EFECTO DE LA EXPANSIÓN DEL ESPACIO DE MENSAJES SOBRE LA LONGITUD DE LA INFORMACIÓN Y LOS TIEMPOS DE CIFRADO Y DESCIFRADO DEL PROTOCOLO BASADO EN EL ESQUEMA CRIPTOGRÁFICO CON CURVAS ELÍPTICAS (ECES)

Jorge Sega
Universidad Dr. Rafael Belloso Chacín. Venezuela

RESUMEN

El protocolo de cifrados ECES está catalogado dentro de los criptosistemas con curvas elípticas, teniendo una alta complejidad computacional, y por ende, una gran seguridad, mayor que los criptosistemas basados en el logaritmo discreto o la factorización. No obstante, este protocolo presenta un problema de lentitud en la transmisión de la información, asociado a la longitud de la misma, y a los tiempos del cifrado y descifrado de los mensajes. Esta investigación se basó en modificar el protocolo ECES, de manera que se expandiera su espacio de mensajes. Para ello se realizó una investigación de tipo exploratoria y explicativa; siendo su diseño experimental. El método aplicado para expandir dicho espacio ha sido aplicar el isomorfismo presente en ciertas familias de curvas elípticas, al protocolo en cuestión. Luego, la eficiencia de ambos protocolos ECES (tanto el original como el modificado) es comparada, en función de la longitud de la información, y de los tiempos de cifrado y descifrado. Los resultados obtenidos en esta investigación reflejan que se han aliviado las desventajas aludidas anteriormente, aumentando la velocidad de las comunicaciones cifradas con curvas elípticas. Se ha logrado rebajar la longitud del mensaje cifrado en un 11%. Los tiempos de cifrado y descifrado, tanto por bloque como por bit, también se han reducido. Luego, se concluye que estas mejoras se dan como consecuencia de la expansión del espacio de mensajes.

ABSTRACT

The protocol of encoding ECES is catalogued within the Elliptic Curve Cryptosystems, having a high computational complexity, and therefore, a great security, greater than cryptosystems based on the discreet logarithm or factorization. However, this protocol presents a problem of slowness for the transmission of the information, associated to its length, and to the times it takes for the coding and decoding of the messages. This investigation was based on modifying the ECES protocol, so that its space of messages expanded. The investigation type is exploratory and explicative; its design is experimental. The method applied to expand this space was to apply the

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

isomorphism that is present in certain families of elliptical curves, to the protocol. Then, the efficiency of both ECES protocols (the original one as well as the modified one) is compared, based on the length of the information, and the times of coding and decoding. The results obtained in this investigation reflect that the disadvantages alluded previously, have been alleviated, increasing the speed of the communications encrypted with elliptical curves. The length of the message has been managed to reduce in 11%. The times of the coding and decoding, per block and per bit, have been reduced, too. Then, one concludes these improvements are given as a result of the expansion of the space of messages.

INTRODUCCIÓN

Los temas de seguridad informática, protección de la información y en particular el uso de técnicas criptográficas para estos fines, comienzan a ser tenidos en cuenta en nuestra sociedad. Los problemas relacionados con la criptología, es decir, con el estudio de los criptosistemas, se han convertido hoy en día en base fundamental de la seguridad en las telecomunicaciones.

Una de las alternativas más efectivas en los criptosistemas son aquellos basados en curvas elípticas, que fueron admitidos como válidos por la comunidad criptográfica, después de que en 1985 Miller y Koblitz sugirieran su uso. Sin embargo, los criptosistemas de curvas elípticas aún presentan grandes inconvenientes, los cuales limitan su utilización en las telecomunicaciones de tiempo real. Las operaciones suma con los puntos de las curvas elípticas no es trivial, y exige una aritmética especial, la cual por lo general implica un tiempo de cómputo elevado, lo cual hace más lento el cifrado y el descifrado. Por otra parte, en todos los protocolos de cifrado ampliamente conocidos con curvas elípticas, los mensajes ya cifrados son por lo menos un 50% más largo que los mensajes en claro.

En esta investigación, se ha planteado el objetivo general de analizar el efecto de la expansión del espacio de mensajes en el protocolo basado en el esquema criptográfico de curvas elípticas (ECES - Elliptic Curve Encryption Scheme), de manera que se disminuya la longitud de la información, y los tiempos de cifrado y descifrado de los mensajes.

MÉTODO DE LA INVESTIGACIÓN

La metodología utilizada en esta investigación se cataloga como de tipo exploratoria y explicativa; siendo su diseño experimental.

El presente estudio partió de la tesis de Yanik (2001), en la cual se

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

sugiere el uso de técnicas de isomorfismo a las curvas elípticas, para aplicaciones criptográficas. Las fases en las cuales se desarrolló esta investigación se pueden observar a continuación.

Este estudio se llevó a cabo en tres fases: la primera es la modificación del protocolo de cifrado ECES. Esta modificación se basa en un método por el cual se logra la expansión del espacio de mensajes. Para lograr dicha expansión, el autor se valió de una herramienta de cálculo simbólico y numérico desarrollada por Wolfram Research Inc. Dicha herramienta es el software Mathematica 4.1, bajo una plataforma de Windows 2000 Server, en un computador Dell PowerEdge 2550, con dos procesadores Pentium III, de 1130 MHz cada uno, y 1 GB SDRAM. La técnica utilizada para expandir el espacio de mensajes es aplicar el isomorfismo de las curvas elípticas al protocolo ECES.

La segunda fase comprende un análisis comparativo entre los dos protocolos, el original y el modificado. Para ello se utiliza un parámetro comparativo, denominado factor de expansión η. Se calcula η para ambos protocolos, y luego se deduce, a manera porcentual, la reducción de la longitud de la información, dadas las modificaciones al protocolo ECES. Luego se comparan de nuevo dichos protocolos, pero en relación a los tiempos de cifrado y descifrado. Para estas comparaciones, se realiza primero un conteo del número de operaciones, para cada protocolo. Se calculan el número de operaciones por bloque, del cual se derivan el número de operaciones por bit, para luego comparar los resultados de ambos protocolos.

La tercera fase se concluye con la incidencia de la expansión del espacio de mensajes, sobre la longitud de la información y los tiempos de cifrado y descifrado del protocolo criptográfico ECES. Se parte de un principio lógico universal, el cual se extrapola a la comparación de los dos protocolos, para concluir acerca del efecto de la expansión del espacio de mensajes.

MODIFICACIÓN DEL PROTOCOLO ECES

a. Expansión del Espacio de Mensajes

La expansión del espacio de mensajes es el método utilizado en esta investigación para modificar y optimizar el protocolo ECES. Dicha expansión se logró mediante las técnicas de isomorfía propuestas por Yanik (2001).

Al hablar de curvas elípticas como herramientas de cifrado, resulta que al crear una curva, se tienen muchas copias de la misma materializadas en el

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

resto de curvas isomorfas a la misma.

El objetivo de utilizar curvas isomorfas no es aumentar la seguridad del protocolo, sino aumentar la velocidad de transmisión expandiendo el espacio de mensajes. Una de las grandes desventajas que se le daba al protocolo ECES era que el tamaño del mensaje cifrado era mucho mayor que el del mensaje en claro.

Entonces, si realmente se quiere reducir esta diferencia, se debe aumentar el tamaño de los bloques de mensaje en claro en la misma proporción que el aumento de tamaño de los bloques de mensaje cifrado.

De ahí surge la idea de utilizar curvas isomorfas, ya que ofrecen el mismo nivel de seguridad que el inicial, pero al tener sus puntos una apariencia exterior distinta, aumentan los elementos que podemos usar. Dos curvas isomorfas se diferencian únicamente en la nomenclatura de sus elementos, ya que estos se operan igual bajo las operaciones de grupo.

b. Curvas Isomorfas

Para definir las clases de isomorfía, es necesario dejar bien claro como se caracterizan dos curvas elípticas isomorfas. Para generalizar, se utiliza en principio la ecuación general de una curva elíptica y un teorema de caracterización:

Teorema: La demostración de este teorema se puede apreciar en Menezes (1993).

Dos curvas elípticas definidas según las siguientes ecuaciones:

$$E1/K: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$
$$E2/K: y^2 + b_1xy + b_3y = x^3 + b_2x^2 + b_4x + b_6$$

Son isomorfas sobre *K* si y sólo si existen $u, r, s, t \in K$ con $u \neq 0$, que satisfagan:

$ub_1 = a_1 + 2s$
$u^2b_2 = a_2 - sa_1 + 3r - s^2$
$u^3b_3 = a_3 + ra_1 + 2t$
$u^4b_4 = a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st$
$u^6b_6 = a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1$

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

Entonces el isomorfismo entre las curvas elípticas E_1 y E_2 queda definido por la función $\Phi:(x, y) \rightarrow (u^{-2}(x - r), u^{-3}(y - sx - t + rs))$, que lleva los puntos de la curva E_1 a los de la curva E_2, o equivalentemente, mediante la función inversa a la misma $\psi:(x, y) \rightarrow (u^2x + r, u^3y + u^2sx + t)$, que lleva los puntos de la curva E_2 a los de la curva E_1.

Tenemos aquí, entonces, una relación que se debe cumplir entre las curvas E_1 y E_2 para que sean consideradas isomorfas; lo cual da como resultado dos funciones de mapeo de los puntos de una curva a otra, y viceversa.

c. Protocolo de Comunicación ECES Original.

Este protocolo es ahora el estándar p1363 de IEEE. La idea principal del método ECES, es que no es necesaria la asignación de mensajes a puntos y viceversa, sino que es posible comunicar un punto de una curva elíptica de forma confidencial y al filtrar ese punto con el mensaje se logra mantener secreto el mensaje enviado.

A continuación se describirá el método de cifrado ECES con curvas elípticas. Dicho método corresponde al protocolo original a ser modificado, y analizado luego en esta investigación.

Para mantener la confidencialidad de los mensajes ha de seguirse un riguroso protocolo en el cifrado y descifrado de los mismos. En este protocolo se evita la asignación de mensajes a puntos, ya que el mensaje se enmascara con operaciones modulares con puntos de la curva. Los puntos están representados por su abscisa y un bit. Si se trabaja en cuerpos de cardinal primo mayor que 3, este bit es el menos significativo de la ordenada del punto, ya que como las dos raíces cuadradas de y^2 en F_p son opuestas y p es impar, una de ellas será par $bms(y)=0$ (bit menos significativo de y) y la otra será impar $bms(-y)=1$.

Según Menezes et. al. (1993), se define a $P=(x_p,y_p)$ como un punto en la curva elíptica E: $y^2=x^3+ax+b$ en el campo de los números primos Z_p. Luego, $bms(y_p)$ es el bit menos significativo de y_p.

Supónganse que se tienen la coordenada x de P (x_p), y el bit $bms(y_p)$. Entonces, la coordenada ordenada y_p se puede obtener de la siguiente manera:

1. Se calcula el elemento $\alpha=x_p^3+ax_p+b \bmod p$.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

2. Se calcula la raíz cuadrada β de α módulo p.
3. Si el bit menos significativo de β es igual a bit(y_p), entonces $y_p \leftarrow \beta$. Si no, entonces $y_p \leftarrow p - \beta$.

Una vez hecha la descripción de los puntos cifrados, es necesario describir el mensaje. El mensaje M es una cadena de octetos (el cual es un conjunto de ocho bits consecutivos, los cuales en consecuencia corresponderán a dos cifras hexadecimales, o a un byte). La longitud del mensaje M va a estar limitada a 2*w*-3 octetos donde *w* es la longitud del cardinal del cuerpo expresado en octetos. Es decir $w = \lceil t / 8 \rceil$ y $t = \lceil \log_2 p \rceil$.

La secuencia de octetos de *M* se rellena a la izquierda con una secuencia inicial *PS* de 2w - 3 - |*M*| octetos, todos ellos con el valor FF, seguido del octeto 00, para formar la secuencia *M'* de 2*w* - 2 octetos exactamente. *M'* = *PS*||00||*M*. Podría ocurrir que *PS* fuese nulo, si la longitud del mensaje es de exactamente 2*w* - 3 octetos. Los 2*w* - 2 octetos resultantes, se dividen en dos mitades de *w* - 1 octetos: M_1 = mitad izquierda de *M'* y M_2 = mitad derecha de *M'*.

Cuadro 1: Parámetros para la comunicación cifrada entre Alicia y Bernardo con el método ECES con curvas elípticas.

Información pública	Claves públicas de cifrado	Claves secretas
p, primo E/F_q: curva elíptica definida en F_q $G = (x_1 , y_1)$ generador de $E(F_q)$ $n = \# E(F_q)$	$\alpha G = (x_2 , y_2)$ clave pública de cifrado de Alicia $\gamma G = (x_3 , y_3)$ clave pública de cifrado de Bernardo	α clave secreta de descifrado de Alicia γ clave secreta de descifrado de Bernardo

Fuente: Autor

Supóngase que Bernardo quiere mandar el mensaje *M* del que obtiene después de todas las modificaciones descritas arriba *M'*, M_1 y M_2.

Elige un entero *k* arbitrario y calcula los puntos $(x_4, y_4) = kG$ y $(x_5, y_5) = k\alpha G$.

Añade a la izquierda de M_1 una secuencia de 8 - 8*w* + *t* ceros formando un elemento $m_1 \in F_q$.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

Añade a la izquierda de M_2 una secuencia de 8 - 8w + t ceros formando un elemento $m_2 \in F_q$.

Define x_6 como el resultado de hacer cero el bit más significativo de x_5.

Calcula x_6^3 y define y_6 al resultado de hacer cero el bit mas significativo de x_6^3.

Forma el elemento x_7 uniendo por la derecha a los $\lceil t/2 \rceil$ bits más significativos de x_6, los $\lfloor t/2 \rfloor$ bits menos significativos de y_6.

Forma el elemento y_7 uniendo por la derecha a los $\lceil t/2 \rceil$ bits más significativos de y_6, los $\lfloor t/2 \rfloor$ bits menos significativos de x_6.

Calcula $z_1 = m_1 \oplus y_6$ y a continuación $c_1 = x_7 z_1$.

Calcula $z_2 = m_2 \oplus x_6$ y a continuación $c_2 = y_7 z_2$.

Entonces manda el mensaje M cifrado como (x_4, c_1, c_2).

Alicia recibe el mensaje cifrado (x_4, c_1, c_2).

A partir de x_4, calcula el punto (x_4, y_4) ó -(x_4, y_4).

Calcula (x_5, y_5) = $\alpha(x_4, y_4)$ ó -$\alpha(x_4, y_4)$

Forma los elementos x_6, y_6, x_7, y_7 de la misma manera que lo hizo Bernardo en el cifrado.

Calcula $z_1 = c_1 x_7^{-1}$, y $m_1 = z_1 \oplus y_6$.

Calcula $z_2 = c_2 y_7^{-1}$, y $m_2 = z_2 \oplus x_6$.

Desecha los 8–8w+t bits más significativos de m_1. De esta manera, se transforma el resultado en la secuencia de octetos M_1, de longitud w-1.

Desecha los 8–8w+t bits más significativos de m2. De esta manera, se transforma el resultado en la secuencia de octetos M2, de longitud w-1.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

Concatena M1||M2 para obtener M'

Se extrae M de M'. Para ello se utiliza la siguiente igualdad, M' = PS||00||M que es siempre posible sin ambigüedad dada la singular definición de PS = FFFF... hasta el primer octeto 00.

d. Protocolo de Comunicación ECES Modificado.

A continuación se hará práctica la expansión del espacio de mensajes a un método de cifrado ya existente, en el que quedará reflejado la simplicidad del cambio y la gran ganancia en la complejidad computacional en las operaciones del cifrado y descifrado. El nuevo método de cifrado consiste en modificaciones de uno ya existente. Para indicar claramente cuales son estas modificaciones, las mismas serán resaltadas en **negrita**.

Estos métodos han sido evaluados para curvas que estén definidas en un cuerpo de cardinal primo mayor que 3.

En este método se puede aplicar la expansión del espacio de mensajes, filtrando el parámetro de isomorfía con una expansión de la coordenada de un punto que es parte secreta en las comunicaciones, y luego con otra parte del mensaje. Tal como se hizo en el punto 3c, para el protocolo ECES original, las modificaciones siguientes se darán para el cuerpo de los números primos F_p.

En este caso se aumenta el espacio de mensajes, agrandando de esta manera el filtro de multiplicación. Por tal motivo, el nuevo método ECES modificado es claramente una ampliación de los parámetros del método ECES original, descrito por Menezes et. al. (1993), y expuesto en el punto 3c de este artículo. De hecho, se mantienen los mismos parámetros de cifrado. A continuación se presenta un cuadro resumen, análogo al del protocolo ECES original, pero con las modificaciones basadas en la expansión del espacio de mensajes, las cuales serán detalladas luego de dicho cuadro:

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

Cuadro 2: Descripción de las claves del nuevo protocolo

Información pública	Claves públicas de cifrado	Claves secretas
p, primo E/F_p: $y^2 = x^3 + Ax + B$, con $A, B \in F_p$ $\beta \in F_p$, $\beta \neq 0$, $\left(\frac{\beta}{p}\right) = -1$, donde β hará el papel de coeficiente de isomorfía. E'/F_p: $y^2 = x^3 + \beta^2 Ax + \beta^3 B$ g generador de F_p $G = (x_1, y_1)$ punto generador de $E(F_p)$ $G' = (x_2, y_2)$ punto generador de $E'(F_p)$ $n = \# E(F_p)$	$\alpha G = (x_3, y_3)$ y $\alpha' G' = (x_4, y_4)$ claves públicas de cifrado de Alicia $\gamma G = (x_5, y_5)$ y $\gamma' G' = (x_6, y_6)$ claves públicas de cifrado de Bernardo	α y α' claves secretas de descifrado de Alicia γ y γ' claves secretas de descifrado de Bernardo

Fuente: Autor

Supóngase que Bernardo quiere mandar el mensaje *M* a Alicia. El mensaje, como en el método ECES descrito anteriormente (capítulo II), se considera como una cadena de octetos y su longitud máxima es de 3*w* - 4 octetos, y no 2*w* - 3 octetos como en el caso del protocolo ECES original, en donde *w* es el tamaño del cuerpo en octetos, es decir, que $w=\lceil t/8 \rceil$, con $t=\lceil \log_2 p \rceil$. Se define como |*M*| al módulo de la longitud del mensaje en octetos.

La secuencia que compone el mensaje se rellenará por la izquierda, siempre que haga falta, con una secuencia inicial *PS* de 3*w* - 4 - |*M*| octetos con el valor ff en hexadecimal seguido del octeto 00, para formar la secuencia *M*' de 3*w*-3 octetos. Esta secuencia se divide en tres partes de *w*-1 octetos de longitud: M_1, M_2 y M_3.

Bernardo define $h = M_1 + 1$, y $\begin{cases} H = \sqrt{h} & impar \quad si \quad \left(\frac{h}{p}\right) = 1 \\ H = \sqrt{\frac{h}{\beta}} & impar \quad si \quad \left(\frac{h}{p}\right) = -1 \end{cases}$

Si $\left(\frac{h}{p}\right) = 1$, entonces $e = 0$ y cifrará con las curvas isomorfas a *E*.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

Si $\left(\frac{h}{p}\right) = -1$, entonces *e* = 1 y cifrará con las curvas isomorfas a *E*'

Bernardo elige un entero *k* aleatorio y llama (x_7, y_7) = *kG* (*kG*' si trabaja en *E*') y (x_8, y_8) = *k*α*G* (*k*α'*G*' si trabaja en *E*')

$$w = g^{x_8} \pmod{p}$$

$$c_1 = w \oplus H \oplus x_8$$

Se define (xx_i, yy_i) = (x_iH^2, y_iH^3) con *i* = 7,8

Llama x_9 al número resultante de hacer 0 el bit más significativo de xx_8

Llama y_9 al número resultante de hacer 0 el bit más significativo de $xx_8^3 \pmod{p}$

Bernardo forma el elemento x_{10} uniendo por la derecha a los $\lceil t/2 \rceil$ bits más significativos de x_9, los $\lfloor t/2 \rfloor$ bits menos significativos de y_9

Bernardo forma el elemento y_{10} uniendo por la derecha a los $\lceil t/2 \rceil$ bits más significativos de y_9, los $\lfloor t/2 \rfloor$ bits menos significativos de x_9

Define $z_2 = M_2 \oplus y_9$ y $c_2 = x_{10}z_2 \pmod{p}$

Define $z_3 = M_3 \oplus x_9$ y $c_3 = y_{10}z_3 \pmod{p}$

Bernardo manda el mensaje cifrado (***e***, x_7, $\boldsymbol{c_1}$, c_2, c_3)

Alicia recibe el mensaje cifrado (***e***, x_7, $\boldsymbol{c_1}$, c_2, c_3)

Si *e* = 0 descifrará con una curva isomorfa a *E*. Si *e* = -1, usará una curva isomorfa a *E*'

$$s = \begin{cases} \sqrt{x_7^3 + Ax + B} \pmod{p} & si \quad e = 0 \\ \sqrt{x_7^3 + A\beta^2 x + \beta^3 B} \pmod{p} & si \quad e = 1 \end{cases}$$

Elige $y_7 = \begin{cases} s \\ p - s \end{cases}$

Calcula (x_8, y_8) = α(x_7, y_7) (o (x_8, y_8) = α'(x_7, y_7) si trabaja con la curva *E*'). Aquí la elección que haya hecho de y_7, es indiferente ya que el resultado es el mismo punto o su opuesto, que en cualquier caso comparten la misma

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

abscisa x_8

$w = g^{x_8} \pmod{p}$

$H = w \oplus x_8 \oplus c_1$

$h = H^2 \pmod{p}$ (βH^2 si trabaja en E')

$M_1 = h - 1$

Define xx_7, xx_8, x_9, y_9, x_{10}, y_{10} tal y como lo ha hecho Bernardo en el cifrado

Define $z_2 = \frac{c_2}{x_{10}} \pmod{p}$ y $M_2 = z_2 \oplus y_9$

Define $z_3 = \frac{c_3}{y_{10}} \pmod{p}$ y $M_3 = z_3 \oplus x_9$

Alicia concatena M_1, M_2 y M_3. Quita la secuencia inicial *PS* y el octeto 00 para obtener el mensaje M.

COMPARACIÓN DE LOS PROTOCOLOS ECES, ORIGINAL Y MODIFICADO

a. Longitud de los Mensajes Cifrados

Para analizar esta reducción se ha de utilizar un parámetro comparativo, definido como factor de expansión, denotado por η.

Definición: Se llamará η al factor de expansión de un método de cifrado, asociado a un cuerpo K, en donde está definido el espacio de mensajes. Matemáticamente, η estará definido por el siguiente cociente:

$$\eta = \frac{longitud \quad máxima \quad del \quad mensaje \quad cifrado}{longitud \quad máxima \quad del \quad mensaje \quad en \quad claro} = \frac{\max_{M \in MS_E} \{L(CS_E)\}}{\max_{M \in MS_E} \{L(M)\}},$$

Donde L(x) es la longitud en bits de x. En otras palabras, η es la relación existente entre el tamaño máximo de un mensaje cifrado y el tamaño máximo del mensaje en claro.

En el método ECES original, si se llama *w* a la longitud del cardinal del cuerpo en octetos (tal como se hizo al definir este protocolo), el mensaje cifrado tiene una longitud de *3w*, correspondiendo a tres elementos del

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

cuerpo (la abscisa de un punto, y el filtrado del mensaje en claro con otros dos elementos del cuerpo relacionados con otro punto de la curva); nótese que el mensaje cifrado tiene la siguiente forma: (x_4, c_1, c_2), lo cual se puede corroborar en el punto 3c de este artículo. Este mensaje cifrado es de un mensaje en claro de longitud *2w-3*. Por lo tanto, se tiene que para curvas definidas en F_p:

$$\eta = \frac{longitud \quad máxima \quad del \quad mensaje \quad cifrado}{longitud \quad máxima \quad del \quad mensaje \quad en \quad claro} = \frac{3w}{2w-3} \approx \frac{3}{2} = 1{,}5$$

Ahora, al calcular cual es el factor de expansión para el método ECES, luego de expandirle el espacio de mensajes, se notan mejoras considerables. Para este cálculo se vuelve a usar como medida los octetos. Con lo cual, el mensaje en claro tiene una medida de 3*w* – 4 octetos, tal como se expresó en el punto 3d, al definir este protocolo modificado.

En contraste, el mensaje cifrado consta con 3 elementos del cuerpo, resultantes del filtrado con elementos del cuerpo relacionados con la curva y una abscisa de un punto. Véase que dicho mensaje cifrado tiene la forma (*e*, x_7, c_1, c_2, c_3), en donde el parámetro e, que corresponde al índice que indica cuál curva isomorfa se utiliza. Pero como el tamaño de e es de un solo bit, este se deprecia para el presente cálculo. Por consiguiente, el tamaño del mensaje cifrado es de 4w. Entonces, el factor de expansión será:

$$\eta = \frac{longitud \quad máxima \quad del \quad mensaje \quad cifrado}{longitud \quad máxima \quad del \quad mensaje \quad en \quad claro} = \frac{4w}{3w-4} \approx \frac{4}{3} \approx 1{,}3$$

Como se puede apreciar, la ganancia en el factor de expansión es bastante notoria, ya que $\eta_{original} = 1{,}5 > \eta_{\mathrm{modificado}} \approx 1{,}3$. Supóngase que se quiere cifrar un mensaje de *k* bloques de longitud *l*. Esto da que la longitud total del mensaje cifrado será siempre ηkl. Si se consigue reducir el valor de η a η', la longitud total del mensaje se reduce en $kl(\eta - \eta')$ unidades de medida de longitud, y supone un $100[(\eta - \eta')/\eta]\%$ de mensaje cifrado menos. Con esto se tiene que la mejora en la longitud de los mensajes cifrados se puede cuantificar. Para el caso de estudio, la mejora es de un 11%.

b. Tiempos de Cifrado y Descifrado

Para analizar la complejidad de cualquier algoritmo se debe establecer que operaciones son las que se van a analizar. En primer lugar hay que tener en cuenta que para el cálculo de raíces cuadradas en F_p, se tiene una

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

complejidad muy alta si la comparamos con el resto de operaciones que se realizan en las comunicaciones cifradas.

Para estimar el número de operaciones, se han considerado cuatro categorías. Según Koblitz (1989), la complejidad computacional de las operaciones básicas utilizadas en comunicaciones cifradas con curvas elípticas en el cuerpo F_p, viene a ser dada por un factor del logaritmo de dicho primo, es decir, *log (p)*. Dicha complejidad se resume como sigue:

i. Suma y resta → *log (p)*
ii. Productos → log^2 *(p)*
iii. Cálculo de inversos → log^2 *(p)*
iv. Cálculo de raíces cuadradas → log^4 *(p)*

Siendo estas las operaciones básicas que se efectúan tanto en el proceso de cifrado como de descifrado.

Tiempo del Cifrado

Los siguientes cuadros muestran el número de operaciones básicas del cifrado, por bloque y por bit, tanto del protocolo ECES original, como del modificado.

Cuadro 3: Cifrado. Número de operaciones básicas por bloque de mensaje en claro, para el protocolo original

Sumas	Productos	Inversos	Raíces cuadradas
42(log (*p*)) + 2	11(log (*p*)) + 4	3(log (*p*))	0

Fuente: Autor

Cuadro 4: Cifrado. Número de operaciones básicas por bit de mensaje en claro, para el protocolo original

Sumas	Productos	Inversos	Raíces cuadradas
21	11/2	3/2	0

Fuente:Autor

Cuadro 5: Cifrado. Número de operaciones básicas por bloque de mensaje en claro, para el protocolo modificado

Sumas	Productos	Inversos	Raíces cuadradas
42(log (*p*)) + 5	(25(log (*p*))/2) + 9	3(log (*p*)) + 1	0

Fuente: Autor

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

Cuadro 6: Cifrado. Número de operaciones básicas por bit de mensaje en claro, para el protocolo modificado

Sumas	Productos	Inversos	Raíces cuadradas
14	25/6	1	0

Fuente: Autor

Al comparar los protocolos ECES original y modificado, se tiene que en el segundo, la complejidad total del cifrado, y por ende el tiempo que toma cifrar un mensaje, es menor que para el primero. Por lo que los cambios significan una mejora de este parámetro.

Tiempo del Descifrado

Los siguientes cuadros muestran el número de operaciones básicas del descifrado, por bloque y por bit, tanto del protocolo ECES original, como del modificado.

Cuadro 7: Descifrado. Número de operaciones básicas por bloque de mensaje en claro, para el protocolo original

Sumas	Productos	Inversos	Raíces cuadradas
$21(\log(p)) + 6$	$(11(\log(p))/2) + 9$	$(3(\log(p))/2) + 2$	1

Fuente: Autor

Cuadro 8: Descifrado. Número de operaciones básicas por bit de mensaje en claro, para el protocolo original

Sumas	Productos	Inversos	Raíces cuadradas
7	11/6	½	0

Fuente: Autor

Cuadro 9: Descifrado. Número de operaciones básicas por bloque de mensaje en claro, para el protocolo modificado

Sumas	Productos	Inversos	Raíces cuadradas
$21(\log(p)) + 9$	$7(\log(p)) + 13$	$(3(\log(p))/2) + 2$	1

Fuente: Autor

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

Cuadro 10: Descifrado. Número de operaciones básicas por bit de mensaje en claro, para el protocolo modificado

Sumas	Productos	Inversos	Raíces cuadradas
21/4	7/4	3/8	0

Fuente: Autor

Si se analizan las operaciones básicas por cada bloque cifrado se ve que sufre un pequeño aumento, debido a que entre otras cosas los bloques cifrados son de mayor tamaño. Pero como también se puede apreciar, aunque se haga una exponenciación, no se añade ninguna operación más con puntos de la curva. Por tanto, el incremento del número de las operaciones básicas es considerable.

Esto se ve reflejado al analizar los resultados de conteo de operaciones básicas por bit del mensaje cifrado. La disminución del número de operaciones básicas es notable.

En resumen, así como ocurrió con el tiempo de cifrado, pero en menor escala, el tiempo del descifrado para el protocolo ECES modificado resulta menor que para el protocolo ECES original. Por lo tanto, las modificaciones hechas también mejoran este parámetro.

INCIDENCIA DE LA EXPANSIÓN DEL ESPACIO DE MENSAJES EN EL PROTOCOLO ECES

Con las modificaciones hechas en esta investigación, ahora se tiene para cifrar con el protocolo ECES, todos los puntos de una familia de curvas elípticas, en vez de los de una sola. Por lo tanto, si se asocia a cada punto un mensaje, se habrá aumentado el espacio de mensajes cifrables. Aunque también se aumente el tamaño de los cifrados, éstos lo hacen de forma proporcional al crecimiento del espacio de mensajes cifrables, produciendo así una disminución del factor de expansión, definido como η.

La metodología de expandir el espacio de mensajes fue la que dio lugar al nuevo protocolo de cifrado, desarrollado de este artículo. Luego, tal como se puede apreciar al confrontar los protocolos ECES original y modificado, tanto la longitud de los mensajes como en el tiempo de cifrado y descifrado de los mismos han descendido para este nuevo protocolo.

Partiendo ahora del principio lógico que si *a* genera *b*, y *b* genera *c*, entonces se deduce que *a* genera *c*. Sustituyendo:

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

a = expansión del espacio de mensajes
b = protocolo ECES modificado
c = disminución de la longitud de la información, y disminución de los tiempos de cifrado y descifrado

Se concluye que, la expansión del espacio de mensajes, da como resultado la disminución de la longitud de la información y la disminución del tiempo de cifrado y descifrado, del protocolo ECES. Lográndose así el tercer objetivo específico, y el objetivo general de esta investigación.

CONCLUSIONES

Las conclusiones de la investigación son alentadoras. En el desarrollo de la misma, se ha generado un método para la reducción de la complejidad tanto en función de la longitud de la información, como en el tiempo del cifrado y descifrado, de las comunicaciones cifradas con curvas elípticas, específicamente del protocolo ECES. El método desarrollado se basa en la expansión del espacio de mensajes utilizando un nuevo parámetro para cifrar, como lo es el coeficiente de isomorfía.

El algoritmo que constituye al protocolo de cifrado ECES ha sido modificado, de manera tal que su espacio de mensajes se ha ampliado. Básicamente, esto se ha dado, ya que en vez de utilizar los puntos de una sola curva elíptica para cifrar un mensaje (tal como se venía haciendo en el protocolo ECES original), se ha desarrollado un método que utiliza los puntos de una familia completa de curvas isomorfas.

Esta expansión del espacio de mensajes, para el protocolo ECES, se ha contabilizado en función del cardinal primo, p; dando como resultado que ahora se pueden cifrar hasta $w = \lceil (\log_2 p)/8 \rceil$ octetos por bloque más que con el protocolo original.

Al comparar los protocolos ECES original y modificado, en función de la longitud de la información, se observó una mejora del 11% al aplicar las modificaciones; lo cual se traduce en una menor complejidad computacional y tiempos de comunicación más cortos.

La disminución de la complejidad en espacio (longitud de la información) es debido a la inclusión en cada bloque cifrado de un nuevo elemento del cuerpo de definición de la curva, a la vez que de la misma manera crece cada bloque de mensaje en claro, debido a la expansión del espacio de mensajes.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

Por otra parte, la comunicación cifrada se hace de forma más rápida debido a la disminución de la cantidad de operaciones, tanto en el cifrado como en el descifrado. Este ahorro en la complejidad en el tiempo tiene como causa principal el ya mencionado descenso de la complejidad en espacio; lo cual hace que el número de bloques a cifrar sea menor para el protocolo modificado.

Como se ha expuesto anteriormente, las modificaciones al protocolo ECES se han basado en la expansión de su espacio de mensajes; y dichas modificaciones han traído como consecuencias la reducción de la longitud de la información en un 11%, y la disminución de los tiempos de cifrado y descifrado de los mensajes. Por consiguiente, estas mejoras, tanto en espacio como en tiempo, son consecuencia directa de la expansión del espacio de mensajes.

Finalmente, se tiene que el protocolo desarrollado en esta investigación, presenta mejoras que pueden dar lugar a aplicaciones, tanto para software como para hardware, mucho más óptimas en lo que se refiere a la velocidad de la información. El método aquí propuesto, además, no compromete la seguridad de la información cifrada con él, ya que en esencia, el protocolo ECES no ha variado; tan solo se ha ampliado el número de curvas elípticas con las cuales se cifra, introduciendo el parámetro de transformación de una curva a otra, como otro parámetro de cifrado.

REFERENCIAS BIBLIOGRÁFICAS

Angel, J. (2000). Criptografía para principiantes. Obtenido en la Red Mundial el 05 de Noviembre de 2002: http://www.criptored.upm.es/descarga/cripto_basica.zip

Arias, F. (1999), El proyecto de investigación. Guía para su elaboración. Caracas: Editorial Episteme.

Barreto, P. (2003). Tesis de Grado. Criptografia Robusta e Marcas D'água Frágeis Construção e Análise de Algoritmos para Localizar Alterações. Universidade de Sao Paulo, Sao Paulo, Brasil.

Belingueres, G. (2000). Introducción A Los Criptosistemas de Curva Elíptica. Obtenido en la Red Mundial el 05 de Noviembre de 2002: http://www.mesea.com/elhacker/articulos/seguridad/criptosistemas_clave_eliptica_by_gabriel_belingueres.zip

Chao, J., Nakamura, O., Sobataka, K., y Tsujii, S. (1998). Construction of

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

Secure Elliptic Cryptosystems Using CM Tests and Liftings. ASIACRYPT, 95-109

Cohen, H., Miyaji, A., y Ono, T. (1998). Efficient Elliptic Curve Exponentiation Using Mixed Coordinates. En (Eds.), Proceedings of the International Conference on the Theory and Applications of Cryptology and Information Security (págs. 51-65). Londres: Springer Verlag.

Fernández Collado, C., Hernández Sampieri, R., y Baptista Lucio, P. (1998). Metodología de la investigación. Mexico: McGraw Hill.

Fujioka, A., Fujisaki, E., y Okamoto, T. (1992). An Efficient Digital Signature Scheme Based on an Elliptic Curve Over the Ring Zn. 54-65. Obtenido en la Red Mundial el 14 de Febrero de 2003: http://dsns.csie.nctu.edu.tw/research/crypto/HTML/PDF/C92/54.PDF

Gadné, M. (2002). Tesis de Grado. Applications of Bilinear Maps in Cryptography. University of Waterloo, Ontario, Canada. Obtenido en la Red Mundial el 11 de Octubre de 2003: http://etd.uwaterloo.ca/etd/m2gagne2002.pdf

Koblitz, N. (1984). Introduction to Elliptic Curves and Modular Forms. Nueva York, EE.UU.: Springer-Verlag.

Koblitz, N. (1987). Elliptic curve cryptosystems. Mathematics of Computation, 48, 203-209.

Menezes, A. J., Okamoto, T., y Vanstone, S. A. (1993). Reducing elliptic curve logarithms in a finite field. IEEE Transactions on Information Theory, 39(5), 1639-1646.

Menezes, A. J., Qu, M., y Vanstone, S. A. (1995). Part 4: Elliptic curve Systems. 5º Working Draft. Standard for RSA, Diffie-Hellman and related Public-key cryptography. IEEE P1363 Standard. Obtenido en la Red Mundial el 15 de Octubre de 2002: http://www.zone-h.org/download/file=792/

Miller, V. (1986). Uses of elliptic curves in cryptography. Advances in Cryptology, CRYPTO' 85, Lecture Notes in Computer Science, 218, 417-426.

Stinson, D. (1995). Cryptography, Theory and Practice. Boca Ratón, EE.UU.: CRC Press.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

Tamayo y Tamayo, Mario. (1998). El Proceso de la Investigación Científica. México: Ed. Limusa S.A.

Yanik, T. (2001). Tesis de Grado. New Methods for Finite Field Arithmetic. Oregon State University, Corvallis, EE.UU. Obtenido en la Red Mundial el 01 de Octubre de 2002: http://security.ece.orst.edu/papers/01Yanik.pdf

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005