 3 tiene (de 3.2) la forma normal de Weierstrass siguiente:

$$E : y^2 = x^3 + ax + b$$

con $a, b \in \mathbb{F}_q$, $\triangle = -16(4a^3 + 27b^2)$ y $j = -1728(4a)^3/\triangle$, además consideraremos que $\triangle \neq 0$. En este caso a la curva la denotaremos como $E_{a,b}$.

Veamos primero cómo se clasifican las curvas elípticas sobre este tipo de campos finitos.

Si dos curvas $E_{a,b}$ y $E_{a',b'}$ son equivalentes, existe por 3.2, una solución $u_0 \in \mathbb{Z}_p^*$ de las ecuaciones $u^4a' = a$ y $u^6b' = b$. La solución nos proporciona el cambio de coordenadas que transforma la ecuación de $E_{a,b}$ en la ecuación de $E_{a',b'}$, dada en este caso por $\varphi(x, y) = (u_0^2x, u_0^3y)$.

Para obtener a u_0 consideramos los siguientes 3 casos:

i) Si $ab \neq 0$, entonces $u^2 = \frac{a'b}{ab'}$, y si u_0 es una solución fija de esta ecuación las soluciones son $\{u_0, -u_0\}$.

ii) Si $a = 0$ y $b \neq 0$, la ecuación es $u^6 = \frac{b}{b'}$, entonces, si $\mathbb{Z}_p^*$ tiene un elemento α de orden 3 las soluciones son $\{\pm u_0, \pm \alpha u_0, \pm \alpha^2 u_0\}$, de lo contrario serán $\{u_0, -u_0\}$.

iii) Si $a \neq 0$ y $b = 0$, la ecuación es $u^4 = \frac{a}{a'}$, y si $\mathbb{Z}_p^*$ tiene un elemento β de orden 4, entonces las soluciones son $\{u_0, \beta u_0, \beta^2 u_0, \beta^3 u_0\}$ de lo contrario serán $\{u_0, -u_0\}$.

El caso particular donde E es equivalente a sí misma, a φ se le llama automorfismo de E. El número de automorfismos se denota por $\#Aut(E)$; de los tres casos anteriores, si $a = 0$ y $\mathbb{Z}_p^*$ tiene un elemento de orden 6, entonces $\#Aut(E) = 6$. Si $b = 0$ y $\mathbb{Z}_p^*$ tiene un elemento de orden 4, entonces $\#Aut(E) = 4$; en el resto de los casos $\#Aut(E) = 2$ ([12.1]).

Para calcular el número de curvas equivalentes a una curva fija E, observamos, de los 3 casos anteriores, que para cada $u \in \mathbb{Z}_p^*$, existe otra curva E' equivalente a E. Entonces el número de curvas equivalentes a E es $\frac{p-1}{\#Aut(E)}$.

Como el número de soluciones a, b, de la ecuación $4a^3 + 27b^2 = 0$, en un campo finito es p ([12.1]); entonces el número de curvas elípticas definidas en $\mathbb{Z}_p$ es $p^2 - p$, así:

$$\sum_E \frac{p-1}{\#Aut(E)} = p^2 - p$$

ó

$$\sum_E \frac{1}{\#Aut(E)} = p$$

TEOREMA 4.1.1: El número N_p de clases de equivalencia de las curvas elípticas definidas sobre el campo finito $\mathbb{Z}_p$ con $p > 3$, es $2p+6$, $2p+2$, $2p+4$, $2p$ para $p \equiv 1, 5, 7, 11 \pmod{12}$ respectivamente.

DEMOSTRACIÓN: Se sigue de la siguiente fórmula tomada de [10.2], donde $\left(\frac{a}{b}\right)$ es el símbolo de Jacobi.

$$N_p = 2p + 3 + \left(\frac{-4}{p}\right) + 2\left(\frac{-3}{p}\right).$$

A manera de ejemplo, a continuación se describen las clases de equivalencia de las curvas elípticas sobre el campo $\mathbf{Z}_7$. Para obtener algunos resultados de la siguiente tabla se usó *Mathematica*.

Isomorfismos $E_{a,b}$	No. de Puntos	Grupo
$E_{1,1} \sim E_{4,1} \sim E_{2,1}$	5	$\mathbf{Z}_5$
$E_{1,3} \sim E_{4,3} \sim E_{2,3}$	6	$\mathbf{Z}_6$
$E_{1,4} \sim E_{4,4} \sim E_{2,4}$	10	$\mathbf{Z}_{10}$
$E_{1,6} \sim E_{4,6} \sim E_{2,6}$	11	$\mathbf{Z}_{11}$
$E_{3,1} \sim E_{5,1} \sim E_{6,1}$	12	$\mathbf{Z}_2 \times \mathbf{Z}_6$
$E_{3,2} \sim E_{5,2} \sim E_{6,2}$	9	$\mathbf{Z}_9$
$E_{3,3} \sim E_{5,3} \sim E_{6,3}$	6	$\mathbf{Z}_6$
$E_{3,4} \sim E_{5,4} \sim E_{5,4}$	10	$\mathbf{Z}_{10}$
$E_{3,5} \sim E_{6,5} \sim E_{5,5}$	7	$\mathbf{Z}_7$
$E_{3,6} \sim E_{5,6} \sim E_{6,6}$	4	$\mathbf{Z}_2 \times \mathbf{Z}_2$
$E_{1,0} \sim E_{2,0} \sim E_{4,0}$	8	$\mathbf{Z}_8$
$E_{3,0} \sim E_{5,0} \sim E_{6,0}$	8	$\mathbf{Z}_2 \times \mathbf{Z}_4$
$E_{0,1}$	12	$\mathbf{Z}_2 \times \mathbf{Z}_6$
$E_{0,2}$	9	$\mathbf{Z}_9$
$E_{0,3}$	13	$\mathbf{Z}_{13}$
$E_{0,4}$	3	$\mathbf{Z}_3$
$E_{0,5}$	7	$\mathbf{Z}_7$
$E_{0,6}$	4	$\mathbf{Z}_2 \times \mathbf{Z}_2$

Observemos primero que en efecto, hay 18 clases de equivalencia, de acuerdo a la fórmula $N_p = 2p + 4$ con $p = 7$.

Por ejemplo, para el caso de $E_{3,2}$ y $E_{5,2}$ tenemos $u^2 = 4$, entonces $u_0 = \pm 2$, y por lo tanto, $\varphi : E_{3,2} \to E_{5,2}$ dada por $\varphi(x, y) = (2^2 x, 2^3 y)$ es el cambio de variable. Sabemos que $\#Aut(E) = 2$, así hay 3 curvas equivalentes a $E_{3,2}$; la tercera se obtiene aplicando φ a $E_{5,2}$. El número de puntos racionales, así como el tipo de grupo se calculó directamente con *Mathematica*.

Por último, observemos que las 6 clases del tipo $E_{0,b}$ tienen a $\#Aut(E) = 6$, y las otras 12 clases tienen 2 automorfismos cada una. Luego $6\left(\frac{1}{6}\right) + 12\left(\frac{1}{2}\right) = 7$, de acuerdo con la relación $\sum_E \frac{1}{\#Aut(E)} = p$.

4.2 Implementación

La implementación de un criptosistema de aquí en adelante la entenderemos como el conjunto de elementos físicos "hardware" y lógicos "software" que intervienen en los criptosistemas. Atenderemos particularmente aquéllos que nos proporcionan beneficios como ahorro de memoria, facilidad en la programación, rapidez de encriptamiento y desencriptamiento, rapidez de transmisión, etcétera.

El tipo de criptosistemas basados en curvas elípticas sobre campos finitos, es variado pero en general son similares a el sistema de ElGamal (ver sección 2.5), esto debido a la seguridad que éste proporciona, cosa que estudiaremos en la siguiente sección.

Con objeto de entender algunos procesos en el encriptamiento primeramente nos dedicaremos a describir un ejemplo del sistema de ElGamal análogo al visto con el grupo multiplicativo $\mathbf{F}_q^*$ (2.5).

4.2.1 Esquema de ElGamal

Primeramente consideraremos a una curva elíptica E definida sobre $\mathbf{Z}_p$ y un punto racional $G \in E(\mathbf{Z}_p)$.

Supongamos que el usuario **A** desea enviar el mensaje m al usuario **B**.

Recordemos de 2.5 que el criptosistema de ElGamal sobre un campo finito tiene el siguiente esquema:

$$CpS = \left(A \hookrightarrow \mathbf{F}_q, \left\{c = \left(\alpha^k, m\alpha^{xk}\right)\right\}, \left\{c_1^{(q-1-x)}c_2\right\}\right)$$
$$L = (k, \alpha^x)$$
$$L^{-1} = (x)$$
$$L \not\simeq L^{-1}$$

donde m es el mensaje, k un entero aleatorio, α un elemento del campo $\mathbf{F}_q$, α^x la llave pública y x la llave privada. Entonces la versión de este criptosistema

con el grupo de puntos racionales de una curva elíptica sobre un campo finito es:

$$CpS = (A \hookrightarrow E(\mathbb{Z}_p), \{c = (kG, P_m + kaG)\}, \{c_2 - ac_1\})$$
$$L = (k, aG)$$
$$L^{-1} = (a)$$
$$L \not\approx L^{-1}$$

donde P_m es el mensaje, k igual que antes, el entero a es la llave privada y aG la llave pública.

De esta forma el proceso a seguir, que llamaremos Esquema de Encriptamiento con Curvas Elípticas (**EECE**), tiene los siguientes pasos:

Dada una curva E sobre $\mathbb{Z}_p$ y un punto racional $G \in E(\mathbb{Z}_p)$.

a) Generación de llaves

1) Se elige un número $a \in [1, p-1]$
2) Se calcula el punto $H = aG \in E(\mathbb{Z}_p)$
3) La llave pública es el punto H
4) La llave privada es el número entero a

b) Proceso de encriptamiento

1) El usuario **A** busca la llave pública de **B**
2) Se representa el mensaje m como un punto $P_m = (m_1, m_2) \in E(\mathbb{Z}_p)$
3) Se elige un número entero $k \in [1, p-1]$ aleatoriamente
4) Se calcula el punto $c = (kG, P_m + kH)$
5) Se transmite el punto $c = (c_1, c_2)$

c) Proceso de desencriptamiento

1) El usuario **B** recibe a c
2) Se recobra a P_m con la llave privada a, calculando $c_2 - ac_1$
3) Se obtiene el mensaje m, a partir de P_m

Demos ahora un ejemplo sencillo para entender el proceso anterior.

Considérese la curva $y^2 = x^3 + 5$ sobre el campo $\mathbf{Z}_{37}$. El grupo de puntos racionales $E(\mathbf{Z}_{37})$ es:

$P_1 = (6,6)$	$P_2 = (32,19)$	$P_3 = (27,2)$	$P_4 = (11,2)$	$P_5 = (31,14)$
$P_6 = (21,4)$	$P_7 = (36,35)$	$P_8 = (25,4)$	$P_9 = (22,21)$	$P_{10} = (8,6)$
$P_{11} = (23,31)$	$P_{12} = (35,21)$	$P_{13} = (29,14)$	$P_{14} = (28,33)$	$P_{15} = (24,19)$
$P_{16} = (17,21)$	$P_{17} = (18,18)$	$P_{18} = (14,23)$	$P_{19} = (14,14)$	$P_{20} = (18,19)$
$P_{21} = (17,16)$	$P_{22} = (24,18)$	$P_{23} = (28,4)$	$P_{24} = (29,23)$	$P_{25} = (35,16)$
$P_{26} = (23,6)$	$P_{27} = (8,31)$	$P_{28} = (22,16)$	$P_{29} = (25,33)$	$P_{30} = (36,2)$
$P_{31} = (21,33)$	$P_{32} = (31,23)$	$P_{33} = (11,35)$	$P_{34} = (27,35)$	$P_{35} = (32,18)$
$P_{36} = (6,31)$	$P_{37} = \mathcal{O}$			

En este caso tenemos que $E(\mathbf{Z}_{37})$ es un grupo cíclico de orden 37 con P_1 un generador, por lo tanto $nP_1 = P_n$, $n = 1, 2, ..., 37$.

Supongamos que el usuario **A** desea enviar el mensaje $m =$ "$OTRO\_EJEMPLO$" al usuario **B**. Con $G = P_1$, y el grupo $E(\mathbf{Z}_{37})$, así el proceso es el siguiente:

a) Generación de llaves

1) El usuario **B** selecciona un número entero $a \in [1, 37]$, digamos $\boxed{a = 10}$, que es su llave privada

2) Se calcula el punto $H = 10G = P_{10} = (8,6)$

3) La llave pública es el punto $(8,6)$

4) La llave privada es el número $a = 10$

En el directorio de usuarios tendremos a **B** con su llave pública P_{10}.

Usuario	Llave pública
⋮	⋮
B	$(8,6)$
⋮	⋮

b) Proceso de encriptamiento

1) El usuario **A** toma la llave pública de **B**, es decir, $H = (8, 6)$

2) El encajamiento del mensaje en $E(\mathbb{Z}_{37})$ se toma de la siguiente manera:

$$\begin{array}{cccccccccc} \_ & A & B & \cdots & Y & Z & 0 & 1 & \cdots & 9 \\ \updownarrow & \updownarrow & \updownarrow & \cdots & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \cdots & \updownarrow \\ 1 & 2 & 3 & \cdots & 26 & 27 & 28 & 29 & \cdots & 37 \\ \updownarrow & \updownarrow & \updownarrow & \cdots & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \cdots & \updownarrow \\ P_1 & P_2 & P_3 & \cdots & P_{26} & P_{27} & P_{28} & P_{29} & \cdots & P_{37} \end{array}$$

Así el mensaje a enviar queda como:

$$\begin{array}{cccccccccccc} O & T & R & O & \_ & E & J & E & M & P & L & O \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ P_{16} & P_{21} & P_{19} & P_{16} & P_1 & P_6 & P_{11} & P_6 & P_{14} & P_{17} & P_{13} & P_{16} \end{array}$$

3), 4) El encriptamiento para cada caracter se lleva a cabo de la siguiente manera, de acuerdo al proceso antes descrito.

$$\begin{array}{llcllcll} k = 2 & O & \mapsto & (2G, P_{16} + 2P_{10}) & = & (P_2, P_{36}) & \hookrightarrow & (A, 8) \\ k = 13 & T & \mapsto & (13G, P_{21} + 13P_{10}) & = & (P_{13}, P_3) & \hookrightarrow & (L, B) \\ k = 21 & R & \mapsto & (21G, P_{19} + 21P_{10}) & = & (P_{21}, P_7) & \hookrightarrow & (T, F) \\ k = 9 & O & \mapsto & (9G, P_{16} + 9P_{10}) & = & (P_9, P_{32}) & \hookrightarrow & (H, 4) \\ k = 31 & \_ & \mapsto & (31G, P_1 + 31P_{10}) & = & (P_{31}, P_{15}) & \hookrightarrow & (3, N) \\ k = 23 & E & \mapsto & (23G, P_6 + 23P_{10}) & = & (P_{23}, P_{14}) & \hookrightarrow & (V, M) \\ k = 17 & J & \mapsto & (17G, P_{11} + 17P_{10}) & = & (P_{17}, P_{33}) & \hookrightarrow & (P, 5) \\ k = 29 & E & \mapsto & (29G, P_6 + 29P_{10}) & = & (P_{29}, P_{37}) & \hookrightarrow & (1, \_) \\ k = 10 & M & \mapsto & (10G, P_{14} + 10P_{10}) & = & (P_{10}, P_3) & \hookrightarrow & (I, B) \\ k = 27 & P & \mapsto & (27G, P_{17} + 27P_{10}) & = & (P_{27}, P_{28}) & \hookrightarrow & (Z, 0) \\ k = 5 & L & \mapsto & (5G, P_{13} + 5P_{10}) & = & (P_5, P_{26}) & \hookrightarrow & (D, Y) \\ k = 23 & O & \mapsto & (23G, P_{16} + 23P_{10}) & = & (P_{23}, P_{24}) & \hookrightarrow & (V, W) \end{array}$$

5) Finalmente se transmite el mensaje

$$m = \text{"}A8LBTFH43NVMP51\_IBZ0DYVW\text{"}$$

c) Proceso de desencriptamiento

1), 2), 3) Para recuperar el mensaje, el usuario **B** aplica la función de desencriptamiento $c_2 - ac_1$, haciendo uso de su llave privada $\boxed{a = 10}$.

De la siguiente forma:

$$\begin{array}{lllllll}
(A,8) & \mapsto & P_{36} - 10P_2 & = & P_{16} & \hookrightarrow & O \\
(L,B) & \mapsto & P_3 - 10P_{13} & = & P_{21} & \hookrightarrow & T \\
(T,F) & \mapsto & P_7 - 10P_{21} & = & P_{19} & \hookrightarrow & R \\
(H,4) & \mapsto & P_{32} - 10P_9 & = & P_{16} & \hookrightarrow & O \\
(3,N) & \mapsto & P_{15} - 10P_{31} & = & P_1 & \hookrightarrow & - \\
(V,M) & \mapsto & P_{14} - 10P_{23} & = & P_6 & \hookrightarrow & E \\
(P,5) & \mapsto & P_{33} - 10P_{17} & = & P_{11} & \hookrightarrow & J \\
(1,_) & \mapsto & 0P_1 - 10P_{29} & = & P_6 & \hookrightarrow & E \\
(I,B) & \mapsto & P_3 - 10P_{10} & = & P_{14} & \hookrightarrow & M \\
(Z,0) & \mapsto & P_{28} - 10P_{27} & = & P_{17} & \hookrightarrow & P \\
(D,Y) & \mapsto & P_{26} - 10P_5 & = & P_{13} & \hookrightarrow & L \\
(V,W) & \mapsto & P_{24} - 10P_{23} & = & P_{16} & \hookrightarrow & O
\end{array}$$

obteniendo así el mensaje original.

Este ejemplo ilustra el funcionamiento del sistema de ElGamal con curvas elípticas definidas sobre un campo $\mathbf{Z}_p$.

4.2.2 Aspectos generales en la implementación

En esta subsección comentaremos algunos aspectos, en lo que se refiere a la implementación del **EECE**.

a) Operaciones sobre $E(\mathbf{Z}_p)$

Al considerar la curva elíptica sobre un campo finito K de característica p mayor a 3.

$$y^2 = x^3 + ax + b$$

donde $4a^3+27b^2 \neq 0$, conjuntamente con el punto al infinito $\mathcal{O}$; de 3.2 vemos que las operaciones de grupo son las siguientes:

Si $P=(x_1,y_1)$, $Q=(x_2,y_2)$ con $P \neq \pm Q$, tenemos que $P+Q=(x_3,y_3)$ donde

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2, \\ y_3 &= \lambda(x_1 - x_3) - y_1, \ \lambda = \frac{y_2 - y_1}{x_2 - x_1} \end{aligned}$$

y si $P=Q$, entonces

$$\begin{aligned} x_3 &= \lambda^2 - 2x_1, \\ y_3 &= \lambda(x_1 - x_3) - y_1, \ \lambda = \frac{3x_1^2 + a}{2y_1}. \end{aligned}$$

Observemos que en el primer caso, la suma de puntos racionales se lleva a cabo efectuando 2 multiplicaciones y una división. Asumiendo que la suma, la resta y la multiplicación por un escalar en el campo, no consumen tiempo, éstas no serán consideradas; mientras que en el segundo caso se requieren 3 multiplicaciones y una división en K.

Los algoritmos existentes (véase [4]), aún consumen mucho más tiempo en la división que en la multiplicación sobre un campo finito, por lo que es preferible tener que efectuar multiplicaciones que divisiones. Por esta razón se opta por realizar las operaciones tomando las coordenadas proyectivas.

A partir de las fórmulas anteriores y considerando los puntos $(x_1', y_1', 1) = \left(\frac{X_1}{Z_1}, \frac{Y_1}{Z_1}, 1\right)$ y $(x_2', y_2', 1) = \left(\frac{X_2}{Z_2}, \frac{Y_2}{Z_2}, 1\right)$, para x_3' la primera coordenada de $P+Q$ es

$$x_3' = \frac{\left(\frac{Y_2}{Z_2} - \frac{Y_1}{Z_1}\right)^2}{\left(\frac{X_2}{Z_2} - \frac{X_1}{Z_1}\right)^2} - \frac{X_1}{Z_1} - \frac{X_2}{Z_2}$$

haciendo $X_3 = Z_3 x_3'$ con $Z_3 = (X_2Z_1 - X_1Z_2)^3 Z_1 Z_2$ para poder eliminar el denominador de x_3' y de y_3'.

Finalmente tenemos que $X_3 = vA$, con $v = X_2Z_1 - X_1Z_2$ y $A = u^2 Z_1 Z_2 - v^2(X_2Z_1 + X_1Z_2)$ con $u = Y_2Z_1 - Y_1Z_2$.

De forma similar se procede para obtener Y_3, Z_3, quedando de la siguiente manera:

Si $P = (X_1, Y_1, Z_1)$, $Q = (X_2, Y_2, Z_2)$ con $P \neq \pm Q$, entonces $P + Q = (X_3, Y_3, Z_3)$ donde

$$\begin{aligned} X_3 &= vA, \\ Y_3 &= u\left(v^2 X_1 Z_2 - A\right) - v^3 Y_1 Z_2, \\ Z_3 &= v^3 Z_1 Z_2. \end{aligned}$$

Para el caso donde $P = Q$ se tiene

$$\begin{aligned} X_3 &= 2hs, \\ Y_3 &= w(4B - h) - 8Y_1^2 s^2, \\ Z_3 &= 8s^3, \end{aligned}$$

donde $w = aZ_1^2 + 3X_1^2$, $s = Y_1 Z_1$, $B = X_1 Y_1 s$, y $h = w^2 - 8B$.

De esta forma se elimina la división, teniendo ahora 12 multiplicaciones para ambos casos, al hacer $Z_1 = 1$.

Como conclusión, podemos decir que las operaciones deben de realizarse en coordenadas proyectivas para obtener más rapidez en un criptosistema.

b) Encajamiento en $E(\mathbf{Z}_p)$

En seguida veamos aspectos en el proceso de encajar un texto ordinario en el conjunto de puntos racionales de una curva elíptica $\mathcal{A} \hookrightarrow E(\mathbf{Z}_p)$. Lo que debe de realizarse usando una función invertible f, del alfabeto $\mathcal{A}$ al conjunto de puntos racionales que sea de fácil implementación.

Sea $M = (m_1, m_2, ..., m_k) \in \mathcal{N}^k$, un mensaje. Una forma de encajar a M en $E(\mathbf{Z}_p)$, es decir, encontrar un punto $P_{m_i} = (x_{m_i}, y_{m_i})$ asociado a cada m_i es relacionando a $m = m_i$ un punto $x_m \in \mathbf{Z}_p$; y al evaluar a $x_m^3 + ax_m + b = z$, tomamos a y_m como $\sqrt{z}$, si no existe y_m, repetimos el proceso.

Un algoritmo para este proceso es el siguiente ([5.1]):

i) Sea k un entero tal que $30 \leq k \leq 50$; como lo sugiere la práctica, y $\mathbf{Z}_p$ un campo con p elementos, tal que $p > Nk$, donde N es un entero fijo tal que $N > m$. Escribimos ahora a $l = mk + j$, $j = 0, 1, 2, \ldots, k-1$; entonces, $1 \leq mk + j < (N-1)k + k = Nk$ por lo tanto, existe una función uno a uno de los enteros l en $\mathbf{Z}_p$.

ii) Para cada m, al variar j tenemos k números l, hacemos $x_m = l$, calculamos a $x_m^3 + ax_m + b = z$. Si z tiene raíz cuadrada, entonces paramos, de lo contrario avanzamos a $j + 1$.

iii) Al encontrar $y_m = \sqrt{z}$, se identifica $m \mapsto P_m = (x_m, y_m)$.

El éxito del algoritmo anterior se debe al siguiente lema.

LEMA 4.2.2.1: Dado un entero $m > 0$; la probabilidad de no encontrar el punto P_m de la curva elíptica es $\frac{1}{2^k}$.

DEMOSTRACIÓN: Cada elemento de $\mathbf{Z}_p$ tiene probabilidad de $\frac{1}{2}$ de tener raíz cuadrada. Por otro lado, la elección de cada $x_m \in \mathbf{Z}_p$ es independiente; entonces, si A_j es el evento "no se encontró un cuadrado a $z = x_m^3 + ax_m + b$ en l_j", tenemos que la probabilidad de no encontrar el punto P_m correspondiente a m es $P(A_1 \cap \ldots \cap A_k) = \prod_{j=1}^{k} P(A_j) = \frac{1}{2^k}$.

Veamos un ejemplo del algoritmo anterior:

Sea $k = 30$, $N = 30$, para poder usar un alfabeto de almenos 26 caracteres, además como $p > kN$ es necesario usar un campo finito $\mathbb{Z}_p$ con $p > 900$, tomemos a $\mathbb{Z}_{907}$, así:

$m = 0$	1	2	$\cdots$	30	j
$m = 1$	31	32	$\cdots$	60	$k + j$
$m = 2$	61	62	$\cdots$	90	$2k + j$
	$\vdots$	$\vdots$		$\vdots$	$\vdots$
$m = M - 1$	$(M-1)k + 1$	$(M-1)k + 2$	$\cdots$	kM	$(M-1)k + j$

Considerando al alfabeto $\mathcal{A} = \{A, B, C, \ldots, Z\}$ y la curva elíptica $E : y^2 = x^3 + x + 1$, y sea $f(x) = x^3 + x + 1$ el algoritmo queda de la siguiente manera:

i) Para identificar a la letra A con un punto racional de la curva, tomemos a $j = 1, m = 0$, entonces $x_A = l = 1$. Como $f(1) = 3$ y éste no tiene raíz cuadrada en $\mathbb{Z}_{907}$ se toma $m = 1$; así $x_A = l = 31$. Como $f(31) = 799$, y su raíz cuadrada es 79, entonces $P_A = (31, 79)$.

ii) El mismo argumento para B : si $j = 2, m = 0$, entonces $x_B = l = 2$, como $f(2) = 11$ no tiene raíz en $\mathbb{Z}_{907}$, seguimos con $m = 1$ y en este caso tenemos que $P_B = (32, 326)$, etcétera.

El siguiente paso es "desencajar" el mensaje, es decir, obtener a m a partir de P_m. Como $x_m \in \mathbb{Z}_p$, entonces $m = \frac{x_m - j}{k}$.

4.3 Seguridad

Para terminar este capítulo, comentaremos algunos aspectos referente a la seguridad de los sistemas que usan curvas elípticas sobre el campo finito $\mathbb{Z}_p$.

Hasta la fecha los sistemas elípticos que se han propuesto, desde N. Koblitz ([7.2]) y V. Miller ([7.3]) basan su seguridad en el Problema del Logaritmo Discreto Elíptico (PLDE), es decir, el PLD sobre el grupo de puntos racionales de una curva elíptica sobre un campo finito $\mathbb{F}_q$, en lugar del grupo $\mathbb{F}_p^*$.

En este caso elíptico, el PLD toma la siguiente forma:

Dados $P, Q \in E(\mathbb{Z}_p)$, entonces, el PLDE es determinar un número entero s tal que $sP = Q$.

Para resolver el PLDE, existen hasta el momento dos alternativas, la primera es aplicar el algoritmo general ([7.1], método de la raíz cuadrada), que se aplica a cualquier grupo. Sin embargo, éste consume mucho tiempo si el orden del grupo tiene un factor de al menos 45 dígitos. La otra alternativa es intentar aplicar el algoritmo conocido como MOV (Menezes, Okamoto y Vanstone [7.9]), el cual reduce el PLDE sobre el grupo de puntos racionales de una curva elíptica definida sobre un campo finito K al PLD sobre una extensión K^s del campo K. Este método hace uso del mapeo de Weil, definido sobre el subgrupo de torsión $E[m]$ (los elementos de orden m). Se comentará más de este método en el siguiente capítulo.

Como el mapeo de Weil se define si m es primo relativo a p, donde m es el orden de los puntos de $E(\mathbb{Z}_p)$ ([7.9]), no se puede aplicar este método MOV en el caso de $p = \#(E(\mathbb{Z}_p))$, este tipo de curva fueron propuestas por Miyaji. Sin embargo, recientemente se ha descubierto por Smart, Satoh y Araki una técnica que desecha por completo a este tipo de curvas. En conclusión podemos afirmar que el sistema es confiable sólo si $\#(E(\mathbb{Z}_p))$ tiene un factor primo de por lo menos 45 dígitos.

Capítulo 5

Criptosistemas Elípticos

Introducción: En este capítulo describimos criptosistemas análogos al de ElGamal, usando el grupo de puntos racionales de una curva elíptica E, definida sobre un campo finito de característica 2.

En los últimos años se ha demostrado que los criptosistemas que usan curvas elípticas (CCE), pueden ser usados eficientemente tanto en la transmisión de información confidencial, en la distribución de llaves de un sistema de llave privada como en la utilización de firmas digitales. En este tipo de procesos los CCE ofrecen grandes ventajas a diferencia de otro tipo de sistemas. Por ejemplo, donde el poder de cómputo es limitado, donde se requiere una gran velocidad de transmisión, donde el requerimiento de firmas es muy frecuente, etcétera. Esto es debido principalmente a la gran seguridad que los CCE ofrecen, así como a la complejidad de las operaciones que dotan a una curva elíptica de estructura de grupo; lo que permite el uso de llaves de longitud menor respecto a sistemas que usan sólo las operaciones del campo finito.

El orden que tomaremos en este capítulo es el siguiente: los aspectos más relevantes sobre la representación de los elementos de un campo finito $\mathbb{F}_{2^n}$, los veremos en 5.1, lo que nos permitirá realizar óptimamente las operaciones en $E(\mathbb{F}_{2^n})$; en 5.2 argumentamos el por qué el uso de curvas elípticas supersingulares arriesga la seguridad, en otras palabras damos a conocer un algoritmo subexponencial que resuelve el problema del logaritmo discreto elíptico (PLDE), por lo tanto, deducimos que las mejores curvas para diseñar sistemas criptográficos son las no supersingulares, éstas las estudiamos en 5.3; en 5.4 describimos los pasos en que consiste un sistema elíptico; finalmente en 5.5 mencionamos algunas tendencias que tiene el estudio de sistemas criptográficos elípticos.

5.1 Representación de los elementos de $\mathbb{F}_{2^n}$

La implementación de un criptosistema depende en gran parte de la rapidez con que se efectúen los procesos de encriptamiento y desencriptamiento. Estos procesos se realizan efectuando operaciones sobre el grupo en consideración; en nuestro caso, las operaciones entre los puntos racionales de $E(\mathbb{F}_{2^n})$, éstos a la vez se reducen a efectuar operaciones sobre el campo finito $\mathbb{F}_{2^n}$. La gran cantidad de operaciones que son necesarias al usar CCE requieren tanto que el "hardware" como el "software" sean eficientes al efectuar las operaciones en $E(\mathbb{F}_{2^n})$, lo que nos lleva a buscar la mejor representación de los elementos del campo finito $\mathbb{F}_{2^n}$ para realizar eficientemente tales operaciones.

5.1.1 Bases polinomiales en $\mathbb{F}_{2^n}$

Al considerar a $\mathbb{F}_{2^n}$ como espacio vectorial sobre $\mathbb{F}_2$, cada elemento $\alpha \in \mathbb{F}_{2^n}$, se puede escribir de la forma $\alpha = c_1a_1 + c_2a_2 + \cdots + c_na_n$, donde $c_i \in \mathbb{F}_2$ y $\{a_1, a_2, ..., a_n\}$ es una base. Del teorema 1.1.2 se sigue que $a_i = \alpha^i$ para $0 \leq i \leq n-1$, con α una raíz de un polinomio irreducible $p(x)$ de grado n en $\mathbb{F}_2[x]$. A este tipo de base se le conoce como base polinomial. En los ejemplos de 1.1 los campos $\mathbb{F}_4$, $\mathbb{F}_8$ se construyeron usando bases polinomiales.

Este tipo de base permite ver a los elementos de $\mathbb{F}_{2^n}$ como polinomios, de tal forma que las operaciones que se realizan se reducen a operaciones de polinomios módulo un polinomio irreducible $p(x)$. Existen varios métodos, para realizar operaciones usando este tipo de bases (véase [4]). La velocidad, en este caso, depende mucho de la forma del polinomio irreducible $p(x)$, por lo que una buena base polinomial para realizar operaciones sobre $\mathbb{F}_{2^n}$ es aquélla generada por un polinomio irreducible con el menor número de términos posible, por ejemplo, en [2.16], [2.17], [2.18] y [2.19] podemos encontrar trinomios irreducibles en $\mathbb{F}_2[x]$.

5.1.2 Bases normales óptimas

En esta sección describimos el tipo de bases más popular, utilizado para efectuar operaciones en $\mathbb{F}_{2^n}$ las bases normales, y como un caso especial, obtendremos a las bases normales óptimas.

Considérese el campo finito $\mathbb{F}_{p^n}$, de característica p un número primo y $N = \left\{\beta, \beta^p, \beta^{p^2}, ..., \beta^{p^{n-1}}\right\}$ una base normal de $\mathbb{F}_{p^n}$ sobre $\mathbb{F}_p$.

Por ejemplo, una base normal de $\mathbb{F}_{2^n}$ sobre $\mathbb{F}_2$ es un conjunto de la forma

$$N = \left\{\beta, \beta^2, \beta^{2^2}, ..., \beta^{2^{n-1}}\right\}$$

$\beta \in \mathbb{F}_{2^n}$, cada elemento α de $\mathbb{F}_{2^n}$ se puede escribir como $\alpha = \sum_{i=0}^{n-1} a_i \beta^{2^i}$, con $a_i \in \{0, 1\}$, en forma vectorial $\alpha = (a_0, a_1, ..., a_{n-1})$; en la literatura de computación es común usar la representación $(a_{n-1}, a_{n-2}, ..., a_0)$ para α.

Son varios aspectos los que hacen a las bases normales más eficientes al efectuar operaciones entre los elementos de un campo finito $\mathbb{F}_{2^n}$.

La operación "suma", en el campo finito $\mathbb{F}_{2^n}$, es la más simple de realizar y se lleva a cabo mediante la función "*xor*", definida como:

$$\begin{aligned} 1 \; xor \; 0 &= 1 \\ 1 \; xor \; 1 &= 0 \end{aligned}$$

La siguiente operación que analizaremos, y una de las más importantes, es el "producto". De su análisis obtendremos la definición de una base normal óptima (BNO).

En general, sean A, B elementos de $\mathbb{F}_{p^n}$

$$A = \sum_{i=0}^{n-1} a_i \beta^{p^i}, \quad B = \sum_{j=0}^{n-1} b_j \beta^{p^j} \;\; 0 \leq a_i, b_j \leq p-1$$

entonces, el producto es:

$$A \cdot B = C = \sum_{i=0}^{n-1} c_i \beta^{p^i}$$

Haciendo las sustituciones, tenemos

$$C = \left(\sum_{i=0}^{n-1} a_i \beta^{p^i}\right)\left(\sum_{j=0}^{n-1} b_j \beta^{p^j}\right) = \left(\sum_{i=0}^{n-1}\left(\sum_{j=0}^{n-1} a_i b_j \beta^{p^i}\beta^{p^j}\right)\right)$$

puesto que N es una base, entonces también cada elemento $\beta^{p^i}\beta^{p^j}$ se puede escribir como:

$$\beta^{p^i}\beta^{p^j} = \sum_{k=0}^{n-1} d_{ij}^{(k)} \beta^{p^k}, \quad d_{ij}^{(k)} \in \mathbb{F}_p.$$

comparando coeficientes tenemos que

$$c_k = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} d_{ij}^{(k)} a_i b_j.$$

Estas fórmulas se obtienen asociando términos, como en el siguiente ejemplo para $n = 3$.

$$\begin{aligned} A &= a_0\beta^{p^0} + a_1\beta^{p^1} + a_2\beta^{p^2} \\ B &= b_0\beta^{p^0} + b_1\beta^{p^1} + b_2\beta^{p^2} \end{aligned}$$

el producto es:

$$\begin{aligned} AB = \; & a_0b_0\beta^{p^0}\beta^{p^0} + a_0b_1\beta^{p^0}\beta^{p^1} + a_0b_2\beta^{p^0}\beta^{p^2} + \\ & a_1b_0\beta^{p^1}\beta^{p^0} + a_1b_1\beta^{p^1}\beta^{p^1} + a_1b_2\beta^{p^1}\beta^{p^2} + \\ & a_2b_0\beta^{p^2}\beta^{p^0} + a_2b_1\beta^{p^2}\beta^{p^1} + a_2b_2\beta^{p^2}\beta^{p^2} \\ & = \sum_{i=0}^{2}\left(\sum_{j=0}^{2} a_ib_j\beta^{p^i}\beta^{p^j}\right) \end{aligned}$$

por otro lado $\beta^{p^i}\beta^{p^j} = \sum_{k=0}^{2} d_{ij}^{(k)}\beta^{p^k}$, que al sustituir tenemos

$$\begin{aligned} AB = \quad & a_0b_0\left(d_{00}^{(0)}\beta^{p^0} + d_{00}^{(1)}\beta^{p^1} + d_{00}^{(2)}\beta^{p^2}\right) \\ & +a_0b_1\left(d_{01}^{(0)}\beta^{p^0} + d_{01}^{(1)}\beta^{p^1} + d_{01}^{(2)}\beta^{p^2}\right) \\ & +a_0b_2\left(d_{02}^{(0)}\beta^{p^0} + d_{02}^{(1)}\beta^{p^1} + d_{02}^{(2)}\beta^{p^2}\right) \\ & +a_1b_0\left(d_{10}^{(0)}\beta^{p^0} + d_{10}^{(1)}\beta^{p^1} + d_{10}^{(2)}\beta^{p^2}\right) \\ & +a_1b_1\left(d_{11}^{(0)}\beta^{p^0} + d_{11}^{(1)}\beta^{p^1} + d_{11}^{(2)}\beta^{p^2}\right) \\ & +a_1b_2\left(d_{12}^{(0)}\beta^{p^0} + d_{12}^{(1)}\beta^{p^1} + d_{12}^{(2)}\beta^{p^2}\right) \\ & +a_2b_0\left(d_{20}^{(0)}\beta^{p^0} + d_{20}^{(1)}\beta^{p^1} + d_{20}^{(2)}\beta^{p^2}\right) \\ & +a_2b_1\left(d_{21}^{(0)}\beta^{p^0} + d_{21}^{(1)}\beta^{p^1} + d_{21}^{(2)}\beta^{p^2}\right) \\ & +a_2b_2\left(d_{22}^{(0)}\beta^{p^0} + d_{22}^{(1)}\beta^{p^1} + d_{22}^{(2)}\beta^{p^2}\right) \end{aligned}$$

donde podemos ver que agrupando términos, se obtiene la fórmula requerida

$$A \cdot B = \left(\sum_{i=0}^{2}\sum_{j=0}^{2} a_i b_j d_{ij}^{(0)}\right)\beta^{p^0} + \left(\sum_{i=0}^{2}\sum_{j=0}^{2} a_i b_j d_{ij}^{(1)}\right)\beta^{p^1} + \left(\sum_{i=0}^{2}\sum_{j=0}^{2} a_i b_j d_{ij}^{(2)}\right)\beta^{p^2}$$

Definimos ahora la matriz $T_i = (d_{ij}^{(k)})$, $0 \leq j,k \leq n-1$, entonces al conjunto de matrices T_i, $0 \leq i \leq n-1$ le llamaremos la tabla de multiplicación de $\mathbb{F}_{p^n}$ sobre $\mathbb{F}_p$ para la base N. Por ejemplo, en el caso anterior

$$T_0 = \begin{pmatrix} d_{00}^{(0)} & d_{00}^{(1)} & d_{00}^{(2)} \\ d_{01}^{(0)} & d_{01}^{(1)} & d_{01}^{(2)} \\ d_{02}^{(0)} & d_{02}^{(1)} & d_{02}^{(2)} \end{pmatrix}$$

$$T_1 = \begin{pmatrix} d_{10}^{(0)} & d_{10}^{(1)} & d_{10}^{(2)} \\ d_{11}^{(0)} & d_{11}^{(1)} & d_{11}^{(2)} \\ d_{12}^{(0)} & d_{12}^{(1)} & d_{12}^{(2)} \end{pmatrix}$$

$$T_2 = \begin{pmatrix} d_{20}^{(0)} & d_{20}^{(1)} & d_{20}^{(2)} \\ d_{21}^{(0)} & d_{21}^{(1)} & d_{21}^{(2)} \\ d_{22}^{(0)} & d_{22}^{(1)} & d_{22}^{(2)} \end{pmatrix}$$

La tabla de multiplicación T_N es entonces $\begin{pmatrix} T_0 \\ T_1 \\ \vdots \\ T_{n-1} \end{pmatrix}$; observemos que las

matrices T_i son independientes de los elementos A, B y dependen sólo de la base, por lo que, para efectuar la operación de multiplicación entre A y B, debemos de diseñar algoritmos o circuitos que den como salida las anteriores n matrices, que vienen siendo las componentes de C.

Antes de definir una base normal óptima observemos lo siguiente.

Si el elemento C del ejemplo anterior se pudiera escribir de la forma:

$$\begin{aligned} c_0 &= (a_0b_0 + a_0b_1 + a_0b_2 + a_1b_0 + a_1b_1 + a_1b_2 + a_2b_0 + a_2b_1 + a_2b_2) \\ c_1 &= (a_1b_1 + a_1b_2 + a_1b_0 + a_2b_1 + a_2b_2 + a_2b_0 + a_0b_1 + a_0b_2 + a_0b_0) \\ c_2 &= (a_2b_2 + a_2b_0 + a_2b_1 + a_0b_2 + a_0b_0 + a_0b_1 + a_1b_2 + a_1b_0 + a_1b_1) \end{aligned}$$

entonces, bastaría diseñar un algoritmo que calcule c_0, ya que los subíndices de c_k, se obtienen de los subíndices c_0 sumándoles k módulo n.

Considérese

$$\beta^{p^i}\beta^{p^j} = \sum_{k=0}^{n-1} d_{ij}^{(k)}\beta^{p^k}$$

elevando esta ecuación a la potencia p^{-l}, obtenemos por un lado

$$\beta^{p^{i-l}}\beta^{p^{j-l}} = \sum_{k=0}^{n-1} d_{ij}^{(k)}\beta^{p^{k-l}}$$

y por el otro al sustituir la potencia

$$\beta^{p^{i-l}}\beta^{p^{j-l}} = \sum_{k=0}^{n-1} d_{i-l,j-l}^{(k)}\beta^{p^k}$$

de tal manera, igualando los coeficientes de β^{p^0} en ambas expresiones, obtenemos:

$$d_{ij}^{(l)} = d_{i-l,j-l}^{(0)}. \qquad 0 \leq i, j, l \leq n-1.$$

Esta igualdad nos dice que hay una relación entre cada columna de T_N y los elementos de la matriz T_0 realmente son los mismos elementos reordenados.

Además nos permite re-escribir la fórmula para c_k, de la siguiente manera:

$$\begin{aligned} c_k &= \sum_{i=0}^{n-1}\sum_{j=0}^{m-1} a_i b_j d^{(0)}_{i-k,j-k} \\ &= \sum_{i=0}^{n-1}\sum_{j=0}^{m-1} a_{i+k} b_{j+k} d^{(0)}_{ij} \end{aligned}$$

Es decir, basta trabajar con c_0, para obtener el producto total de A y B.

Definimos entonces la *complejidad* C_N de una base normal N como el número de elementos $d^{(k)}_{0j}$ diferentes de cero de la matriz T_0.

Sea ahora c^k, el conjunto de elementos de la matriz $T_N = \left(d^{(k)}_{ij}\right)$ $0 \leq i, j \leq n-1$, que se encuentran en la k-ésima columna, entonces la colección de columnas $\left\{c^k\right\}$, forman también la tabla de multiplicación de $\mathbb{F}_{p^n}$ sobre $\mathbb{F}_p$ para la base N.

Como C_N es también el número de elementos $d^{(0)}_{ij}$, entonces $C_N = |c^0|$.

Las definiciones anteriores nos dicen que el producto de los elementos A, B depende de la complejidad C_N de la base normal N. Entonces el problema es ahora encontrar la base de $\mathbb{F}_{2^n}$ sobre $\mathbb{F}_2$ con la menor complejidad. Es decir una base normal donde T_0 tenga el número mínimo de elementos diferentes de cero. Obviamente $C_N \leq n^2$. El siguiente resultado demuestra que existe una cota inferior para C_N que depende de n la cual es $2n-1$.

TEOREMA 5.1.2.1: Si N es una base normal para $\mathbb{F}_{p^n}$, entonces $C_N \geq 2n-1$.

DEMOSTRACIÓN: Sea $N = \left\{\beta, \beta^p, \beta^{p^2}, \ldots, \beta^{p^{n-1}}\right\}$ y $b = tr(\beta)$; entonces $\beta^{p^0} b = \sum_{i=0}^{n-1} \beta^{p^0}\beta^{p^i} = \sum_{i=0}^{n-1}\left(d^{(0)}_{0i}\beta^{p^0} + d^{(1)}_{0i}\beta^{p^1} + \cdots + d^{(k)}_{0i}\beta^{p^k}\right)$; comparando coeficientes tenemos que, la suma de los renglones de la matriz T_0, es una n-núpla de la forma $(b, 0, \ldots, 0)$; por lo tanto, cada columna de T_0 contiene al menos 2 elementos no cero, con la posible excepción de la primera columna. Como el conjunto $\left\{\beta^{p^0}\beta^{p^i} \mid 0 \leq i \leq n-1\right\}$ el *l.i.*, entonces el total

de elementos no cero en T_0 es al menos $2(n-1)+1 = 2n-1$, es decir, $C_N \geq 2n-1$.

DEFINICIÓN 5.1.2.2: Se dice que una base normal N de $\mathbb{F}_{p^n}$ sobre $\mathbb{F}_p$ es óptima si $C_N = 2n-1$.

Veamos algunos ejemplos.

i) Para el campo $\mathbb{F}_{2^3} = \{0, 1, \alpha, \alpha^2, 1+\alpha, 1+\alpha^2, \alpha+\alpha^2, 1+\alpha+\alpha^2\}$, con la relación $\alpha^3 = \alpha + 1$. Primero observamos que los polinomios $x^n - 1$ y $\beta x^{n-1} + \beta^2 x^{n-2} + \cdots + \beta^{2^{n-1}}$, $\beta \in \mathbb{F}_{2^n}$ del teorema 1.2.6 son primos relativos, si $tr(\beta) \neq 0$ y al usar que $tr(\beta) = tr(\beta^2)$ podemos obtener un generador β de una base normal. En este caso, con $\beta = \alpha^3$ obtenemos $N = \left\{\beta, \beta^2, \beta^{2^2}\right\} = \{1+\alpha, 1+\alpha^2, 1+\alpha+\alpha^2\}$ una base normal. Entonces todos los elementos del campo se pueden representar como combinación lineal de N.

		β	β^2	β^{2^2}
$\alpha^0 =$	$1 =$	1	1	1
$\alpha^1 =$	$\alpha =$	0	1	1
$\alpha^2 =$	$\alpha^2 =$	1	0	1
$\alpha^3 =$	$1+\alpha =$	1	0	0
$\alpha^4 =$	$\alpha+\alpha^2 =$	1	1	0
$\alpha^5 =$	$1+\alpha+\alpha^2 =$	0	0	1
$\alpha^6 =$	$1+\alpha^2 =$	0	1	0

La matriz T_N queda de la siguiente forma:

	$k=0$	$k=1$	$k=2$
$\beta^{p^0}\beta^{p^0} =$	0	1	0
$\beta^{p^0}\beta^{p^1} =$	1	0	1
$\beta^{p^0}\beta^{p^2} =$	0	1	1
$\beta^{p^1}\beta^{p^0} =$	1	0	1
$\beta^{p^1}\beta^{p^1} =$	0	0	1
$\beta^{p^1}\beta^{p^2} =$	1	1	0
$\beta^{p^2}\beta^{p^0} =$	0	1	1
$\beta^{p^2}\beta^{p^1} =$	1	1	0
$\beta^{p^2}\beta^{p^2} =$	1	0	0

Por lo que tenemos $C_N = 5$, es decir, la base es óptima.

ii) Ahora para el campo $\mathbb{F}_{2^4}$ los elementos son: $\alpha^0 = (1000)$, $\alpha^1 = (0100)$, $\alpha^2 = (0010)$, $\alpha^3 = (0001)$, $\alpha^4 = (1100)$, $\alpha^5 = (0110)$, $\alpha^6 = (0011)$, $\alpha^7 = (1101)$, $\alpha^8 = (1010)$, $\alpha^9 = (0101)$, $\alpha^{10} = (1110)$, $\alpha^{11} = (0111)$, $\alpha^{12} = (1111)$, $\alpha^{13} = (1011)$, $\alpha^{14} = (1001)$. Con $\alpha^4 = \alpha + 1$.

Como en el ejemplo anterior, al calcular las trazas de estos elementos vemos que si $\beta = \alpha^3$ ó $\beta = \alpha^7$, entonces β genera una base normal.

Para el primer caso, $\beta = \alpha^3$ la matriz T_0 queda de la siguiente manera:

$$\begin{array}{rcccc} & 0 & 1 & 2 & 3 \\ \beta^{2^0}\beta^{2^0} = & 0 & 1 & 0 & 0 \\ \beta^{2^0}\beta^{2^1} = & 0 & 0 & 0 & 1 \\ \beta^{2^0}\beta^{2^2} = & 0 & 0 & 1 & 0 \\ \beta^{2^0}\beta^{2^3} = & 1 & 1 & 1 & 1 \end{array}$$

Por lo tanto $C_N = 7$, es decir, la base es óptima.

Sin embargo, para $\beta = \alpha^7$ T_0 es:

$$\begin{array}{rcccc} & 0 & 1 & 2 & 3 \\ \beta^{2^0}\beta^{2^0} = & 0 & 1 & 0 & 0 \\ \beta^{2^0}\beta^{2^1} = & 1 & 1 & 0 & 1 \\ \beta^{2^0}\beta^{2^2} = & 1 & 0 & 1 & 0 \\ \beta^{2^0}\beta^{2^3} = & 1 & 0 & 1 & 1 \end{array}$$

donde $C_N = 9$.

Los ejemplos anteriores motivan a preguntar si siempre existe una base normal óptima. En los siguientes resultados damos respuesta a tal pregunta.

TEOREMA 5.1.2.3: Supóngase que $\mathbb{F}_{p^n}$ contiene $n + 1$ raíces de la unidad. Si las n raíces diferentes de 1 son linealmente independientes entonces $\mathbb{F}_{p^n}$ contiene una base normal óptima.

DEMOSTRACIÓN: Sea β una raíz de la unidad y sea $N = \left\{\beta, \beta^p, \ldots, \beta^{p^{n-1}}\right\}$, N es linealmente independiente, por lo tanto N es una base normal. Además N es el conjunto de las n raíces diferentes de la unidad en $\mathbb{F}_{p^n}$, entonces $\beta^{p^0}\beta^{p^i} = \beta^{p^j}$, y si $\beta^{p^i} = \left(\beta^{p^0}\right)^{-1}$ se tiene que

$$\beta^{p^0}(\beta^{p^0})^{-1} = 1 = tr(\beta) = \sum_{i=0}^{n-1} \beta^{p^i}.$$

Por lo tanto $C_N = 2n - 1$.

Sabemos ahora que es importante preguntarse para qué enteros n el campo $\mathbb{F}_{p^n}$ tiene una BNO, en particular, cuando $p = 2$. A continuación daremos una respuesta a esto.

PROPOSICIÓN 5.1.2.4 ([2.7]): Supóngase que $n+1$ es número primo y que q es raíz primitiva de $\mathbb{Z}_{n+1}$, donde q es número primo o potencias de números primos. Entonces las n raíces $(n+1)$-ésimas de la unidad, diferentes de 1 son *l.i.* y forman una base normal óptima de $\mathbb{F}_{p^n}$ sobre $\mathbb{F}_p$.

PROPOSICIÓN 5.1.2.5 ([2.7]): Sea $2n + 1$ un número primo y supongamos que

i) 2 es raíz primitiva en $\mathbb{Z}_{2n+1}$,

ó

ii) $2n + 1 \equiv 3 \ mod\, 4$ y 2 genera a los residuos cuadráticos de $\mathbb{Z}_{2n+1}$.

Entonces $\alpha = \gamma + \gamma^{-1}$ genera una base normal óptima de $\mathbb{F}_{2^n}$ sobre $\mathbb{F}_2$, donde γ es una $(2n + 1)$ −ésima raíz de la unidad primitiva.

La BNO obtenida con el método de la primera proposición se llama de tipo I, y a las obtenidas en la proposición 5.1.2.5 se le llama de tipo II.

En el anexo I listamos a los números $n \leq 2000$ para los cuales existe una BNO de $\mathbb{F}_{2^n}$ sobre $\mathbb{F}_2$. Obtuvimos alrededor de un 30% de los n usando los criterios mencionados en [2.3] y [2.7], el resto se obtuvo usando un criterio más general usando resultados de [1.2]. Estos fueron programados en *Mathematica*.

Podemos concluir que en la implementación de criptosistemas que usen campos finitos de característica 2 y que utilice una gran cantidad de productos el elegir un n, donde exista una BNO, minimiza la cantidad de operaciones efectuadas.

Finalmente es bueno mencionar que la operación más rápida que se realiza en un campo finito que usa una base normal, es la exponencial. Ésta basa su eficacia en la linealidad de la exponencial.

Sea $N = \left\{\beta, \beta^2, \ldots, \beta^{2^{n-1}}\right\}$ una base normal, y $\alpha = \sum_{i=0}^{n-1} b_i \beta^{2^i}$, entonces

$$\alpha^2 = \sum_{i=0}^{n-1} b_{i-1} \beta^{2^i}$$

donde $b_{-1} = b_{n-1}$; lo que significa que elevar un elemento al cuadrado es equivalente a recorrer los bits a la derecha.

Para potencias en general α^e, donde e es un número entero; al representar a e en base 2, $e = \sum_{i=0}^{n-1} a_i 2^i$, se tiene

$$\begin{aligned} \alpha^e &= \alpha^{\sum_{i=0}^{n-1} a_i 2^i} \\ &= \prod_{i=0}^{n-1} \alpha^{a_i 2^i} \end{aligned}$$

donde se requieren tantas multiplicaciones como coeficientes $a_i \neq 0$, es decir $A = \left(\sum_{i=0}^{n-1} a_i\right) - 1$ multiplicaciones.

Existen varios métodos para mejorar este número, por ejemplo en [2.10], [2.12], [2.13] y [2.14].

Entre los métodos a que hacemos referencia antes, existen varios que usan la técnica de programar en paralelo. Existen también varios métodos para calcular inversos multiplicativos, sin embargo en las operaciones sobre curvas elípticas se pueden eliminar.

En esta sección hemos notado la importancia que tiene el elegir una buena representación de los elementos del campo para efectuar operaciones sobre él mismo. Podemos mencionar que la mejor implementación para cualquier sistema criptográfico sobre el campo finito $\mathbb{F}_{2^n}$ se tiene al elegir, ya sea una buena base polinomial, por ejemplo, los trinomios irreducibles $x^n + x^k + 1$, donde $k \leq \lfloor n/2 \rfloor$ ó también tomar una BNO.

5.2 Curvas elípticas supersingulares

Brevemente veremos algunos aspectos importantes sobre el uso en criptografía de las curvas elípticas supersingulares definidas sobre el campo finito $\mathbb{F}_{2^n}$. Este tipo de curvas en términos estrictos no son buenas, ya que para los sistemas criptográficos que las usan y cuya seguridad se basa en el PLD sobre el grupo $E(\mathbb{F}_{2^n})$, existe un método para reducir el PLDE (Poblema del logaritmo discreto elíptico) a el PLD sobre una extensión $\mathbb{F}_{2^{nk}}$, con $k \leq 6$, lo que obliga a usar campo más grande, por otra parte del teorema 3.3.1.1 sólo existen 10 clases de equivalencia de este tipo de curvas.

5.2.1 El PLD para curvas supersingulares

El PLDE se plantea como sigue: dados $P, R \in E(\mathbb{F}_{2^n})$ con m el orden de P conocido, entonces el problema del logaritmo discreto es determinar un entero l, $0 \leq l \leq m-1$, tal que $R = lP$. En el caso de las curvas supersingulares y computacionalmente hablando, este problema se ha resuelto, al haber encontrado un algoritmo subexponencial, que reduce el PLDE a el PLD sobre una extensión del campo $\mathbb{F}_{2^n}$. Con este propósito se usa el mapeo de Weil, para establecer un isomorfismo entre el subgrupo generado por P, $\langle P \rangle$, y el subgrupo de las $m-$ésimas raíces de la unidad de $\mathbb{F}_{2^{nk}}$. En este trabajo veremos sólo la idea general del algoritmo, conocido como el MOV (de Menezes, Okamoto y Vanstone), ya que insistimos, este tipo de curvas ha perdido interés en el campo de la criptografía.

Sea m un número entero primo relativo a $q = p^n$, el mapeo de Weil e_m es la función:

$$e_m : E[m] \times E[m] \to \overline{\mathbb{F}_q}$$

que cumple las siguientes propiedades:

i) Identidad: $\forall P \in E[m]$, $e_m(P,P) = 1$.

ii) Alternancia: $\forall P_1, P_2 \in E[m]$, $e_m(P_1,P_2) = e_m(P_2,P_1)^{-1}$.

iii) Bilinealidad: $\forall P_1, P_2, P_3 \in E[m]$,

$$\begin{aligned} e_m(P_1+P_2,P_3) &= e_m(P_1,P_3)\,e_m(P_2,P_3) \\ e_m(P_1,P_2+P_3) &= e_m(P_1,P_3)\,e_m(P_1,P_3) \end{aligned}$$

iv) No degenerativa: Si $P_1 \in E[m]$, entonces $e_m(P_1,\mathcal{O}) = 1$. Si $e_m(P_1,P_2) = 1$, $\forall P_2 \in E[m]$, entonces $P_1 = \mathcal{O}$.

v) Si $E[m] \subseteq E\left(\mathbb{F}_{q^k}\right)$, entonces $e_m(P_1,P_2) \in \mathbb{F}_{q^k}$, $\forall P_1, P_2 \in E[n]$.

Para más detalles respecto al mapeo de Weil y su uso en el MOV se puede consultar [2.3], [7.1], [7.9], [9.1] y [10.10].

El algoritmo para reducir el PLDE al PLD es el siguiente:

Entrada: Un elemento $P \in E(\mathbb{F}_q)$ de orden m, donde $mcd(m,q) = 1$ y $R \in \langle P \rangle$

Salida: Un entero l, tal que $R = lP$

Paso 1: Determinar el entero más pequeño k, tal que $E[m] \subseteq E\left(\mathbb{F}_{q^k}\right)$

Paso 2: Encontrar $Q \in E[m]$ y calcular $\alpha = e_m(P,Q)$

Paso 3: Calcular $\beta = e_m(R,Q)$

Paso 4: Calcular l el logaritmo discreto de β base α, en $\mathbb{F}_{q^k}$

El número l es el logaritmo elíptico buscado, ya que

$$\beta = e_m(R,Q) = e_m(lP,Q) = e_m(P,Q)^l = \alpha^l$$

Resta conocer el valor de k. En la siguiente tabla lo tenemos para cada clase de curvas elípticas supersingulares ([2.3], [7.1], [7.9]).

Clase	t	k	$E(\mathbb{F}_q)$
I	0	2	*cíclico*
II	0	2	$\mathbb{Z}_{(q+1)/2} \times \mathbb{Z}_2$
III	$\pm\sqrt{q}$	3	*cíclico*
IV	$\pm\sqrt{2q}$	4	*cíclico*
V	$\pm\sqrt{3q}$	6	*cíclico*
VI	$\pm 2\sqrt{q}$	1	$\mathbb{Z}_{\sqrt{q}\mp 1} \times \mathbb{Z}_{\sqrt{q}\mp 1}$

Se puede ver ([7.1]) que para las curvas elíptica supersingulares, el número de puntos racionales cae dentro de los 6 casos y para cada uno está su respectivo k, donde se cumple que $\#E(\mathbb{F}_q) = q + 1 - t$.

Como un ejemplo de una curva supersingular tomemos el siguiente. Sea $= x^2 + x + 1$, y $E_1 : y^2 + y = x^3$, entonces

$$E_1(\mathbb{F}_{2^2}) = \left\{\mathcal{O}, (0,0), (0,1), (1,\alpha), \left(1,\alpha^2\right), (\alpha,\alpha), \left(\alpha,\alpha^2\right), \left(\alpha^2,\alpha\right), \left(\alpha^2,\alpha^2\right)\right\}$$

que denotaremos como:

$$E_1 = \{P_0, P_1, P_2, P_3, P_4, P_5, P_6, P_7, P_8\}$$

Donde la tabla de suma para $E(\mathbb{F}_{2^2})$ es:

$+$	P_0	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8
P_0									
P_1		P_2	P_0	P_5	P_8	P_7	P_4	P_3	P_6
P_2		P_0	P_1	P_7	P_6	P_3	P_8	P_5	P_4
P_3		P_5	P_7	P_4	P_0	P_8	P_2	P_6	P_1
P_4		P_8	P_6	P_0	P_3	P_1	P_7	P_2	P_5
P_5		P_7	P_3	P_8	P_1	P_6	P_0	P_4	P_2
P_6		P_4	P_8	P_2	P_7	P_0	P_5	P_1	P_3
P_7		P_3	P_5	P_6	P_2	P_4	P_1	P_8	P_0
P_8		P_6	P_4	P_1	P_5	P_2	P_3	P_0	P_7

podemos mostrar que: $E \simeq \mathbb{Z}_3 \times \mathbb{Z}_3$ de acuerdo a la clase VI.

Concluyendo, en las curvas supersingulares existe un algoritmo, el MOV, como método para romper sistemas criptográficos que basen su seguridad en el PLDE. En caso de utilizar este tipo de curvas habría que usar campos $\mathbb{F}_{q^k}$, de orden donde aún sea lento resolver el PLD, que según [3.13], tendría que ser $nk > 600$, donde $q^k = 2^{nk}$

5.3 Curvas no-supersingulares sobre $\mathbb{F}_{2^n}$

En esta sección estudiamos el tipo de curvas elípticas, que es más atractivo para implementar sistemas criptográficos, las curvas no supersingulares definidas sobre el campo $\mathbb{F}_{2^n}$. Finalizaremos con la propuesta de una curva E y un campo finito K para la implementación de un sistema criptográfico seguro, y que pueda ser implementado con pocos recursos.

La forma normal de Weierstrass de una curva elíptica no supersingular definida sobre un campo finito de característica 2 toma la forma

$$E : y^2 + xy = x^3 + a_2x^2 + a_6$$

donde $a_6 \neq 0$. Como se vio en 3.3, tenemos $2(q-1)$ clases de equivalencia, donde $q = 2^n$. Podemos entonces decir que en este caso existe un gran número de posibilidades de tomar una curva aleatoria. Sin embargo, tenemos el problema de calcular el número de puntos racionales de E, esto en general, no es fácil de determinar y aún no existe un buen algoritmo que lo haga ([10.9], [10.12], [10.13], [10.14], [10.17]).

Recordemos algunas definiciones que nos ayudarán a ver un panorama general sobre este tipo de curvas.

DEFINICIÓN 5.3.1: Sea E una curva elíptica sobre $\mathbb{F}_q$, $q = p^n$. El endomorfismo de Frobenius $\phi \in End_{\overline{F}_q}(E)$ es el endomorfismo de E que actúa en $E\left(\overline{F}_q\right)$ elevando las coordenadas de los puntos racionales a la q–ésima potencia: $\phi : (x, y) \rightarrow (x^q, y^q)$.

PROPOSICIÓN 5.3.2 ([9.11]): Sea E una curva elíptica sobre $\mathbb{F}_{2^n}$, y ϕ el endomorfismo de Frobenius, entonces:

i) El endomorfismo ϕ satisface la ecuación $\phi^2 - t\phi + q = 0$, donde t es la traza del endomorfismo ϕ.

ii) $|t| \leq 2\sqrt{q}$.

iii) $\#E(\mathbb{F}_q) = N(\phi - 1) = q + 1 - t$.

iv) $p \mid t$, sí y sólo si E es supersingular.

DEMOSTRACIÓN: Ver [9.11] y [10.2].

De la proposición anterior, para poder encontrar el número de puntos racionales de una curva elíptica $E(\mathbb{F}_{2^n})$ no supersingular basta encontrar a t, y por iv), t debe ser impar. Por otra parte, es importante también conocer el número de curvas elípticas no equivalentes con el mismo t, es decir, con el mismo número de elementos.

Si N_t es el número de curvas elípticas no supersingulares no equivalentes, de [10.2] se obtienen los siguientes resultados:

Sea Δ un número entero no negativo congruente con 0 ó 1 $mod\, 4$, sea

$$B(\Delta) = \left\{ ax^2 + bxy + cy^2 \in \mathbb{Z}[x, y] \mid a > 0, \Delta = b^2 - 4ac \right\}$$

el conjunto de formas cuadráticas definidas positivas con discriminante Δ, y $CL(\Delta) = B(\Delta)/SL_2$, donde SL_2 es el grupo modular, definimos a $H(\Delta) = |CL(\Delta)|$. Entonces:

$$N_t = H\left(t^2 - 4q\right).$$

Por ejemplo, tomando los valores de H de la tabla que se encuentra en [10.2], obtenemos la siguiente tabla para las curvas elípticas no supersingulares E sobre el campo $\mathbb{F}_{2^5}$.

t	t^2-4q	$H(t^2-4q)$	$\lvert E\rvert$
1	-127	5	32
3	-119	10	30
5	-103	5	28
7	-79	5	26
9	-47	5	24
11	-7	1	22
-1	-127	5	34
-3	-119	10	36
-5	-103	5	38
-7	-79	5	40
-9	-47	5	42
-11	-7	1	44

observamos primero que $\sum_t H(t^2-4q) = 62$ de acuerdo con $2(2^5-1)$ número de clases de equivalencia para curvas elípticas no supersingulares definidas sobre $\mathbb{F}_{2^5}$. Esta tabla se encuentra también en [7.7] y fue usada para analizar el grupo $E(\mathbb{F}_{2^{155}})$.

El principal objeto de usar una curva elíptica no supersingular es que en este tipo de curvas el MOV no es eficiente. Recordamos que MOV encaja a $E(\mathbb{F}_q)$ en una extensión $\mathbb{F}_{q^k}$, entonces cualquier método que haga lo anterior requiere que $m =$ el orden de P, $P \in E(\mathbb{F}_q)$ divida a q^k-1. Cosa que incluso se puede verificar para curvas elípticas que se generen aleatoriamente.

Lo anterior nos lleva a elegir curvas no supersingulares donde en principio lo primordial es que el número de elementos, $\#(E(\mathbb{F}_q))$, tenga un factor primo "suficientemente" grande, para que los ataques conocidos al PLD en grupos arbitrarios no sea factible aplicar. Los métodos conocidos hasta el momento ([3.14], [3.15]), reducen el cálculo del logaritmo discreto sobre m el orden de $E(\mathbb{F}_q)$, a calcular el logaritmo discreto sobre los factores primos de m; además estos métodos dependen fuertemente del número de dígitos que tenga el factor primo. En la actualidad podemos decir que un número seguro debe ser mayor a 50 dígitos, aún con los modernos algoritmos en paralelo.

Es prudente mencionar que existe una fuerte relación de el PLD y toda la criptografía con el problema de la factorización y primacidad de números enteros. Para una completa información y estudio del tema véase [11] y [12].

Según la conjetura de Weil, una curva elíptica E definida sobre $\mathbb{F}_q$ puede ser vista como una curva elíptica sobre cualquier extensión $\mathbb{F}_{q^n}$, y además podemos calcular el número de puntos racionales de $E(\mathbb{F}_{q^n})$ a partir de $\#E(\mathbb{F}_q)$; con la siguiente igualdad $\#E(\mathbb{F}_{q^n}) = q^n + 1 - \alpha^n - \beta^n$, donde α, β son números complejos conjugados tales que $1 - tT + qT^2 = (1 - \alpha T)(1 - \beta T)$. En algunos casos esto es fácil de determinar, y si además agregamos que la curva elíptica sea extensión de una curva definida en un campo pequeño con $t = \pm 1$, es decir $\#E(\mathbb{F}_q) = q, q+2$, la operación nP puede efectuarse eficientemente ([7.10]). A tales curvas se les conoce con el nombre de *anómalas*.

Antes de determinar el número de elementos de curvas elípticas que provienen de curvas anómalas, veamos algunas definiciones relacionadas con esto.

DEFINICIÓN 5.3.3: Dada la curva $E : y^2 + xy = x^3 + a_2 x + a_6$, sobre $\mathbb{F}_q$ no supersingular, la curva $\tilde{E} : y^2 + xy = x^3 + (a_2 + D)x + a_6$, se le llama la pareja de E, donde $D \in \mathbb{F}_q$ y $t^2 + t + D$ es irreducible sobre $\mathbb{F}_q$, $q = 2^n$.

PROPOSICIÓN 5.3.4: Sea E una curva elíptica como antes mencionamos, entonces $\tilde{E} : y^2 + xy = x^3 + (a_2 + D)x + a_6$ es su pareja si y sólo si $tr(D) = 1$.

DEMOSTRACIÓN: $t^2 + t + D$ es irreducible sobre $\mathbb{F}_q$, si y sólo si $t^2 + t + D \neq 0 \ \forall t \in \mathbb{F}_q$, es decir, que $tr(D) = 1$, ya que $tr(D) = 0$, si y sólo si existe t tal que $t^2 + t = D$.

PROPOSICIÓN 5.3.5: Para todo elemento $x \in \mathbb{F}_{2^n}$, este x aparece como la coordenada x de exactamente 2 puntos de E o 2 de $\tilde{E}$. De donde $\#E + \#\tilde{E} = 2(2^n + 1)$.

DEMOSTRACIÓN: Tomemos a $x \neq 0$, entonces la ecuación de E puede ser escrita como (1) $t^2 + t + c = 0$, donde $t = \frac{y}{x}$, y $c = \frac{x^3 + a_2 x^2 + a_6}{x^2}$ que es constante, de forma similar para $\tilde{E}$ tenemos la ecuación (2) $t^2 + t + (c + D) = 0$. La ecuación (1) tiene solución si y sólo si c es imagen de la función $f(t) =$

t^2+t. Un elemento s es imagen de f si y sólo si $tr(s)=0$. Luego $D \notin Im(f)$, es decir sólo uno de los dos elementos c o $c+D$ pertenecen a $Im(f)$, o sea solo (1) ó (2) tiene dos soluciones. El caso de que $x=0$, tenemos a $y^2=a_6$. Por otro lado, al contar los puntos racionales de $\#E+\#\tilde{E}$: para cada $x \neq 0$ tenemos dos puntos racionales, por lo que llevamos $2(2^n-1)$ puntos; si $x=0$ tenemos otros dos, y más dos infinitos, hay un total de $2(2^n+1)$.

En la siguiente proposición damos una forma fácil para poder obtener el número de puntos racionales de una curva anómala sobre una extensión $\mathbb{F}_{q^n}$, y por la proposición anterior se sigue que podemos obtener también el número de puntos racionales de la pareja de la curva. Más aún $N_n = q^n+1-a_n$ y $\widetilde{N}_n = q^n+1+a_n$, donde $a_n = \alpha^n+\beta^n$, y $\alpha = \frac{(1+\sqrt{1-4q})}{2}$.

PROPOSICIÓN 5.3.6: Si $a_0=2$, $a_1=1$, la sucesión a_n, satisface la siguiente relación de recurrencia $a_n = a_{n-1} - qa_{n-2}$.

DEMOSTRACIÓN: Se sigue de la relación $a_n = (\alpha+\beta)(\alpha^{n-1}+\beta^{n-1}) - \alpha\beta(\alpha^{n-2}+\beta^{n-2})$.

Veamos finalmente algunos ejemplos de este tipo de curvas:

Primero obsérvese que para $n=5$, tenemos a $a_5=11$, y por lo tanto la curva $E: y^2+xy = x^3+x^2+1$ tiene 22 $\mathbb{F}_{2^5}$-puntos racionales y su pareja $\tilde{E}: y^2+xy = x^3+1$, tiene 44 $\mathbb{F}_{2^5}$-puntos racionaless de acuerdo a la tabla que muestra todas las curvas sobre $\mathbb{F}_{2^5}$.

Recordemos que estamos buscando curvas donde el número de puntos racionales tenga un factor primo "grande", esto garantiza la seguridad del sistema criptográfico. Pero además de la seguridad, es necesario que tenga el menor número de dificultades de poder ser implementado. De acuerdo a 5.1, esto es, que para el campo de definición exista una BNO (Base Normal Óptima) o por otro lado una buena base polinomial, es decir, un trinomio irreducible de la forma x^n+x^k+1. Para $n \leq 360$ impar tenemos los siguientes candidatos que cumplen las dos condiciones:

n	k	n	k	n	k
3	1	81	4	209	6
5	2	89	38	231	26
9	1	95	11	233	74
11	2	105	4	239	36
23	5	113	9	273	23
29	2	119	8	281	93
33	10	135	11	303	1
35	2	155	62	329	50
41	3	183	56	359	68
65	18	191	9	375	16

para tales valores de n existe una BNO y una buena base polinomial donde, $x^n + x^k + 1$, es el polinomio irreducible.

Finalmente damos algunos valores de a_n, y el número de puntos racionales de la curva elíptica correspondiente que cumplen las dos condiciones de implementación, donde $E : y^2 + xy = x^3 + x^2 + 1$, y $\tilde{E} : y^2 + xy = x^3 + 1$, ya que n es impar. Los resultados los obtuvimos usando *Mathematica*.

$a_3 = -5$, $\#E = 7 \cdot 2$, $\#\tilde{E} = 2 \cdot 2$
$a_5 = 11$, $\#E = 11 \cdot 2$, $\#\tilde{E} = 2^2 \cdot 11$
$a_9 = -5$, $\#E = 2 \cdot 7 \cdot 37$, $\#\tilde{E} = 2^2 \cdot 127$
$a_{11} = 67$, $\#E = 2 \cdot 991$, $\#\tilde{E} = 2^2 \cdot 23^2$

$a_{89} = 337619992448 59$
$\#E = 2 \cdot 179 \cdot 5874 \cdot 29433726618795774893$
$\#\tilde{E} = 2^2 \cdot 179 \cdot 1962451 \cdot 440512026877326167$

$a_{113} = 1267584991505179$
$\#E = 2 \cdot 5192\ 29685\ 85348\ 27627\ 89670\ 38334\ 67507$
$\#\tilde{E} = 2^2 \cdot 6329 \cdot 27826703 \cdot 147411942910839506174 89$

Observamos que la curva elíptica E definida sobre el campo finito $\mathbb{F}_{2^{113}}$, ofrece cierta seguridad, ya que el número de puntos racionales es producto

de 2 por un número de 34 dígitos y en $\mathbb{F}_{2^{113}}$ tenemos grandes posibilidades de implementación, ya que existe tanto una BNO como una buena base polinomial, por lo que podemos utilizar los mejores algoritmos, creados hasta la fecha, para efectuar la aritmética de un campo finito.

5.4 Criptosistemas elípticos

En esta sección (culminación de todo lo expuesto) describimos los pasos consistentes de un sistema criptográfico elíptico que utiliza el grupo de puntos racionales de una curva no supersingular definida sobre el campo finito $\mathbb{F}_{2^n}$, que está representado por una base normal óptima y se ilustra con ejemplos. Los pasos que seguimos son exactamente los mismos que se llevan en el diseño de un sistema real ([7.6]).

5.5.1 Elementos del sistema

1.- Como ya sabemos, los elementos de un campo finito los podemos representar por medio de una BNO o una buena base polinomial. Si decidimos tomar una BNO primeramente hay que fijar un entero n y verificar que para este entero existe una BNO. Posteriormente, para construir la BNO se procede como en los métodos de las proposiciones 5.1.2.4 ó 5.1.2.6, es decir, se quiere encontrar a un elemento β que genere a la BNO.

Veamos un ejemplo para el campo $\mathbb{F}_{2^3}$, sus elementos se pueden representar como:

$$\begin{aligned}
\alpha^0 &= 1 && \sim (001)\\
\alpha^1 &= \alpha && \sim (010)\\
\alpha^2 &= \alpha^2 && \sim (100)\\
\alpha^3 &= \alpha + 1 && \sim (011)\\
\alpha^4 &= \alpha^2 + \alpha && \sim (110)\\
\alpha^5 &= \alpha^2 + \alpha + 1 && \sim (111)\\
\alpha^6 &= \alpha^2 + 1 && \sim (101)
\end{aligned}$$

añadiendo al (000), donde α es una raíz del polinomio $x^3 + x + 1$. De 5.1 $\beta = \alpha^3$, genera una base normal. En este caso es la única base normal, que

además es óptima. Así, los elementos del campo $\mathbb{F}_{2^3}$ representados en una base normal óptima quedan como:

$$\begin{array}{lll} \beta & = \beta & \sim (001) \\ \beta^2 & = \beta^2 & \sim (010) \\ \beta^3 & = \beta^{2^2} + \beta & \sim (101) \\ \beta^4 & = \beta^{2^2} & \sim (100) \\ \beta^5 & = \beta^2 + \beta^{2^2} & \sim (110) \\ \beta^6 & = \beta + \beta^2 & \sim (011) \\ \beta^7 & = \beta + \beta^2 + \beta^{2^2} & \sim (111) \end{array}$$

2.- La curva no supersingular

La curva elíptica no supersingular se elige aleatoriamente. Por ejemplo, sea $E : y^2 + xy = x^3 + x^2 + 1$ la curva que tiene $2 \cdot 7$ puntos racionales sobre $\mathbb{F}_{2^3}$ (5.3), a continuación damos estos puntos racionales considerando la representación con la base normal óptima de $\mathbb{F}_{2^3}$.

$$\begin{array}{llll} P_0 = \mathcal{O} & P_1 = (\beta, \beta) & P_2 = (\beta, 0) & P_3 = (\beta^2, \beta^2) \\ P_4 = (\alpha^2, 0) & P_5 = (\beta^3, \beta) & P_6 = (\beta^3, \beta^4) & P_7 = (\beta^4, \beta^4) \\ P_8 = (\beta^4, 0) & P_9 = (\beta^5, \beta^2) & P_{10} = (\beta^5, \beta^4) & P_{11} = (\beta^6, \beta) \\ P_{12} = (\beta^6, \beta^2) & P_{13} = (0, \beta^7) & & \end{array}$$

Por 5.3, este grupo es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_7$. En efecto, $2P_{13} = \mathcal{O}$, y por otra parte el subgrupo de orden 7 es

$\{P_1, 2P_1 = P_7, 3P_1 = P_4, 4P_1 = P_3, 5P_1 = P_8, 6P_1 = P_2, 7P_1 = \mathcal{O}\}$

En el anexo 2 tenemos una tabla completa de este grupo.

3.- Aritmética de $F(2^n)$

Recordemos de 3.3.2 que las operaciones que hacen a $E(\mathbb{F}_{2^n})$ un grupo son:

Si $P = (x_1, y_1) \in E(\mathbb{F}_{2^n})$, entonces $-P = (x_1, y_1 + x_1)$. Si $Q = (x_2, y_2) \in E(\mathbb{F}_{2^n})$ y $Q \neq -P$, entonces $P + Q = (x_3, y_3)$ donde

$$\begin{pmatrix} x_3 \\ y_3 \end{pmatrix} = \begin{pmatrix} \left(\frac{y_1+y_2}{x_1+x_2}\right)^2 + \frac{y_1+y_2}{x_1+x_2} + x_1 + x_2 + a_2 \\ \left(\frac{y_1+y_2}{x_1+x_2}\right)(x_1 + x_3) + x_3 + y_1 \end{pmatrix}$$

si $P \neq Q$, y

$$\begin{pmatrix} x_3 \\ y_3 \end{pmatrix} = \begin{pmatrix} \frac{a_6}{x_1^2} + x_1^2 \\ x_1^2 + \left(x_1 + \frac{y_1}{x_1}\right) x_3 + x_3 \end{pmatrix}$$

si $P = Q$.

Estas operaciones se realizan en el campo, observamos que hay que calcular inversos y aún con los algoritmos existentes consumen mucho tiempo, por tal motivo las operaciones se realizan en el plano proyectivo donde se elimina la división.

Si $P = (x_1, y_1, z_1)$ y $Q = (x_2, y_2, z_2)$ son puntos en $\mathbb{P}^2(\mathbb{F}_{2^n})$, entonces $P = \left(\frac{x_1}{z_1}, \frac{y_1}{z_1}, 1\right)$ y $Q = \left(\frac{x_2}{z_2}, \frac{y_2}{z_2}, 1\right)$ son puntos en el plano afín que satisfacen las anteriores relaciones, que al reducirlas obtenemos lo siguiente:

Si $P, Q \neq \mathcal{O}$ y $P \neq -Q$, entonces $P + Q = (x_3, y_3, z_3)$ donde

$$\begin{pmatrix} x_3 \\ y_3 \\ z_3 \end{pmatrix} = \begin{pmatrix} AD \\ CD + A^2(Bx_1 + Ay_1) \\ A^3 z_1 z_2 \end{pmatrix}$$

donde $P \neq Q$ y $A = x_2 z_1 + x_1 z_2$, $B = y_2 z_1 + y_1 z_2$, $C = A + B$, y $D = A^2(A + a_2 z_1 z_2) + z_1 z_2 BC$.

Para $P = Q$, tenemos

$$\begin{pmatrix} x_3 \\ y_3 \\ z_3 \end{pmatrix} = \begin{pmatrix} AB \\ x_1^4 A + B(x_1^2 + y_1 z_1 + A) \\ A^3 \end{pmatrix}$$

donde $A = x_1 z_1$, y $B = a_6 z_1^4 + x_1^4$.

Otro método para calcular kP se puede ver en [7.10].

5.5.2 Criptosistemas con curvas elípticas

Los criptosistemas elípticos son usados principalmente para diseñar esquemas de encriptamiento de información, esquemas de firma digital y protocolos de intercambio de llaves usados en los sistemas de llave privada. En los tres casos varían los pasos a seguir, pero escencialmente los tres basan su seguridad en la dificultad de resolver el PLDE. En seguida describimos un esquema de encriptamiento y desencriptamiento de información usando el grupo de puntos racionales de una curva elíptica.

Parámetros de un sistema de encriptamiento con curvas elípticas (ECE): se supone que el campo $\mathbb{F}_q$, la curva E definida sobre $\mathbb{F}_q$, y un punto $P \in E(\mathbb{F}_q)$, son elegidos; al orden de P se le denotará como s; la anterior información es pública.

Generación de llaves

1) Se elige un número entero aleatorio $d \in [1, s-1]$
2) Se calcula el punto $Q = dP$
3) La llave pública consiste del punto Q
4) La llave secreta es el entero d

Proceso de encriptamiento

El usuario **A** desea mandar el mensaje M a **B**

1) Se busca la llave pública de **B**, es decir Q
2) Se representa el mensaje M como un par de puntos $(m_1, m_2) \in (\mathbb{F}_q)^2$
3) Se selecciona un número aleatorio k
4) Se calcula el punto $(x_1, y_1) = kP$
5) Se calcula el punto $(x_2, y_2) = kQ$
6) Se combinan los elementos m_1, m_2, x_2 y y_2 para obtener dos elementos c_1, c_2
7) **A** transmite a $c = (x_1, y_1, c_1, c_2)$

Proceso de desencriptamiento

1) El usuario **B** calcula el punto $(x_2, y_2) = d(x_1, y_1)$ con la llave secreta d.

2) Recobra el mensaje a partir de c_1, c_2, x_2 y y_2.

Veamos ahora ejemplos concretos:

(a) Considere el campo $\mathbb{F}_{2^3}$, la curva $E : y^2 + xy = x^3 + x^2 + 1$ y al punto $P_1 = (\beta, \beta)$ de orden 7 de la sección anterior. Así los parámetros del ECE son $(\mathbb{F}_{2^3}, E, P_1, 7)$.

Generación de llaves

1) **B** selecciona a $d = 6$
2) **B** calcula el punto $Q = 6P_1 = P_2 = (\beta, 0)$
3) La llave privada es 6
4) La llave pública es P_2

Proceso de encriptamiento

1) **A** busca la llave pública de **B**, $Q = P_2 = (\beta, 0)$
2) **A** representa el mensaje M como $m_1 = \beta^5$, $m_2 = \beta^2$
3) **A** selecciona un número aleatorio $k = 2$
4) **A** calcula el punto $2P_1 = P_7 = (\beta^4, \beta^4)$
5) **A** calcula el punto $2Q = 2P_2 = P_8 = (x_2, y_2) = (\beta^4, 0)$
6) **A** calcula el elemento $x_2^3 = (\beta^4)^3 = \beta^5$
7) **A** forma a $x_4 = (100)$ concatenando los dos primeros dígitos binarios (bits) de x_2 y el último de x_2^3. También forma a $y_4 = (110)$ de forma simétrica, es decir, tomando los dos primeros bits de x_2^3 y el último de x_2. Observe que M y (x_4, y_4) no necesariamente están en la curva.
8) **A** forma los elementos

$$c_1 = (m_1 + y_2)\, x_4 = \left(\beta^5 + 0\right) \beta^4 = \beta^2$$

$$c_2 = (m_2 + x_2)\, y_4 = \left(\beta^2 + \beta^4\right) \beta^5 = \beta^3$$

9) Finalmente **A** transmite el mensaje

$$c = \left(\beta^4, \beta^4, \beta^2, \beta^3\right)$$

Proceso de desencriptamiento

1) **B** calcula el punto $6\,(\beta^4, \beta^4) = 6P_7 = P_8$
2) **B** calcula a $x_4 = (100)$ y $y_4 = (110)$ de la misma forma que A
3) **A** calcula los elementos

$$\begin{aligned} m_1 + y_2 &= \beta^2 x_4^{-1} = \beta^5 \\ m_2 + x_2 &= \beta^3 y_4^{-1} = \beta^5 \end{aligned}$$

4) Finalmente **B** recobra el mensaje M por

$$\begin{aligned} m_1 &= \beta^5 + 0 = \beta^5 \\ m_2 &= \beta^5 + \beta^4 = \beta^2 \end{aligned}$$

(b) En el siguiente ejemplo tomaremos al campo $\mathbb{F}_{2^6}$, con el polinomio irreducible $p(x) = x^6 + x + 1$ y α una raíz de $p(x)$: la curva $E : y^2 + xy = x^3 + (1 + \alpha^5)x^2 + 1$, con 74 $\mathbb{F}_{2^6}-$puntos racionales. Por otra parte si $\beta = \alpha^{23}$, entonces β genera una base normal óptima. En la segunda parte del anexo II damos más información del grupo $E(\mathbb{F}_{2^6})$.

En este ejemplo tenemos entonces a $(\mathbb{F}_{2^6}, E, P, 37)$ como parámetros, donde $P = (\beta^2, \beta^3)$.

Generación de llaves

1) **B** selecciona a $d = 10$

2) **B** calcula el punto $Q = 10P = (\beta^{51}, \beta^{38})$
3) La llave privada es 10
4) La llave pública es Q

Proceso de encriptamiento

1) **A** busca la llave pública de **B**, $Q = (\beta^{51}, \beta^{38})$
2) **A** representa el mensaje M como $M = (\beta^{23}, \beta^{14}) = (m_1, m_2)$
3) **A** selecciona un número aleatorio $k = 8$
4) **A** calcula el punto $8P = (\beta^{57}, \beta^{33}) = (x_1, y_1)$
5) **A** calcula el punto $8Q = (\beta^{39}, \beta^{15}) = (x_2, y_2)$
6) **A** calcula el elemento $x_2^3 = (\beta^{39})^3 = \beta^{54} = (101101)$
7) **A** forma a $x_4 = (011101)$, concatenando los tres primeros bits de $x_2 = (\beta^{39}) = (011111)$ y los tres últimos de x_2^3. De forma simétrica forma a $y_4 = (101111)$ con los primeros tres bits de x_2^3 y los últimos de x_2: una vez más observe que no es necesario que M sea punto racional.
8) **A** forma los elementos:

$$\begin{aligned} c_1 &= (m_1 + y_2)\, x_4 = \left(\beta^{23} + \beta^{15}\right) \beta^{11} = \beta^{23} \\ c_2 &= (m_2 + x_2)\, y_4 = \left(\beta^{14} + \beta^{39}\right)\ \beta^{15} = \beta^{53} \end{aligned}$$

9) Finalmente **A** transmite el mensaje

$$c = \left(\beta^{57}, \beta^{33}, \beta^{23}, \beta^{53}\right)$$

Proceso de desencriptamiento

1) **B** calcula al punto $10\,(\beta^{57}, \beta^{33}) = (x_2, y_2)$
2) **B** calcula a x_4 y y_4 de la misma forma que **A**
3) **A** calcula los elementos

$$\begin{aligned} m_1 + y_2 &= \beta^{23} x_4^{-1} \\ m_2 + x_2 &= \beta^{53} y_4^{-1} \end{aligned}$$

4) Finalmente **A** recupera el mensaje M

$$\begin{aligned} m_1 &= \beta^{12} + \beta^{15} = \beta^{23} \\ m_2 &= \beta^{38} + \beta^{39} = \beta^{14} \end{aligned}$$

5.5 Conclusiones

En esta última sección trataremos de resumir los principales resultados que estudiamos en esta tesis, así como mencionar las posibles direcciones que pueden tomar los diferentes temas; esto a manera de tener el panorama global sobre el área que mantuvo nuestro interés: la criptografía elíptica.

1) Para elegir el campo finito, ya sea de la forma $\mathbb{Z}_p$ o $\mathbb{F}_{2^n}$, hay que considerar lo siguiente: en el primer caso que la aritmética sobre $\mathbb{Z}_p$ sea la más eficaz ([6.4]); en el segundo caso hay que considerar tanto la aritmética que exista una BNO o una buena base polinomial.

2) Sobre la elección de la curva elíptica E, recordamos que si el campo elegido es $\mathbb{Z}_p$, entonces la curva por usar es aquella que evite los ataques conocidos hasta hoy, y esto se logra conociendo el número de puntos racionales para así elegir la curva que evite el MOV, el método general de la raíz cuadrada y el recientemente difundido método de Smart, Satoh, y Araki es pertinente mencionar que las curvas propuestas por A. Miyaji [7.12] son desechadas por este ataque. Por otro lado, si el campo es del tipo $\mathbb{F}_{2^n}$, entonces, las curvas no-supersingulares son las que garantizan mayor seguridad; además que existe una gran cantidad de este tipo de curvas. Sin embargo, hasta hoy se siguen mejorando los métodos para calcular el número de puntos racionales sobre E, asi como el cálculo de nP, por lo que tiene gran significado el estudio de curvas elípticas que son extesión de las curvas anómalas, donde nP es de fácil obtención (7.10).

3) En el caso general, es decir, si la curva elíptica no-supersingular se elige aleatoriamente, se deben de evitar los ataques conocidos. El ataque de la raíz cuadrada ([3.14]) o el conocido como MOV ([7.9]). El primero lo evitamos si se logra que el orden del grupo de puntos racionales de la curva elíptica tenga un factor primo de almenos 45 dígitos ([3.15]); el segundo ataque consiste escencialmente en incluir al grupo $E(\mathbb{F}_{2^n})$ en una extensión del campo $\mathbb{F}_{2^{nk}}$, por lo tanto, el evitar este ataque consiste en elegir una curva cuyo número de puntos racionales m tenga un factor primo que no divida a $2^{nk}-1$ para un k considerable, por ejemplo, $k=20$.

4) Últimamente han tenido gran atención este tipo de sistemas, por lo que una línea obvia de estudio es el encontrar un ataque eficiente para el caso general (no-supersingular). El resolver el Problema del Logaritmo Discreto Elíptico, PLDE, sería la mejor forma; sin embargo, hasta el momento no se ha podido encontrar un eficiente algoritmo que calcule logaritmos discretos en $E(\mathbb{F}_{2^n})$. De forma natural nos podemos preguntar si existe otra forma de ataque al sistema, esto es otra línea de investigación en la que todavía no se conocen buenos resultados.

5) Es notable la lentitud que existe en la criptografía de llave pública, en comparación a la criptografía de llave privada, por lo que son aún investigados nuevos y más rápidos métodos que efectúen las operaciones sobre el grupo de puntos racionales de una curva elíptica sobre un campo finito.

6) En la búsqueda de otro tipo de protocolo que use curvas elípticas se mencionan con frecuencia los protocolos que usan curvas elípticas definidas sobre el anillo $\mathbb{Z}_{pq}$, donde p, q son números primos. Sin embargo, se ha mostrado que este tipo de sistemas es equivalente en seguridad al sistema RSA, por lo que no ofrece alguna ventaja sobre éstos, además que es más complicado efectuar operaciones sobre $E(\mathbb{Z}_{pq})$ ([7.16], [7.17], [7.18], [7.19]).

7) Desde 1989 ([8.1]), como natural generalización para criptosistemas, fueron sugeridas las curvas hiperelípticas C definidas sobre el campo $\mathbb{F}_{2^n}$. Las curvas elípticas son realmente un caso particular de las hiperelípticas. Hasta hoy se desconoce mucho sobre este tema, lo cual lo hace más atractivo para la investigación. El obtener resultados sobre la seguridad que este tipo de sistemas ofrece es aún problema abierto ([8.2]), de forma análoga, el cómo clasificar a las curvas hiperelípticas más atractivas en criptografía es otra pregunta sin respuesta; de forma similar el encontrar métodos que calculen eficientemente la suma de divisores sobre el jacobiano de la curva hiperelíptica C, es un buen tema de estudio ([8.3], [8.4], [8.5], [8.6], [8.7]).

ANEXO I

Valores de números n, para los cuales existe una BNO en $\mathbb{F}_{2^n}$. Los números marcados por $*$ tienen sólo la BNO de tipo I, † significa la existencia de una BNO de tipo I y II. El número sin marca tiene sólo la BNO de tipo II

2†	3	4*	5	6	9	10*	11	12*	14
18†	23	26	28*	29	30	33	35	36*	39
41	50	51	52*	53	58*	60*	65	66*	69
74	81	82*	83	86	89	90	95	98	99
100*	105	106*	113	119	130*	131	134	135	138*
146	148*	155	158	162*	172*	173	174	178*	179
180*	183	186	189	191	194	196*	209	210†	221
226*	230	231	233	239	243	245	251	254	261
268*	270	273	278	281	292*	293	299	303	306
309	316*	323	326	329	330	338	346*	348*	350
354	359	371	372*	375	378†	386	388*	393	398
410	411	413	414	418*	419	420*	426	429	431
438	441	442*	443	453	460*	466*	470	473	483
490*	491	495	508*	509	515	519	522*	530	531
540*	543	545	546*	554	556*	558	561	562*	575
585	586*	593	606	611	612*	614	615	618†	629
638	639	641	645	650	651	652*	653	658*	659
660*	676*	683	686	690	700*	708*	713	719	723
725	726	741	743	746	749	755	756*	761	765
771	772*	774	779	783	785	786*	791	796*	803
809	810	818	820*	826*	828*	831	833	834	846
852*	858*	866	870	873	876*	879	882*	891	893
906*	911	923	930	933	935	938	939	940*	946*
950	953	965	974	975	986	989	993	998	1013
1014	1018*	1019	1026	1031	1034	1041	1043	1049	1055
1060*	1065	1070	1090*	1103	1106	1108*	1110	1116*	1118
1119	1121	1122*	1133	1134	1146	1154	1155	1166	1169
1170*	1178	1185	1186*	1194	1199	1211	1212*	1218	1223
1228*	1229	1233	1236*	1238	1251	1258*	1265	1269	1271
1274	1275	1276*	1278	1282*	1289	1290*	1295	1300*	1306*
1310	1323	1329	1331	1338	1341	1346	1349	1353	1355
1359	1370	1372*	1380*	1394	1398	1401	1409	1418	1421
1425	1426*	1430	1439	1443	1450*	1451	1452*	1454	1463
1469	1478	1481	1482*	1492*	1498*	1499	1505	1509	1511
1518	1522*	1530*	1533	1539	1541	1548*	1559	1570*	1583
1593	1601	1618*	1620*	1626	1636*	1649	1653	1659	1661
1666*	1668*	1673	1679	1685	1692*	1703	1706	1730	1732*
1733	1734	1740*	1745	1746*	1749	1755	1758	1763	1766
1769	1773	1778	1779	1785	1786*	1790	1791	1806	1811
1818	1821	1829	1835	1838	1845	1850	1854	1859	1860*
1863	1866†	1876*	1883	1889	1898	1900*	1901	1906*	1923
1925	1926	1930*	1931	1938	1948*	1953	1955	1958	1959
1961	1965	1972*	1973	1978*	1983	1986*	1994	1996*	

ANEXO II

En este anexo presentamos:

I) El grupo de puntos racionales $E(\mathbb{F}_{2^3})$ de la curva elíptica no supersingular $y^2 + xy = x^3 + x^2 + 1$, donde el campo $\mathbb{F}_{2^3}$, está representado en una base normal óptima y los elementos del grupo son $P_0, ..., P_{13}$, como en 2) de 5.5.1, donde P_0 es la identidad.

$+$	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}	P_{13}
P_1	P_7	P_0	P_8	P_3	P_{12}	P_{10}	P_4	P_2	P_5	P_9	P_6	P_{13}	P_{11}
P_2	P_0	P_8	P_4	P_7	P_9	P_{11}	P_1	P_3	P_{10}	P_6	P_{13}	P_5	P_{12}
P_3	P_8	P_4	P_1	P_0	P_6	P_{12}	P_2	P_7	P_{11}	P_{13}	P_5	P_{10}	P_9
P_4	P_3	P_7	P_0	P_2	P_{11}	P_5	P_8	P_1	P_{13}	P_{12}	P_9	P_6	P_{10}
P_5	P_{12}	P_9	P_6	P_{11}	P_4	P_0	P_{13}	P_{10}	P_7	P_1	P_2	P_3	P_8
P_6	P_{10}	P_{11}	P_{12}	P_5	P_0	P_3	P_9	P_{13}	P_2	P_8	P_4	P_1	P_7
P_7	P_4	P_1	P_2	P_8	P_{13}	P_9	P_3	P_0	P_{12}	P_5	P_{10}	P_{11}	P_6
P_8	P_2	P_3	P_7	P_1	P_{10}	P_{13}	P_0	P_4	P_6	P_{11}	P_{12}	P_9	P_5
P_9	P_5	P_{10}	P_{11}	P_{13}	P_7	P_2	P_{12}	P_6	P_1	P_0	P_8	P_4	P_3
P_{10}	P_9	P_6	P_{13}	P_{12}	P_1	P_8	P_5	P_{11}	P_0	P_2	P_3	P_7	P_4
P_{11}	P_6	P_{13}	P_5	P_9	P_2	P_4	P_{10}	P_{12}	P_8	P_3	P_7	P_0	P_1
P_{12}	P_{13}	P_5	P_{10}	P_6	P_3	P_1	P_{11}	P_9	P_4	P_7	P_0	P_8	P_2
P_{13}	P_{11}	P_{12}	P_9	P_{10}	P_8	P_7	P_6	P_5	P_3	P_4	P_1	P_2	P_0

El grupo $E(\mathbb{F}_{2^3})$ es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_7$, donde P_1 tiene orden 7 y P_{13} es de orden 2. Además $\#E(F_{2^3}) = 7 \cdot 2$

II) Otro grupo de puntos racionales que fue usado es el $E(\mathbb{F}_{2^6})$, con $E : y^2 + xy = x^3 + \beta^{52}x^2 + 1$, donde $\beta = \alpha^{23} = (1 + \alpha^5)$ y α es una raíz de $x^6 + x + 1$, en este caso β genera una BNO. Sin embargo, por espacio solo escribiremos a los puntos racionales de este grupo de la forma (i, j) donde esto significa el punto (β^i, β^j)

(11,25)	(11,45)	(22,12)	(22,5)	(33,6)	(33,24)	(44,6)	(44,5)
(3,2)	(3,41)	(25,40)	(25,27)	(58,20)	(58,19)	(6,20)	(6,40)
(17,47)	(17,21)	(39,15)	(39,40)	(50,23)	(50,41)	(20,14)	(20,36)
(53,55)	(53,5)	(12,58)	(12,2)	(23,22)	(23,61)	(34,20)	(34,54)
(15,63)	(15,2)	(26,37)	(26,29)	(37,36)	(37,12)	(48,63)	(48,50)
(29,12)	(29,19)	(40,58)	(40,4)	(51,36)	(51,38)	(10,50)	(10,45)
(43,24)	(43,16)	(13,42)	(13,56)	(24,48)	(24,49)	(46,17)	(46,60)
(57,33)	(57,58)	(5,47)	(5,26)	(38,50)	(38,19)	(60,47)	(60,45)
(19,11)	(19,8)	(30,6)	(30,31)	(41,41)	(52,15)	(52,48)	(0,11)
(41,0)	$\mathcal{O}$						

Donde 0 es el cero del campo y $\mathcal{O}$ el punto al infinito. Este grupo tiene 74 puntos racionales y es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_{37}$

ANEXO III

En la Actualidad existe la Asociación Internacional para la Investigación de la Criptografía (IACR the International Association for Cryptologic Research). dedicada principalmente a la organización de reuniones internacionales. En seguida presentamos los números de la serie Lecture Notes in Computer Science (LNCS) de Springer Verlag, que publica los artículos presentados en las reuniones antes mencionadas.

Damos también algunas fuentes donde se publican temas relacionados con criptografía, incluyendo revistas y sitios de la WWW.

Lista de los "Proceedings" obtenidos de la reunión anual en la Universidad de Santa Barbara California

- **Advances in Cryptology**: a Report on **CRYPTO 81**, ECE Report No. 82-04, Allen Gersho, Ed. ECE Dpt, UCSB, Santa Barbara, CA 93106.
- **Advances in Cryptology: Proceedings of Crypto 82,**
  D. Chaum, R.L. Rivest, A.T. Sherman, Eds., Plenum NY, 1983.
- **Advances in Cryptology: Proceedings of Crypto 83.**
  D. Chaum Ed., Plenum NY, 1984.
- **Advances in Cryptology: Proceedings of CRYPTO 84,**
  R. Blakley, D. Chaum, Eds., **LNCS 196,** 1985.
- **Advances in Cryptology: CRYPTO'85,**
  H.C. Williams Ed., **LNCS 218,** 1986.
- **Advances in Cryptology: CRYPTO'86,**
  A. M. Odlyzko Ed., **LNCS 263,** 1987.
- **Advances in Cryptology: CRYPTO'87,**
  C. Pomerance Ed., **LNCS 293,** 1988.

- **Advances in Cryptology: CRYPTO'88,**
  S. Goldwasser Ed., **LNCS 403,** 1989.
- **Advances in Cryptology: CRYPTO'89,**
  G. Brassard Ed., **LNCS 435,** 1990.
- **Advances in Cryptology: CRYPTO'90,**
  A. J. Menezes, S. A. Vanstone Eds., **LNCS 537,** 1991.
- **Advances in Cryptology: CRYPTO'91,**
  J. Feigenbaum Ed., **LNCS 576,** 1992.
- **Advances in Cryptology: CRYPTO'92,**
  E. F. Brickell Ed., **LNCS 740,** 1993.
- **Advances in Cryptology: CRYPTO'93,**
  D. R. Stinson Ed., **LNCS 773,** 1994.
- **Advances in Cryptology: CRYPTO'94,**
  Y.G. Desmedt Ed., **LNCS 839,** 1994.
- **Advances in Cryptology: CRYPTO'95,**
  D. Coppersmith Ed., **LNCS 963,** 1995.
- **Advances in Cryptology: CRYPTO'96,**
  N. Koblitz Ed., **LNCS 1109,** 1996.
- **Advances in Cryptology: CRYPTO'97,**
  B. S. Kaliski Ed., **LNCS 1294,** 1997.

Lista de los "Proceedings" publicados en la reunión conocida como EUROCRYPT llevada a cabo cada año a partir de 1982, en una ciudad diferente de Europa

- **Cryptography: Proceedings Burg Feuerstein, 1982,**
  T. Beth Ed., **LNCS 149,** Germany, 1983.
- **Advances in Cryptology: Proceedings of EUROCRYPT 84,**
  T. Beth, N. Cot, I. Ingermarsson Eds., **LNCS 209,** Paris France, 1985.
- **Advances in Cryptology: EUROCRYPT'85,**
  F. Pichler Ed., **LNCS 219,** Linz Austria, 1986.
- **Advances in Cryptology: EUROCRYPT'87,**
  D. Chaum, W.L. Price Eds., **LNCS 304.** Amsterdam The Netherlands. 1988.
- **Advances in Cryptology: EUROCRYPT'88,**
  C. G. Günther Ed., **LNCS 330**, Davos Switzerland, 1988.
- **Advances in Cryptology: EUROCRYPT'89,**
  J.J. Quisquater, J. Vandewalle Eds., **LNCS 434**, Houthalen Belgium, 1990.
- **Advances in Cryptology: EUROCRYPT'90,**
  I.B. Damgard Ed., **LNCS 473**, Aarhus Denmark. 1991.
- **Advances in Cryptology: EUROCRYPT'91,**
  D.W. Davies Ed., **LNCS 547**. Brighton United Kingdom. 1991.
- **Advances in Cryptology: EUROCRYPT'92,**
  R.A. Rueppel Ed., **LNCS 658**. Balatonfüred Hungaria. 1993.
- **Advances in Cryptology: EUROCRYPT'93,**
  T. Helleseth Ed., **LNCS 765**. Lofthus Norway. 1994.

- **Advances in Cryptology: EUROCRYPT'94,**
  A. DeSantis Ed., **LNCS 950**, Perugia Italy, 1995.
- **Advances in Cryptology: EUROCRYPT'95,**
  L.C. Guillou, J.J. Quisquater Eds., **LNCS 921**, Saint-Malo France, 1995.
- **Advances in Cryptology: EUROCRYPT'96,**
  U. Maurer Ed., **LNCS 1070**, Saragossa Spain, 1996.
- **Advances in Cryptology: EUROCRYPT'97,**
  W. Fumy Ed., **LNCS 1233**, Konstanz Germany, 1997.

Lista de la serie LNCS de reuniones realizadas en Asia y Australia

- **Advances in Cryptology: AUSCRYPT'90,**
  J. Seberry, J. Pieprzyk Eds., **LNCS 453**, 1990.
- **Advances in Cryptology: ASIACRYPT'91,**
  H. Imai, R.L. Rivest, T. Matsumoto Eds., **LNCS 739**, 1993.
- **Advances in Cryptology: AUSCRYPT'92,**
  J. Seberry, Y. Zheng Eds., **LNCS 718**, 1993.
- **Advances in Cryptology: ASIACRYPT'94,**
  J. Pieprzyk R. Safavi-Naini Eds., **LNCS 917**, 1995.
- **Advances in Cryptology: ASIACRYPT'96,**
  K. Kim, T. Matsumoto., **LNCS 1163**, 1996.

En seguida se ofrece otra lista de la serie LNCS que contiene excelentes artículos relacionados con criptografía

Conferencia Fast Software Encryption

- **Fast Software Encryption: Cambridge Security Workshop,**
  R. Anderson Ed., **LNCS 809** Cambridge UK, 1994.
- **Fast Software Encryption: Second International Workshop,**
  B. Preneel Ed., **LNCS 1008**, Leuven Belgium, 1995.
- **Fast Software Encryption: Third International Workshop,**
  D. Gollmann Ed., **LNCS 1039**, Cambridge UK, 1995.

Conferencia Algorithmic Number Theory

- **Algorithmc Number theory: First International Symposium, ANTS-I,**
  L.M. Adleman, M. Huang Eds., **LNCS 877**, 1994.
- **Algorithmc Number Theory: Second International Symposium, ANTS-II,**
  H. Cohen Ed., **LNCS 1122,** Talence France, 1996.

Conferencias relacionadas con criptografía

- **Distributed Programming Paradigms with Cryptography Applications,**

  J. S. Greenfield, **LNCS 870**, 1994.

- **Integrity Trimitives for Secure Information Systems,**

  A. Bosselaers, B. Preneel Eds., **LNCS 1007**, 1995.

- **Cryptography and Coding,**

  C. Boyd Ed., **LNCS 1025**, 1995.

- **Cryptography: Policy and Algorithms,**

  E. Dawson, J. Golic Eds., **LNCS 1029**, 1996.

- **Computer Security- ESORICS 96,**

  E. Bertino, H. Kurth, G. Martella E. Mintolivo Eds., **LNCS 1146**, 1996.

- **Security Protocols,**

  M. Lomas Ed., **LNCS 1189**, 1997.

- **Information Security and Privacy.**

  V. Varadharajan, J. Pieprzyk Eds., **LNCS 1270**, 1997.

En la actualidad existen revistas periódicas, además de la serie LNCS, que publican temas predominantemente sobre criptografía. Las más importantes de éstas son:

- **Journal of Cryptology,**

  Publicada por IACR.

- **CryptoBytes,**

  Publicada por RSA Data Security, Inc.

- **Designs, Codes and Cryptography.**
  Publicada por Kluwer Academic Publishers.

Sitios en WWW que se relacionan con criptografía

- **http://theory.lcs.mit.edu/~rivest**
- **http://www.iacr.org/**
- **http://www.swcp.com/~iacr**
- **http://www.rsa.com**
- **http://www.certicom.com**
- **http://www.digicash.com**
- **http://www.first.org/**
- **http://www.cryptography.com/**
- **http://www.cs.hut.fi/crypto**

Bibliografía

[1] Álgebra

[1.1] "A Classical Introduction Modern Number Theory", **Rosen M., Ireland K.,** *Springer Verlag GTM 84, 1981.*

[1.2] "Elementary Number Theory and Its Applications", **Rosen K.H.**, *Addison Wesley Publishing Company, 1988.*

[1.3] "A First Course in Rings and Ideals", **Burton D.**, *Reading Addison Wesley, 1970.*

[1.4] "A Concise Introduction to the Theory of Numbers", **Baker A.,** *Cambridge University Press, 1984.*

[1.5] "Basic Abstract Algebra", **Bhattacharya P.B., Jain S.K., Nagpaul S.R.,** *Cambridge University Press, 1986.*

[1.6] "Introducción al Algebra Conmutativa", **Atiyah M.F., Macdonald I.G.,** *Reverté, 1989.*

[1.7] "Recreations in Theory of Numbers", **Beiler A.H.,** *Dover Publications Inc., 1964.*

[1.8] "Algebra Abstracta", **Fraleigh J.B.,** *Addison Wesley Iberoamericana, 1987.*

[1.9] "Topics from the Theory of Numbers", **Grosswald E.**, *Birkhäuser, 1984.*

[1.10] "Fundamental Concepts of Higher Algebra", **Albert A.A.**, *The University of Chicago Press, 1956.*

[2] Campos finitos

[2.1] "Finite Fields", **Lidl R., Niederreiter H.**, *Encyclopedia of Mathematics and its Applications Vol. 20, Addison Wesley Publishing Company, 1983.*

[2.2] "Introduction to Finite Fields and their Applications", **Lidl R., Niederreiter H.**, *Cambridge University Press, 1986.*

[2.3] "Applications of Finite Fields", **Blake I.F., Gao X., Menezes A.J., Mullin R.C., Vanstone S.A., Yaghoobian T.**, *Kluwer Academic Publishers, 1992.*

[2.4] "Finite Fields for Computer Scientists and Engineers", **McEliece R.J.**, *Kluwer Academic Publishers, 1987.*

Bases en campos finitos

[2.5] "Primitive Normal Bases for Finite Fields", **Lenstra H.W. Jr., Schoof R.J.**, *Mathematics of Computation Vol. 48, No. 177, 1987, pp. 217-231.*

[2.6] "Normal Bases of Finite Field $GF(2^n)$", **Omura J.K., Pei D.Y., Wang C.C.**, *IEEE Transactions on Information Theory Vol. IT-32, No. 2, 1986, pp. 285-287.*

[2.7] "Optimal Normal Bases in $GF(p^n)$.", **Mullin R.C., Onyszchuk I.M., Vanstone S.A., Wilson R.M.**, *Discrete Applied Mathematics Vol. 22, 1988/89, pp. 149-161.*

[2.8] "Low Complexity Normal Bases", **Ash D.W., Blake I.F., Vanstone S.A.**, *Discrete Applied Mathematics Vol. 25, 1989, pp. 191-210.*

[2.9] "Normal and Self-Dual Normal Bases From Factorization of $cx^{q-1} + dx^q - ax - b$.", **Blake I.F., Gao S., Mullin R.C.**, *SIAM J. Discrete Mathematics Vol. 7 No. 3, 1994, pp. 499-512.*

Operaciones sobre campos finitos

[2.10] "Arithmetic Operations in $GF(2^n)$.", **Agnew G.B., Beth T., Mullin R.C., Vanstone S.A.,** *Journal of Cryptology Vol. 6, 1993, pp. 3-13.*

[2.11] "A Method for Computing Addition Tables in $GF(p^n)$.", **Imamura K.,** *IEEE Transactions on Information Theory Vol. IT-26, No. 3, 1980, pp. 367-369.*

[2.12] "Fast Exponentiation in $GF(2^n)$.", **Agnew G.B., Mullin R.C., Vanstone S.A.,** *Advances in Cryptology Eurocrypt'88, LNCS 330, 1988, pp. 251-255.*

[2.13] "Some Observations on Parallel Algorithms for Fast Exponentiation in $GF(2^n)$.", **Stinson D.R.,** *SIAM Journal on Computing Vol. 19 No. 4, 1990, pp. 711-717.*

[2.14] "Computing Powers in Parallel", **Gathen J.V.Z.,** *SIAM Journal on Computing Vol. 16 No. 5, 1987, pp. 930-945.*

[2.15] "A Simple and Fast Probabilistic Algorithm for Computing Square Roots Modulo a Prime Number", **Peralta R.C.,** *IEEE Transactions on Information Theory, Vol. IT-32 No. 6, 1986, pp. 846-847.*

Polinomios irreducibles en campos finitos

[2.16] "On Primitive Trinomials (Mod 2), II", **Zierler N.,** *Information and Control Vol. 14, 1969, pp. 566-569.*

[2.17] "Primitive Trinomials Whose Degree is a Mersenne Exponent", **Zierler N.,** *Information and Control Vol. 15, 1969, pp. 67-69.*

[2.18] "On $x^n + x + 1$ over $GF(2)$.", **Zierler N.,** *Information and Control Vol. 16, 1970, pp. 502-505.*

[2.19] "On Trinomials $x^n + x^2 + 1$ and $x^{8l\pm3} + x^k + 1$ Irreducible over $GF(2)$.", **Fredricksen H., Wisniewski R.,** *Information and Control Vol. 50, 1981, pp. 58-63.*

[2.20] "Primitive Normal Polynomials Over Finite Fields", **Morgan I.H., Mullen G.L.,** *Mathematics of Computation Vol. 63 No. 208, 1994, pp. 759-765.*

[2.21] "Table of Primitive Binary Polynomials II", **Zivkovic M.,** *Mathematics of Computation Vol. 63 No. 207, 1994, pp. 301-306.*

[2.22] "Primitive Polynomials and M-Sequences Over $GF(q^m)$.", **Komo J.J., Lam M.S.,** *IEEE Transactions on Information Theory Vol. 39 No. 2, 1992, pp. 647.*

Factorización en campos finitos

[2.23] "Factoring Polynomials Over Large Finite Fields", **Berlkamp E.R.**, *Mathematics of Computation Vol. 24 No. 111, 1970, pp. 713-735.*

[2.24] "On a New Factorization Algorithm for Polynomials Over Finite Fields", **Niederreiter H., Göttfert R.**, *Mathematics of Computation Vol. 64 No. 209, 1995, pp. 347-353.*

[2.25] "Critères D'irréductibilite des Polynômes Composés à Coefficients dans un Corps Fini", **Agou S.**, *Acta Arithmetica XXX, 1976, pp. 213-223.*

[2.26] "Polynômes sur un Corps Fini", **Agou S.,** *Bull. Sc. math., 2ª série Vol. 95, 1971, pp. 327-330.*

[2.27] "A Method of Factoring and the Factorization of F_7.", **Morrison M., Brillhart J.**, *Mathematics of Computation Vol. 29 No. 129, 1975, pp. 183-205.*

[2.28] "Improving an Algorithm for Factoring Polynomials Over a Finite Field and Constructing Large Irreducible Polynomials", **Camion P.F.**, *IEEE Transactions on Information Theory, Vol. IT-29 No. 3, 1983, pp. 378-385.*

[2.29] "Probabilistic Algorithms in Finite Fields", **Rabin M.O.,** *SIAM Journal on Computing Vol. 9 No. 2, 1980, pp. 273-280.*

Polinomios permutación sobre campos finitos

[2.30] "A Characterization of Permutation Polynomials Over a Finite Field", **Carlitz L., Lutz A. J.,** *American Mathematical Monthly Vol. 38, 1978, pp. 746-748.*

[2.31] "When Does a Polynomial Over a Finite Field Permute the Elements of the Field?", **Lidl R., Mullen G.L.,** *University of Tasmania Hobart, Tasmania 7001, Australia.*

[2.32] "Test for Permutation Polynomials", **Gathen J.V.Z.,** *SIAM Journal on Computing Vol. 20 No. 3, 1991, pp. 591-602.*

Otros tópicos

[2.33] "Why Study Equations over Finite Fields", **Koblitz N.,** *Mathematics Magazine Vol. 55 No. 3, 1982, pp. 144-149.*

[2.34] "A Geometric Approach to Root Finding in GF(q^m)." **Oorschot P.C.V., Vanstone S.A.,** *IEEE Transactions on Information Theory Vol. 35 No. 2, 1989, pp. 444-453.*

[2.35] "Subgroup Refinement Algorithms for Root Finding in GF(q)", **Menezes A.J., Oorschot P.C.V., Vanstone S.A.,** *SIAM Journal on Computing Vol. 21 No.2, 1992, pp. 228-239.*

[3] Problema del Logaritmo Discreto

[3.1] "Discrete Logarithms and Smooth Polynomials", **Odlyzko A.M.,** *Contemporary Mathematics Vol. 168, 1994, pp. 269-278.*

[3.2] "The Function Field Sieve", **Adleman L.M.,** *University of Southern California, 1995.*

[3.3] "Discrete logarithms in GF(p) Using the Number Field Sieve", **Gordon D.M.,** *SIAM Journal on Discrete Mathematics Vol. 6 No. 1, 1993, pp. 124-138.*

[3.4] "Fast, Rigorous Factorization and Discrete Logarithm Algorithms", **Pomerance C.,** *Department of Mathematics, The University of Georgia Athens, Georgia 30602, USA 1978.*

[3.5] "A Subexponential Algorithm for Discrete Logarithms", **Adleman L.M., Demarrais L.,** *Mathematics of Computation Vol. 61 No. 203, 1993, pp. 1-15.*

[3.6] "Rigorous, Subexponential Algorithms for Discrete Logarithms over Finite Fields", **Lovorn R.,** *Ph.D. Thesis, University of Georgia, 1992.*

[3.7] "Computation of Discrete Logarithms in Prime Fields", **LaMacchia B. A., Odlyzko A.M.,** *Designs, Codes and Cryptography Vol. 1, 1991, pp. 47-62.*

[3.8] "Discrete Logarithms in $GF(p)$", **Coppersmith D., Odlyzko A.M., Schroeppel R.,** *Algorithmica Vol. 1, 1986, pp. 1-15.*

[3.9] "Discrete Logarithms and Factoring", **Bach E.,** *Report No. UCB/CSD 84/186, University of California Berkeley, California 94720.*

[3.10] "On the Complexity of Computing Discrete Logarithms and Factoring Integers", **Odlyzko A.M.,** *Bell Laboratories Murray Hill, New Jersey 07974.*

[3.11] "Discrete Logarithms in Finite Fields and their Cryptographic Significance", **Odlyzko A.M.,** *Advances in Cryptology Eurocrypt'84, LNCS 209, 1985, pp. 224-314.*

[3.12] "A Subexponential-Time Algorithm for Computing Discrete Logarithms over $GF(p^2)$", **ElGamal T.,** *IEEE Transactions on Information Theory Vol. IT-31, No. 4, 1985, pp. 473-481.*

[3.13] "Fast Evaluation of Logarithms in Fields of Characteristic Two", **Coppersmith D.,** *IEEE Transactions on Information Theory Vol. IT-30 No. 4, 1984, pp. 587-597.*

[3.14] " Monte Carlo Method for Index Computation (mod p)", **Pollard J.M.,** *Mathematics of Computation Vol. 32 No. 143, 1978, pp. 918-924.*

[3.15] "An Improved Algorithm for Computing Logarithms over $GF(p)$ and Its Cryptographic Significance", **Pohlig S.C., Hellman M.E.,** *IEEE Transactions on Information Theory Vol. IT-24 No. 1, 1978, pp. 106-110.*

[3.16] "A Polynomial Form for Logarithms Modulo a Prime", **Wells A.L. Jr.**, *IEEE Transactions on Information Theory Vol. IT-30 No. 6, 1984, pp. 845-846.*

[3.17] "On Computing Logarithms over $GF(2^p)$.", **Herlestam T., Johanneson R.**, *BIT Bol. 21, 1981, pp. 326-334.*

[3.18] "Diffie-Hellman is as Strong as Discrete Log for Certain Primes", **Boer B.**, *Advances in Cryptography Crypto'88, LNCS 403, 1990, pp. 530-539.*

[3.19] "Polylog Depth Circuits for Integer Factoring and Discrete Logarithms", **Sorenson J.**, *Information and Computation Vol. 110, 1994, pp. 1-18.*

Sistemas dispersos

[3.20] "On The Asymptotic Complexity of Matrix Multiplication", **Coppersmith D., Winograd S.**, *SIAM Journal of Computing Vol. 11 No. 3, 1982, pp. 472-492.*

[3.21] "Solving Linear Equations over $GF(2)$: Block Lanczos Algorithm", **Coppersmith D.**, *Linear Algebra and Its Applications Vol. 192, 1993, pp. 33-60.*

[3.22] "Solving Homogeneous Linear Equations over $GF(2)$ via Block Wiedemann Algorithm", **Coppersmith D.**, *Mathematics of Computation Vol. 62 No. 205, 1994, pp. 333-350.*

[4] Multiplicadores

[4.1] "VLSI Design for Exponentiation in $GF(2^n)$.", **Geiselmann W., Gollmann D.**, *Advances in Cryptology Auscrypt 90, LNCS 453, 1990, pp. 398-405.*

[4.2] "Systolic Architectures for Multiplication over Finite Field $GF(2^m)$.", **Diab M.,** *Laboratoire AAECC/LSI, IRIT, Université Paul Sabatier, 118 Route de Narbonne, 31062 Toulouse cedex, FRANCE.*

[4.3] "A New Bit-Serial Systolic Multiplier over $GF(2^m)$.", **Zhou B.B.,** *IEEE Transactions on Computers Vol. 37 No. 6, 1988, pp. 749-751.*

[4.4] "A VLSI Design of a Pipeline Reed-Salomon Decoder", **Deutsch L.J., Reed I.S., Shao H.M., Truong T.K., Yuen J.H.**, *IEEE Transaction on Computer Vol. c-34 No. 5, 1985, pp. 393-403.*

[4.5] "Systolic VLSI Arrays for Polynomial GCD Computation", **Brent R.P., Kung H.T.**, *IEEE Transaction on Computer Vol. c-33 No. 8, 1984, pp. 731-736.*

[4.6] "New Multipliers Modulo 2^n-1.", **Rao P.B., Skavantzos A.,** *IEEE Transactions on Computers Vol. 41 No. 8, 1992, pp. 957-961.*

[4.7] "VLSI Architectures for Computing Multiplications and Inverse in $GF(2^m)$.", **Deutsch L.J., Omura J.K., Reed I.S., Shao H.M., Truong T.K., Wang C.C.**, *IEEE Transaction on Computer Vol. c-34 No. 8, 1985, pp. 709-717.*

[4.8] "Systolic Multipliers for Finite Fields $GF(2^m)$.", **Reed I.S., Truong T.K., Yeh C.S.**, *IEEE Transaction on Computer Vol. c-33 No. 4, 1984, pp. 357-360.*

[5] Criptografía Aplicada

[5.1] "A course in Number Theory and Cryptography", **Koblitz N.**, *Springer Verlag GTM 114, 1987.*

[5.2] "Number Theory and Cryptography", **Cloxton J.H.** (Editor), *London Mathematical Society Lecture Notes Series 154, Cambridge University Press, 1990.*

[5.3] "An Introduction to Crptology", **Tilborg H.C.A.V.**, *Kluwer Academic Publishers, 1988.*

[5.4] "Introduction to Cryptology", **Beckett A.**, *Blackwell Scientific Publications, 1988.*

[5.5] "Primality and Cryptology", **Kranakis E.**, *John Wiley & Sons, 1987.*

[5.6] "Public-Key Crytology", **Salomaa A.**, *Monographs on Theoretical Computer Science Vol. 23, Springer Verlag, 1990.*

[5.7] "Mathematical Cryptology", **Patterson W.**, *Rowman & Littlefield, 1987.*

[5.8] "Public-Key cryptography State of the Art and Future Directions", **Beth Th., FrischM., Simmons G.L.**, (Eds.), *LNCS No. 578, 1991.*

[5.9] "Cryptology and Computational Number Theory", **Lagarias G.S., Lenstra A.K.**, *Proceeding of Simposia in Applied Mathematics Vol. 42, 1990.*

[5.10] "Distributed Computing and Cryptography", **Feigenbaum J.,Merritt M.**, (Eds.), *DIMACS Vol. 2, 1989.*

[5.11] "Codes, Ciphers and Secret Writing", **Gardner M.**, *Dover Publications, Inc., 1972.*

[5.12] "Cryptograms and Spygrams", **Gleason M.**, *Dover Publications, Inc., 1981.*

[5.13] "Cryptology", **Simmons G.J.**, *The New Encyclopaedia Britannica, Macropaedia, Vol. 16, pp. 913-924B.*

[5.14] "New Directions in Cryptography", **Diffie W., Hellman M.E.,** *IEEE Transactions on Information Theory, Vol. IT-22 No. 6, 1976, pp. 644-654.*

[5.15] "The First Ten Years of Public-Key Cryptography", **Diffie W.**, *Proceedings of the IEEE Vol. 76 No. 5, 1988, pp. 560-577.*

[5.16] "Public Key Cryptography", **Odlyzko A.M.,** *AT&T Technical Journal Sep./Oct., 1994, pp. 17-23.*

[5.17] "Public Key Cryptography", **Odlyzko A.M.,** *AT&T Bell Laboratories, Murray Hill, New Jersey 0797, 1993.*

[5.18] "Cryptography", **Coppersmith D.**, *IBM J. Res. Develop. Vol. 31 No. 2, 1987, pp. 244-248.*

[5.19] "An Introduction to Contemporary Cryptology", **Massey J.L.**, *Proceedings of the IEEE Vol. 76 No. 5, 1988, pp. 533-549.*

[5.20] "Course d'Algorithmique et Cryptographie", **Harari S.,** *pre-print 1994.*

[5.21] "Security Technologies", **Brooks T. A., Kaplan M. M.**, *AT&T Technical Journal Sep./Oct., 1994, pp. 4-8.*

Criptoanálisis

[5.22] "Cryptoanalysis: A Survey of Recent Results", **Brickell E.F., Odlyzko A.M.,** *Proceedings of the IEEE Vol. 76 No. 5, 1988, pp. 578-583.*

[5.23] "An Introduction to Cryptanalysis", **Siil K.A.**, *AT&T Technical Journal Sep./Oct. 1994, pp. 24-29.*

[5.24] "To Decode Short Cryptograms", **Hart G.W.**, *Communications of the ACM Vol. 37 No. 9, 1994, pp. 56-65.*

[5.25] "Cryptanalysis and Protocol Failures", **Simmons G.J.,** *Communications of the ACM Vol. 37 No. 11, 1994, pp. 56-65.*

[5.26] "Protocol Failures in Cryptosystems", **Moore J.H.,** *Proceedings of the IEEE Vol. 76 No. 5, 1988, pp. 594-602.*

[5.27] "A Cryptanalytic Time-Memory Trade-Off", **Hellman M.E.,** *Transactions on Information Theory Vol. IT-26 No. 4, 1980, pp. 401.406.*

[5.28] "On the Security of Public Key Protocols", **Dolev D., Yao A.C.,** *IEEE Transactions on Information Theory Vol. IT-29 No. 2, 1983, pp. 198-208.*

[5.29] "On Secrecy Systems with Side Information about the Message Available to a Cryptanalyst", **Lu S.C.,** *IEEE Transactions on Information Theory Vol. IT-25 No. 4, 1979, pp. 472-475.*

[5.30] "Hiding Information and Signatures in Trapdoor Knapsacks", **Merkle R.C., Hellman M.E.,** *IEEE Transaction on Information Theory Vol. IT-24 No. 5, 1978, pp. 525-530.*

[5.31] "A Polynomial-Time Algorithm for Breaking the Basic Merkle-Hellman Cryptosystem", **Shamir A.,** *IEEE Transaction on Information Theory Vol. IT-30 No. 5, 1984, pp. 699-704.*

[5.32] "Cryptanalytic Attacks on the Multiplicative Knapsack Cryptosystem and on Shamir's Fast Signature Scheme", **Odlyzko A.M.,** *IEEE Transaction on Information Theory Vol. IT-30 No. 4, 1984, pp. 594-601.*

[5.33] "A Critical Analysis of the Security of Knapsack Public-Key Algorithms", **Desmendt Y.G., Govaerts R.J.M., Vandewalle J.P.,** *IEEE Transactions on Information Theory Vol. IT-30 No. 4, 1984, pp. 601-611.*

[5.34] "On the Security of the Merkle-Hellman Cryptographic Scheme", **Shamir A., Zippel R.,** *IEEE Transactions on Information Theory Vol. IT-26 No. 3, 1980, pp. 339-340.*

Otros tópicos

[5.35] "A Survey of Information Authentication", **Simmons G.L.,** *Proceedings of the IEEE Vol. 76 No. 5, 1988, pp. 603-620.*

[5.36] "Concerning Certain Linear Transformation Apparatus of Cryptography", **Hill L.S.,** *American Mathematical Montly Vol. 38, 1931, pp. 135-154.*

[5.37] "The Mathematics of Public-Key Cryptography", **Hellman M.E.,** *Scientific American Vol. 241-2, 1979, pp. 130-139.*

[5.38] "The Commercial Data Masking Facility (CDMF) data privacy algorithm", **John-son D.B., Matyas S.M., Le A.V., Wilkins J.D.,** *IBM J. Res. Develop. Vol. 38 No. 2, 1994, pp. 217-226.*

[5.39] "Deciphering a Linear Congruential Encryption", **Knuth D.E.,** *IEEE Transactions on Information Theory Vol. IT-31 No. 1, 1985, pp. 49-52.*

[5.40] "An efficient Solution of the Congruence $x^2 + ky^2 \equiv m$ *modn.*",**Pollard J.M., Schnorr C.P.,** *IEEE Transactions on Information Theory Vol. IT-33 No. 5, 1987, pp. 702-709.*

[5.41] "An Extension of the Shannon Theory Approach to Cryptography", **Hellman M.E.,** *IEEE Transactions on Information Theory Vol. IT-23 No. 3, 1977, pp. 289-294.*

[5.42] "Privacy and Authentication on a Portable Communications System", **Beller M.J., Chang L.F., Yacobi Y.,** *IEEE Journal on Selected Areas in Communications Vol. 11 No. 6, 1993, pp. 821-829.*

[5.43] "A Note on the Complexity of Cryptography", **Brassard G.,** *IEEE Transactions on Information Theory Vol. IT-25 No. 2, 1979, pp. 232-233.*

[5.44] "Cryptographic Systems Using Redundancy", **Agnew G.B.,** *IEEE Transactions on Information Theory Vol. 36 No. 1, 1990, pp. 31-39.*

[5.45] "Relativized Cryptography", **Brassard G.,** *IEEE Transactions on Information Theory Vol. IT-29 No. 6, 1983, pp. 877-893.*

[5.46] "Secret Key Agreement by Public Discussion From Common Information", **Maurer U.M.,** *IEEE Transactions on Information Theory Vol. 39 No. 3, 1993, pp. 733-742.*

[5.47] "Bounds on Key Equivocation for Simple Substitution Ciphers", **Blom R.J.,** *IEEE Transactions on Information Theory Vol. IT-25 No. 1, 1979, pp. 8-18.*

[5.48] "A Fair Protocol for Signing Contracts", **Ben-or M., Goldreich O., Micali S., Rivest R.L.,** *IEEE Transactions on Information Theory Vol. 36 No. 1, 1990, pp. 40-46.*

[5.49] "Deliberate Noise in a Modern Cryptographic System", **Willett M.,** *IEEE Transactions on Information Theory Vol. IT-26 No. 1, 1980, pp. 102-105.*

[5.50] "A Modular Approach to Key Safeguarding", **Asmuth C., Bloom J.,** *IEEE Transactions on Information Theory Vol. IT-29 No. 2, 1983, pp. 208-210.*

[6] Criptosistema RSA

[6.1] "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", **Rivest R.L., Shamir A., Adleman L.,** *Communication of the ACM Vol. 21 No. 2, 1978, pp. 120-126.*

[6.2] "A Modification of the RSA Public-Key Encryption Procedure", **Williams H. C.,** *IEEE Transactions on Information Theory Vol. IT-26 No. 6, 1980, pp. 726-729.*

[6.3] "Short RSA Key and Their Generation", **Vanstone S.A., Zuccherato R.J.,** *Dept. of Combinatorics and Optimization University of Waterloo, Ontario, N2L 3G1, Canada, 1995.*

[6.4] "High-Speed RSA Implementacion", **Koc C.K.,** *RSA Laboratories , RSA Data Security, Inc., 100 Marine Parkway City, CA 94065, 1995.*

[6.5] "RSA Key Generation and Strong Primes", *An RSA Laboratories Seminar, RSA Data Security, Inc., 1995.*

[6.6] "Distributed Programming Paradigms with Cryptography Applications", **Greenfield J.S.,** *LNCS 970, 1994.*

[6.7] "Parameter Selection for Sever-Aided RSA Computation Schemes", **Burns J., Mitchell C. J.,** *IEEE Transactions on Computer Vol. 43 No. 2, 1994, pp. 163-229.*

[6.8] "On Using RSA with Low Exponent in a Public Key Network", **Hastad J.,** *Advances in Cryptology Crypto'85, LNCS 218, 1985, pp. 403-408.*

[6.9] "A Chosen Text Attack on the RSA Cryptosystem and some Discrete Logarith Schemes", **Desmedt Y., Odlyzko A.M.,** *Aangesteld Navorser NFWO, Katholieke Universiteit Leuven, Laboratorium ESAT B-3030 Heverlee, Belgium and AT&T Bell LAboratories, Murray Hill, NJ 07974, USA.*

[6.10] "Implementing the Rivest Shamir and Adleman Public Key Encryption Algorithm on a Standard Digital Signal Processor", **Barrett P.,** *Advances in Cryptology Crypto'86, LNCS 263, 1986, pp. 302-323.*

[6.11] "Finding Four Million Large Random Primes", **Rivest R.,** *Advances in Cryptology Crypto'90 LNCS 537, 1990, pp. 625-626.*

[6.12] "Fast Generation of Secure RSA-Moduli with Almost Maximal Diversity", **Maurer U.,** *Advances in Cryptology Eurocrypt '89, LNCS 434, 1990, pp. 636-647.*

[6.13] "VICTOR, An Efficient Hardware Implementation", **Orup H., Svendsen E., Andreasen E.,** *Advances in Cryptology Eurocrypt '90, LNCS 473, 1990, pp. 245-251.*

[6.14] "A Survey of Hardware Implementations of RSA", **Brickell E.,** *Advances in Cryptology Crypto '89, LNCS 435, 1989, pp. 368-370.*

[6.15] "Fast RSA-hardware: Dream or Reality?", **Hoornaert F.,** *Advances in Cryptology Eurocrypt '88, LNCS 330, 1988, pp. 257-264.*

[6.16] "A Complete Single Chip RSA Device", **Rankine G.,** *Advances in Cryptology Crypto '86, LNCS 263, 1986, pp. 480-487.*

[6.17] "Strong Primes are Easy to Find", **Gordon J.,** *Advances in Cryptology Eurocrypt '84, LNCS 209, 1984, pp. 216-223.*

[6.18] "Some Remarks Concerning the MIT Public-Key Cryptosystem", **Williams H.C., Schmid B.,** *BIT Vol. 19, 1979, pp. 525-538.*

[6.19] "Properties of the Euler Totient Function Modulo 24 and Some of Its Cryptographic Implications", **Gorgui–Naguib R.N., Satnam S.D.,** *Advances in Cryptology Eurocrypt 88, LNCS 330, 1988, pp. 267-274.*

[7] Criptografía Elíptica

[7.1] "Elliptic Curve Public Key Cryptosystems", **Menezes A.,** *Kluwer Academic Publishers, 1993.*

[7.2] "Elliptic Curve Cryptosystems", **Koblitz N.,** *Mathematics of Computation Vol. 48 No. 177, 1987, pp. 203-209.*

[7.3] "Use of Elliptic Curves in Cryptography", **Miller V.S.,** *Advances in Cryptology Crypto'85, LNCS 218, pp. 417-426.*

[7.4] "Elliptic Curve Cryptosystems and Their Implementation", **Menezes A.J., Vanstone S.A.,** *Journal of Cryptology Vol. 6, 1993, pp. 209-224.*

[7.5] "Constructing Elliptic Curve Cryptosystems in Characteristic 2", **Koblitz N.,** *Advances in Cryptology Crypto '90, LNCS 537, 1991, pp. 156-167.*

[7.6] "Elliptic Curve Systems", **Menezes A.J., Qu M., Vanstone S.A.,** *IEEE P1363, part 6, 1995, Draft.*

[7.7] "An Implementacion of Elliptic Curve Cryptosystems over $F_{2^{155}}$.", **Agnew G.B., Mullin R.C., Vanstone S.A.,** *IEEE Journal on Selected Areas in Communications Vol. 11 No. 5, 1993, pp. 804-813.*

[7.8] "The Implementation of Elliptic Curve Cryptosystems", **Menezes A.J., Vanstone S.A.,** *Advances in Cryptology Auscrypt '90, LNCS 453, 1990, pp. 2-13.*

[7.9] "Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field", **Menezes A.J., Okamoto T., Vanstone S.A.,** *IEEE Transactions on Information Theory Vol. 39, No. 5, 1993, pp. 1639-1646.*

[7.10] "CM-Curves with Good Cryptographic Properties", **Koblitz N.,** *Advances in Cryptology Crypto '91, LNCS 576, 1992, pp. 279-287.*

[7.11] "Non Supersingular Elliptic Curves for Public Key Cryptosystems", **Beth T., Schaefer F.,** *Advances in Cryptology Eurocrypt '91, LNCS 547, 1991, pp. 316-327.*

[7.12] "Elliptic Curve Cryptosystems Immune to Any Reduction into the Discrete Logarithm Problem", **Miyaji A.,** *IEICE Trans. Fundamentals Vol. E76-A No.1, 1993, pp. 50-54.*

[7.13] "Elliptic Curves Suitable for Cryptosystems", **Miyaji A.,** *IEICE Trans. Fundamentals Vol. E77-A No. 1, 1994, pp. 98-104.*

[7.14] "On Implementing Elliptic Curve Cryptosystems", **Kit C. Y., Lidl R.,** *Contributions to General Algebra Vol. 6, pp. 155-166.*

[7.15] "Building Cyclic Elliptic Curves Modulo Large Primes", **Morain F.,** *Advances in Cryptology Eurocrypt'91, LNCS 547, 1991, pp. 328-335.*

[7.16] "New Public-Key Schemas Based on Elliptic Curves over the Ring $\mathbb{Z}_n$.", **Koyama K., Maurer U.M., Okamoto T., Vanstone S.A.,** *Advances in Cryptology Crypto'91, LNCS 576, 1992, pp. 252-266.*

[7.17] "A New Elliptic Curves Based Analogue of RSA", **Demytko N.,** *Advances in Cryptology Eurocrypt'93, LNCS 765, 1992, pp. 40-49.*

[7.18] "A Signed Binary Window Method for Fast Computing over Elliptic Curves", **Koyama K., Tsuruoka Y.,** *Advances in Cryptology Crypto'92, LNCS 740, 1992, pp. 345-357.*

[7.19] "An Efficient Digital Signature Schema Based on an Elliptic Curve over the Ring $\mathbb{Z}_n$.", **Fujioka A., Fujisaki E., Okamoto T.,** *Advances in Cryptology Crypto'92, LNCS 740, 1992, pp. 54-65.*

[7.20] "Fast RSA-type Schemes Based on Singular Cubic Curves $y^2 + axy \equiv x^3 \,(\, mod\, n)$.", **Koyama K.,** *Advances in Cryptology Eurocrypt'95, LNCS 921, 1995, pp. 329-339.*

[7.21] "Low Exponent Attack Against Elliptic Curve RSA", **Kurosawa K., Okada K., Tsujii S.,** *Information Processing Letters Vol. 53, 1995, pp. 77-83.*

[7.22] "One-Way Permutations on Elliptic Curves", **Kaliski Jr. B.S.,** *Journal of Cryptology Vol. 3, 1991, pp. 187-199.*

[7.23] "Elliptic Curve Implementation of Zero-Knowledge Blobs", **Koblitz N.,** *Journal of Cryptology Vol. 4, 1991, pp. 207-213.*

[7.24] "A Pseudo-Random Bit Generator Based on Elliptic Logarithm", **Kaliski Jr. B.S.,** *Advances in Cryptology Crypto'86, LNCS 263, 1987, pp. 84-103.*

[7.25] "A Note on Cyclic Groups, Finite Fields, and the Discrete Logarithm Ploblem", **Menezes A.J., Vanstone S.A.,** *Applicable Algebra in Engineering, Communication and Computing Vol. 3, 1992, pp. 67-74.*

[8] Criptografía Hiperelíptica

[8.1] "Hyperelliptic Cryptosystems", **Koblitz N.**, *Journal of Cryptology Vol. 1, 1989, pp. 139-150.*

[8.2] "A Subexponential Algorithm for Discrete Logarithms over the Racional Subgroup of the Jacobians of Large Genus Hyperelliptic Curves over Finite Fields", **Adleman L. M., DeMarrais J., Huang M.**, *Department of Computer Science, University of Southern California, Los Angeles CA 90089, 1995.*

[8.3] "Efficient Algorithms for the Construction of Hyperelliptic Cryptosystems", **Okamoto T., Sakurai K.**, *Advances in Cryptology Crypto'91 LNCS 576, 1992, pp. 267-278.*

[8.4] "On The Complexity of Hyperelliptic Discrete Logarithm Problem", **Shizuya H.**, *Advances in Cryptology Eurocrypt'91, LNCS 547, 1991, pp. 337-351.*

[8.5] "Computing in the Jacobian of a Hyperelliptic Curve", **Cantor D.G.**, *Mathematics of Computation Vol. 48, No. 177, 1987, pp. 95-101.*

[8.6] "A Family of Jacobians Suitable for Discrete Log Cryptosystems", **Koblitz N.**, *Advances in Cryptology Crypto'88, LNCS 403, 1990, pp. 94-99.*

[8.7] "Abelian Surfaces and Jacobian Varietes over Finite Fields", **Rück H.**, *Compositio Mathematica Vol. 76, 1990, pp. 351-366.*

[9] Curvas Elípticas

[9.1] "The Arithmetic of Elliptic Curves", **Silverman J.H.**, *Springer Verlag GTM 106, 1986.*

[9.2] "Racional Points on Elliptic Curves", **Silverman J.H., Tate J.**, *Springer Verlag UTM, 1992.*

[9.3] "Elliptic Curves", **Husemöller D.**, *Springer Verlag GTM 111, 1987.*

[9.4] "Introduction to Elliptic Curves and Modular Forms", **Koblitz N.**, *Springer Verlag GTM 97, 1984.*

[9.5] "Elliptic Curves Diophantine Analysis", **Lang S.**, *Springer Verlag, Grundlehren der Mathematischen Wissenschaften 231, 1978.*

[9.6] "Elliptic Curves", **Knapp A.W.**, *Mathematical Notes 40, Princeton University Press, 1992.*

[9.7] "Algebraic Curves", **Fulton W.**, *Addison-Wesley Publishing Company, Inc., 1989.*

[9.8] "Introduction to Algebraic Curves", **Griffiths P.A.**, *American Mathematical Society, Translations of Methematical Monographs 76, 1989.*

[9.9] "Geometry of Projective Algebraic Curves", **Namba M., Marcel D.**, *Inc., Monographs and Textbooks in Pure and Applied Mathematics 88, 1984.*

[9.10] "Elementary theory of Analytic Functions of one or Several Complex Variables", **Cartan H.**, *Addison-Wesley Publishing Company, Inc., 1963.*

[9.11] "Elliptic Functions", **Lang S.**, *Springer Verlag, GTM 112, New York, 1987.*

[9.12] "The Arithmetic of Elliptic Curves", **Tate J.**, *Inventiones Math., Vol. 23, 1974, pp. 179-206.*

[9.13] "Primitive Points on Elliptic Curves", **Gupta R., Murty R. M.**, *Compositio Mathematica Vol. 58, 1986, pp. 13-44.*

[9.14] "Primitive Points on Elliptic Curves", **Lang S., Trotter H.**, *Bulletin of the American Mathematical Society Vol. 83 No. 2, 1977, pp. 189-292.*

[10] Curvas Elípticas Sobre Campos Finitos

[10.1] "Endomorphisms of Abelian Varieties over Finite Fields", **Tate J.**, *Inventiones Math. Vol. 2, 1966, pp. 134-144.*

[10.2] "Nosingular Plane Cubic Curves Over Finite Fields", **Schoof R.**, *Journal of Combinatorial Theory, Series A 46, 1987, pp. 183-211.*

[10.3] "Die Typen der Multiplikatorenringe elliptischer Funktionenkörper", **Deuring M.**, *Abh. Math. Sem. Hamburg, Bd. 14, 1941, pp. 197-272.*

[10.4] "Abelian Varieties over Finite Fields", **Waterhouse W.C.**, *Ann. scient. Éc. Norm. Sup., 4^a série, t. 2, 1969, pp. 521-560.*

[10.5] "An Elementary Introduction to Elliptic Curves", **Charlap L.S., Robbins D.P.**, *Institute for Defense Analyses, Princeton, New Jersey, CDR Expository Report No. 31, 1988.*

[10.6] "A Note on Elliptic Curves Over Finite Fields", **Rück H.**, *Mathematics of Computation Vol. 49, 1987, pp. 301-304.*

[10.7] "A Note on Elliptic Curves Over Finite Fields", **Voloch J.F.**, *Bull. Soc. Math. France., Vol 116, 1988, pp. 455-458.*

[10.8] "Isomorphism Classes of Elliptic Curves over Finite Fields of Characteristic 2", **Menezes A.J., Vanstone S.A.**, *Utilitas Mathematica Vol. 38, 1990, pp. 135-153.*

[10.9] "Counting Points on Elliptic Curves Over $\mathbb{F}_{2^m}$.", **Menezes A.J., Vanstone S.A., Zuccherato R.J.**, *Mathematics of Computation Vol. 60 No. 201, 1993, pp. 407-420.*

[10.10] "Short Programs for Function on Curves", **Miller V.S.**, *Exploratory Computer Science, IBM Thomas J. Watson Research Center, Yorktown Heights, NY 10598, 1996.*

[10.11] "Elliptic Curves Over Finite Fields and the Computation of Square Roots mod p", **Schoof R.**, *Mathematics of Computation Vol. 44, No. 170, 1985, pp. 483-494.*

[10.12] "Primality of the Number of Points on a Elliptic Curve Over a Finite Fields", **Koblitz N.**, *Pacific Journal of Mathematics Vol. 131 No. 1, 1988, pp. 157-165.*

[10.13] "On the Number of Points of Elliptic Curves over a Finite Fields and a Problem of B. Segre", **Ughi E.**, *Europ. J. Combinatorics Vol. 4, 1983, pp. 263-270.*

[10.14] "The Number of Points on an Elliptic Cubic Curve over a Finite Field", **Groote R., Hirschfeld J.W.P.**, *Europ. J. Combinatorics Vol. 1, 1980, pp. 327-333.*

[10.15] "Isogeny Classes of Abelian Varieties over Finite Fields", **Honda T.**, *J. Math. Soc. Japan Vol. 20 No. 1-2, 1968, pp. 83-95.*

[10.16] "Frobenius Maps of Abelian Varieties and Finding Roots of Unity in Finite Fields", **Pila J.**, *Mathematics of Computation Vol. 55 No. 192, 1990, pp. 745-763.*

[11] Factorización

[11.1] "The Future of Integer Factorization", **Odlyzko A.M.**, *AT&T Bell Laboratories, Murray Hill, NJ 07974, 1995.*

[11.2] "Factoring", **Pomerance C.**, *Proceedings of Simposia in Applied Mathematics Vol. 42, 1990, pp. 27-47.*

[11.3] "The Number Field Sieve", **Pomerance C.**, *Proceedings of Symposia in Applied Mathematics Vol. 48, 1994, pp. 465-480.*

[11.4] "Rabin-Miller Primality Test: Composite Numbers Which Pass It", **Arnault F.**, *Mathematics of Computation Vol. 64 No. 209, 1995, pp. 355-361.*

[11.5] "Very Short Primality Proofs", **Pomerance C.**, *Mathematics of Computation Vol. 48 No. 177, 1987, pp. 315-322.*

[11.6] "Implementation of a New primality Test", **Cohen H., Lenstra A. K.**, *Mathematics of Computation Vol. 48 No. 177, pp. 103-121.*

[11.7] "A Rigorous Time Bound for Factoring Integers", **Lenstra W.H., Pomerance C.**, *Journal of the American Mathematics Society Vol. 5 No. 3, 1992, pp. 483-516.*

[11.8] "Integers Without Large Prime Factors", **Hildebrand A., Tenenbaum G.**, *Journal de Théorie des Nombres de Bordeaux 5, 1993, pp. 411-484.*

[11.9] "The Factorization of the Ninth Fermat Number", **Lenstra A.K., Lenstra Jr. H.W. , Manasse M.S., Pollard J.M.**, *Mathematics of Computation Vol. 61 No. 203, 1993, pp. 319-349.*

[11.10] "The Primality of R1031", **Williams H.C., Dubner H.**, *Mathematics of Computation Vol. 47 No. 176, 1986, pp. 703-711.*

[11.11] "Effective Primality Tests for Integer of the Forms $N = k3^n + 1$ and $N = k2^m 3^n + 1$.", **Guthmann A.**, *Bit 32, 1992, pp. 529-534.*

[11.12] "A New Factorization Technique Using Quadratic Forms", **Lehmer D.H., Lehmer E.**, *Mathematics of Computation Vol. 28 No.126, 1974, pp. 625-635.*

[11.13] "Factoring with Two Large Primes", **Lenstra A.K., Manasse M.S.**, *Advances in Cryptology Eurocrypt'90, LNCS 473, 1990, pp. 72-82.*

[12] Factorización Elíptica

[12.1] "Factoring Integers with Elliptic Curves", **Lenstra Jr. H.W.**, *Annals of Mathematics Vol. 126, 1987, pp. 649-673.*

[12.2] "Lenstra's Factorization Method Based on Elliptic Curves", **Stephens N.M.**, *Advances in Cryptology Crypto'85, LNCS 218, 1986, pp. 409-416.*

[12.3] "Elliptic Curves and Primality Proving", **Atkin A.O., Morain F.**, *Mathematics of Computation Vol. 61 No. 203, 1993, pp. 29-68.*

[12.4] "Finding Suitable Curves for the Elliptic Curve Method of Factorization", **Atkin A.O., Morain F.**, *Mathematics of Computation Vol. 60 No. 201, 1993, pp. 399-405.*

[12.5] "An FFT Extension of The Elliptic Curves Method of Factorization", **Montgomery P.L.**, *Ph. D. Thesis University of California, Los Angeles, 1992.*

[12.6] "Speeding the Pollard and Elliptic Curve Methods of Factorization", **Montgomery P.L.**, *Mathematics of Computations Vol. 48 No. 177, 1987, pp. 243-264.*

[12.7] "On the Number of Elliptic Pseudoprimes", **Gordon D. M.**, *Mathematics of Computation Vol. 52 No. 185, 1989, pp. 231-245.*

[13] Información General

[13.1] "Trust in the New Information Age", **Maher D.P.**, *AT&T Technical Journal Sep./Oct., 1994, pp. 9-16.*

[13.2] "Cryptography Policy", **Hoffman L.J., Ali F.A., Heckler S. L., Huybrechts A.**, *Communications of the ACM Vol. 37 No. 9, 1994, pp. 109-117.*

[13.3] "Crypto Policy Perspectives", **Brooks C., Charney S., Denning D., Diffie W., Kent S., Landau S., Lauck A., Miller D., Neumann P., Sobel D.**, *Communications of the ACM Vol. 37 No. 8, 1994, pp. 115-121.*

[13.4] "A Plain Text on Crypto Policy", **Barlow J.P.**, *Communications of the ACM Vol. 36 No. 11, 1993, pp. 21-26.*

[13.5] "Denning's Article", **Denning D.E.**, *Communications of the ACM Vol. 36 No. 3, 1993, pp. 26-33.*

[13.6] "The Verdict on Plaintext Signatures: They're Legal", **Wright B.**, *Communications of the ACM Vol. 37 No. 10, 1994, pp. 122.*

[13.7] "Expectations of Security and Privacy", **Neumann P.G.**, *Communications of the ACM Vol. 37 No. 9, 1994, pp. 138.*

[13.8] "Secure Network Access Using Multiple Applications of AT&T's Smart Card", **Sherman S.A., Skibo R., Murray R.S.**, *AT&T Technical Journal Sep./Oct., 1994, pp. 61-72.*

[13.9] "Network Security In a Heterogeneous Environment", **Sharp R.L., Eisen S.R., Kleppinger W.E., Smith M.E.**, *AT&T Technical Journal Sep./Oct., 1994, pp. 52-60.*

[13.10] "Why Cryptosystems Fail", **Anderson B.**, *Communications of the ACM Vol. 37 No. 11, 1994, pp. 32-40.*

[13.11] "Internet Privacy Enhanced Mail", **Kent S.T.**, *Communications of the ACM Vol. 36 No. 8, 1993, pp. 48-60.*

[13.12] "Communications Privacy: Implications for Network Design", **Rotenberg M.**, *Communications of the ACM Vol. 36 No. 8, 1993, pp. 1-68.*

[13.13] "Protecting Telecommunications Privacy in Japan", **Hiramatsu T.**, *Communications of the ACM Vol. 36 No. 8, 1993, pp. 74-77.*

[13.14] "The Underpinnings of Privacy Protections", **Tuerkheimer F.M.**, *Communications of the ACM Vol. 36 No. 8, 1993, pp. 69-73.*

[13.15] "Encryption Need, Requirements and Solutions in Banking Networks", **Rimensberger U.**, *Advances in Cryptology Eurocrypt'85, LNCS 219, 1985, pp. 208-213.*

[13.16] "E-Mail & Messaging", **Barrus K.L.**, *Network Computing, 1995, pp. 146-149.*

[13.17] "Decrypting the Puzzle Palace", **Barlow J.P.**, *Communications of the ACM Vol. 35 No. 7, pp. 25-31.*

[14] Sobre la Historia de la Criptografía

[14.1] "The Codebreakers, the Story of Secret Writing", **Kahn D.**, *Macmillan Publishing Co. Inc., New York 1967.*

[14.2] "Machine Cryptography and Modern Cryptanalysis", **Deavours C.A., Kruh L.**, *Artech House, Inc., 1985.*

[14.3] "A Classical Cipher Machine: The ENIGMA, some Aspects Its History and Solution", **Churchhouse R.F.**, *The Institute of Mathematics and Its Applications Vol. 27, 1991, pp. 129-137.*

[15] Otros Criptosistemas

[15.1] "A Public-Key Cryptosystem Utilizing Cyclotomic Fields", **Scheidler R., Williams H.**, *Designs, Codes and Cryptography Vol. 6, 1995, pp. 117-131.*

[15.2] "A Key Exchange Protocol Using Real Quadratic Fields", **Scheidler R., Buchmann J.A., Williams H.C.**, *Journal of Cryptology Vol. 7, 1994, pp. 171-199.*

[15.3] "A Key Exchange System Based on Real Quadratic Fields, Extended Abstract", **Buchmann J.A., Williams H.C.**, *FB 10-Informatik, Universität des Saarlandes, 6600 Saarbrücken, West Germany, and Department of Computer Science, University of Manitoba, Winnipeg, Manitoba Canada R3T2N2.*

[15.4] "A Key Exchange System Based on Imaginary Quadratic Fields", **Buchmann J., Williams H.C.**, *Journal of Cryptology Vol. 1, 1988, pp. 107-118.*

[15.5] "Public Key Distribution in Matrix Ring", **Odoni R.W.K., Varadharajan V., Sanders P.W.**, *Electronic Letters Vol. 20, 1984, pp. 87.*

[15.6] "A New Public Key Cipher System Based Up on the Diophantine Equations", **Chang C.C., Lee R.C.T., Lin C.H.**, *IEEE Transactions on Computer Vol. 44 No. 1, 1995, pp. 13-19.*

[15.7] "Algorithms for Quantum Computation: Discrete Log and Factoring", **Shor P.W.**, *AT&T Bell Labs., Room 2D-149, 600 Mountain Ave., Murray Hill, N.J. 07974 USA.*

[15.8] "A Fast Signature Scheme Based on Congruential Polynomial Operations", **Okamoto T.**, *IEEE Transactions on Information Theory Vol. 36 No. 1, 1990, pp. 47-53.*

[15.9] "A Public Key Cryptosystem and Signature Scheme Based on Discrete Logarithms", **ElGamal T.**, *IEEE Transactions on Information Theory Vol. IT-31 No. 4, 1985, pp. 469-472.*

[15.10] "On Public Key Cryptosystems Built Using Polynomial Rings", **Pieprzyk J.P.**, *Advances in Cryptology Eurocrypt'85, LNCS 219, pp. 73-78.*

[15.11] "Two New Secret Key Cryptosystems", **Meijer H., Akl S.**, *Advances in Cryptology Eurocrypt'85, 1985, pp. 96-102.*

[15.12] "A Knapsack Type Public Key Cryptosystem Based on Arithmetic in Finite Fields", **Chor B., Rivest R.L.**, *IEEE Transactions on Information Theory Vol. 34 No. 5, 1988, pp. 901-909.*

[15.13] "Debating Encryption Standards", **Anderson J.C., Hellman M.E., Rivest R.L.**, *Communication of the ACM Vol. 35 No. 7, 1992, pp. 54.*

[15.14] "Improved Digital Signature Scheme Based on Discrete Exponentiation", **Agnew G.B., Mullin R.C., Vanstone S.A.**, *Department of Electrical and Computer Engineering, University of Waterloo, Ontario Canada N2L3G1.*

[15.15] "An Implementation for a Fast Public Key Cryptosystem", **Agnew G.B., Mullin R.C., Onyszchuk I.M., Vanstone S.A.**, *Journal of Cryptology Vol. 3, 1991, pp. 63-79.*

[15.16] "Data Encryption Standard", *Federal Information Processing Standards Publication 46, National Bureau of Standards U.S. Department of commerce, Washington, DC, January 15, 1977.*

[15.17] "MD2, MD4, MD5, SHA and other Hash Functions", **Robshaw M.J.B.**, *RSA Laboratories Technical Report TR-101 Version 3.0, 1994.*

[15.18] "A Public Key Cryptosystem Based on Algebraic Coding theory", **McEliece R. J.**,*DSN Progress Report 42-44, Jet Propulsion Laboratory , 1978, pp. 114-116.*

[15.19] "On the Equivalence of McEliece's and Niederreiter's Public Key Cryptosystem", **Li Y. X., Deng R. H., Wang X. M.**, *IEEE Transactions on Information Theory Vol. 40 No.1, 1994, pp. 271-273.*

[15.20] "Encryption and Error Correction Coding Using D Sequences", **Kak S.C.**, *IEEE Transactions on Computers Vol. C-34 No. 9, 1985, pp. 803-809.*

[15.21] "Combinatorially Based Cryptography for Children (and Adults)", **Fellows M.R., Koblitz N.**, *Department of Computer Science, University of Victoria, Victoria, B.C. V8W 3P6, Canada and Department of Mathematics GN-50, University of Washington Seattle, Washington 98195, USA 1993.*

[15.22] "The RC5 Encryption Algorithm", **Rivest R. L.**, *Dr. Dobb's Journal, January 1995, pp. 146-148.*

[15.23] "The IDEA Encryption Algorithm", **Schneier B.**, *Dr. Dobb's Journal, December 1993, pp. 50-56.*

[15.24] "The GOST Encryption Algorithm", **Schneier B.**, *Dr. Dobb's Journal, January 1995.*