Síntesis de esquemas criptográficos de clave pública no convencionales basados en campos finitos no binarios

Prof. Dr. Javier Areitio Bertolín

Director del Grupo de Investigación Redes y Sistemas. Catedrático de la Facultad de Ingeniería. ESIDE. Universidad de Deusto (UD). E. Mail: jareitio@eside.deusto.es

En el presente artículo se desarrollan y analizan diversos esquemas criptográficos de clave pública ó asimétricos sobre campos finitos no binarios como GF(3^4) y GF(p). Se desarrolla un cripto-sistema estilo E-G sobre GF(3^4), otro estilo E-G sobre GF(p), un cripto-sistema estilo D-H sobre GF(p), un cripto-sistema de firma electrónica basado en curvas elípticas sobre GF(p) y un cripto-sistema de firma electrónica estilo DSA sobre GF(p). Se concluye con la especificación de los algoritmos de Euclides y Euclides Extendido muy útiles en criptografía.

Actualmente la información es un activo muy valioso del que dependen todo tipo de gobiernos y organizaciones ya sean públicas y privadas de tipo comercial, financiero, sanitario, I+D, etc.. La información en formato electrónico presenta amenazas de seguridad más graves que las existentes en información impresa en papel. La información en formato electrónico puede ser potencialmente robada desde una posición remota, puede ser interceptada e incluso manipulada a distancia. En este contexto de la sociedad de la información y del conocimiento, la seguridad de la información describe todas las medidas tomadas para prevenir el uso no autorizado de todo tipo de datos electrónicos.

El uso no autorizado de datos puede ser la revelación, alteración, sustitución o destrucción de los datos de interés. La seguridad de la información proporciona entre otros los siguientes servicios:

(a) Confidencialidad. Previene la revelación no autorizada de información.

(b) Integridad. Previene la modificación no autorizada de información.

(c) Disponibilidad. Previene la retención (ó negación de acceso) no autorizada a la información o recursos (periféricos, recursos de red, etc.).

Entre las distintas contramedidas propuestas, la utilización de los sistemas criptográficos ofrece el mayor nivel de seguridad junto con un nivel máximo de flexibilidad. De hecho, un sistema criptográfico que se gestiona e implementa correctamente ofrece el nivel más alto de seguridad para la información electrónica disponible hoy en día.

Servicios proporcionados por los sistemas criptográficos. Tipos de criptosistemas

Los sistemas criptográficos ó cripto-sistemas ofrecen o ayudan a ofrecer entre otros los siguientes servicios:

(a) Confidencialidad de los datos. Protección de los datos de revelación no autorizada, para ello se utilizan algoritmos de cifrado con vistas a ocultar el contenido de los mensajes.

(b) Integridad de datos. Protección de los datos de alteración o destrucción no autorizada, para ello se utilizan funciones de comprobación de integridad para detectar si un documento se ha modificado o no (mediante firmas electrónicas basadas en algoritmos asimétricos, funciones criptográficas unidireccionales ó resumen ó hash (como SHA1, MD5, etc.), funciones MAC basadas el algoritmos simétricos, utilización de "nonces", etc.).

(c) Autenticación del origen de los datos. Corrobora el origen de los datos que puede ser realizado con firmas electrónica o digitales.

(d) Autenticación de usuario. Asegura que las partes implicadas en una transacción-comunicación en tiempo real son quienes dicen ser y no hay suplantación de extremos comunicantes. La firma digital ayuda en este problema.

(e) No repudio. La criptografía por si sola no resuelve el problema pero ayuda. Permite la existencia de evidencias de que los datos se han enviado o se han recibido, por tanto ayudan a que el emisor o receptor no pueda posteriormente negar de forma falsa este hecho.

Los cripto-sistemas tienen en cuenta el hecho de que no sólo es importante hacer segura una transacción sino también que su funcionamiento sea eficiente.

$\alpha^0 = 1 = (0001)$, $\alpha^1 = (0010)$, $\alpha^2 = (0100)$, $\alpha^3 = (1000)$, $\alpha^4 = (2\alpha+1) = (0021)$, $\alpha^5 = (2\alpha^2+\alpha) = (0210)$, $\alpha^6 = (2\alpha^3+\alpha^2) = (2100)$, $\alpha^7 = (\alpha^3+\alpha+2) = (1012)$, $\alpha^8 = (\alpha^2+\alpha+1) = (0111)$, $\alpha^9 = (\alpha^3+\alpha^2+\alpha) = (1110)$, $\alpha^{10} = (\alpha^3+\alpha^2+\alpha+1) = (1111)$, $\alpha^{11} = (\alpha^3+2\alpha^2+1) = (1201)$, $\alpha^{12} = (2\alpha^3+1) = (2001)$, $\alpha^{13} = (2\alpha+2) = (0022)$, $\alpha^{14} = (2\alpha^2+2\alpha) = (0220)$, $\alpha^{15} = (2\alpha^3+2\alpha^2) = (2200)$, $\alpha^{16} = (2\alpha^3+\alpha+2) = (2012)$, $\alpha^{17} = (\alpha^2+2) = (0102)$, $\alpha^{18} = (\alpha^3+2\alpha)$, $\alpha^{19} = (2\alpha^2+2\alpha+1)$, $\alpha^{20} = (2\alpha^3+2\alpha^2+\alpha)$, $\alpha^{21} = (2\alpha^3+\alpha^2+\alpha+2)$, $\alpha^{22} = (\alpha^3+\alpha^2+2)$, $\alpha^{23} = (\alpha^3+\alpha+1)$, $\alpha^{24} = (\alpha^2+1)$, $\alpha^{25} = (\alpha^3+\alpha)$, $\alpha^{26} = (\alpha^2+2\alpha+1)$, $\alpha^{27} = (\alpha^3+2\alpha^2+\alpha)$, $\alpha^{28} = (2\alpha^3+\alpha^2+2\alpha+1)$, $\alpha^{29} = (\alpha^3+2\alpha^2+2\alpha+2)$, $\alpha^{30} = (2\alpha^3+2\alpha^2+\alpha+1)$, $\alpha^{31} = (2\alpha^3+\alpha^2+2\alpha+2)$, $\alpha^{32} = (\alpha^3+2\alpha^2+2)$, $\alpha^{33} = (2\alpha^3+\alpha+1)$, $\alpha^{34} = (\alpha^2+2\alpha+2)$, $\alpha^{35} = (\alpha^3+2\alpha^2+2\alpha)$, $\alpha^{36} = (2\alpha^3+2\alpha^2+2\alpha+1)$, $\alpha^{37} = (2\alpha^3+2\alpha^2+2\alpha+2)$, $\alpha^{38} = (2\alpha^3+2\alpha^2+2)$, $\alpha^{39} = (2\alpha^3+2)$, $\alpha^{40} = (2)$, $\alpha^{41} = (2\alpha+2)$, $\alpha^{42} = (2\alpha^2)$, $\alpha^{43} = (2\alpha^3)$, $\alpha^{44} = (\alpha+2)$, $\alpha^{45} = (\alpha^2+2\alpha)$, $\alpha^{46} = (\alpha^3+2\alpha^2)$, $\alpha^{47} = (2\alpha^3+2\alpha+1)$, $\alpha^{48} = (2\alpha^2+2\alpha+2)$, $\alpha^{49} = (2\alpha^3+2\alpha^2+2\alpha)$, $\alpha^{50} = (2\alpha^3+2\alpha^2+\alpha+2)$, $\alpha^{51} = (2\alpha^3+\alpha^2+2)$, $\alpha^{52} = (\alpha^3+2)$, $\alpha^{53} = (\alpha+1)$, $\alpha^{54} = (\alpha^2+\alpha)$, $\alpha^{55} = (\alpha^3+\alpha^2)$, $\alpha^{56} = (\alpha^3+2\alpha+1)$, $\alpha^{57} = (2\alpha^2+1)$, $\alpha^{58} = (2\alpha^3+\alpha)$, $\alpha^{59} = (\alpha^2+\alpha+2)$, $\alpha^{60} = (\alpha^3+\alpha^2+2\alpha)$, $\alpha^{61} = (\alpha^3+2\alpha^2+2\alpha+1)$, $\alpha^{62} = (2\alpha^3+2\alpha^2+1)$, $\alpha^{63} = (2\alpha^3+2\alpha+2)$, $\alpha^{64} = (2\alpha^2+2)$, $\alpha^{65} = (2\alpha^3+2\alpha)$, $\alpha^{66} = (2\alpha^2+\alpha+2)$, $\alpha^{67} = (2\alpha^3+\alpha^2+2\alpha)$, $\alpha^{68} = (\alpha^3+2\alpha^2+\alpha+2)$, $\alpha^{69} = (2\alpha^3+\alpha^2+\alpha+1)$, $\alpha^{70} = (\alpha^3+\alpha^2+2\alpha+2)$, $\alpha^{71} = (\alpha^3+2\alpha^2+\alpha+1)$, $\alpha^{72} = (2\alpha^3+\alpha^2+1)$, $\alpha^{73} = (\alpha^3+2\alpha+2) = (1022)$, $\alpha^{74} = (2\alpha^2+\alpha+1) = (0211)$, $\alpha^{75} = (2\alpha^3+\alpha^2+\alpha) = (2110)$, $\alpha^{76} = (\alpha^3+\alpha^2+\alpha+2) = (1112)$, $\alpha^{77} = (\alpha^3+\alpha^2+\alpha+1) = (1111)$, $\alpha^{78} = (\alpha^3+\alpha^2+1) = (1101)$, $\alpha^{79} = (\alpha^3+1) = (1001)$, $\alpha^{80} = 1 = (0001)$.

NOTA: $\alpha^{95} = \alpha^{15}$ ya que 95 entre 80 tiene por resto 15. Además $\alpha^{-2} = \alpha^{78}$ ya que (-2 + 80) = 78 donde n = 80.

Fig. 1.- Conjunto de elementos no nulos del campo $GF(3^4)$ definido sobre el polinomio $f(x) = x^4 + x + 2$, base de un criptosistema asimétrico estilo E-G en sus representaciones de potencia y como tupla de cuatro elementos.

La criptografía moderna no depende del secreto de sus algoritmos sino de sus claves privadas. Los algoritmos criptográficos utilizan claves para proteger la información. Por tanto la gestión de claves es una cuestión de capital importancia y necesita protegerse por medio de mecanismos de control de acceso en los sistemas de computación.

El cifrado es el término utilizado para definir el proceso que transforma los datos inteligibles, denominados texto en claro a una versión no legible denominada texto cifrado o cripto-grama. Esta conversión se controla por medio de una clave electrónica.

Por otra parte, el descifrado se emplea para transformar el texto cifrado o criptograma en texto en claro y se controla utilizando una clave.

Existen dos clases de cripto-sistemas:

(a) Cripto-sistemas simétricos o de clave secreta ó de secreto compartido. Utilizan la misma clave para cifrar y descifrar, p.e. AES, IDEA, 3DES, RC5, etc.

(b) Cripto-sistemas asimétricos ó de clave pública. Utilizan dos claves una pública para cifrar y otra secreta-privada para descifrar. Por ejemplo RSA, Mochilas, etc.

Un protocolo criptográfico es una secuencia de mensajes y respuestas pasados entre dos o mas partes que se comunican que proporciona a una o varias partes algún tipo de servicio criptográfico. Un ejemplo de protocolo criptográfico entre dos parte utilizado para la identificación de entidades se denomina “desafío-respuesta”.

Problemas matemáticos en criptosistemas. Factores para determinar la eficiencia de un criptosistema asimétrico

La criptografía de clave pública fue introducida en 1976 por Whitfield Diffie y Martin Hellman, desde entonces los sistemas criptográficos de clave pública han demostrado ser efectivos y más controlables que los sistemas de clave simétrica. Los sistemas criptográficos de clave pública basan su seguridad en la dificultad de resolver problemas matemáticos. Muchos de los sistemas se han roto o han demostrado no ser prácticos.

Actualmente entre los sistemas que se consideran seguros y eficientes se pueden identificar los siguientes cuya seguridad se basa en los problemas matemáticos siguientes:

(a) Problema de la factorización de números enteros. Ejemplos de cripto-sistemas son el de estilo RSA

tradicional con claves de 1024 bits, el estilo Rabin tradicional, etc.

(b) Problema del logaritmo discreto. Ejemplos de cripto-sistemas son el esquema de acuerdo de claves estilo Diffie-Hellman, esquemas de cifrado y firma estilo ElGamal, etc.

(c) Problema del logaritmo discreto sobre curvas elípticas (algo más difícil que los anteriores). Ejemplos de cripto-sistemas son la firma estilo ECDSA, el cifrado ECC con claves de 160 bits, etc.

Los problemas anteriores son difíciles de resolver en tiempo polinomial. Se pueden identificar cuatro factores a la hora de determinar la eficiencia de un cripto-sistema asimétrico:

(1) Costo computacional. Cantidad de computación requerida para realizar las transformaciones de cifrado, descifrado, firmado, verificación de firma, etc.

(2) Tamaño de clave. Tamaño en bits para almacenar el par de claves (pública-privada) y demás parámetros del cripto-sistema.

(3) Ancho de banda. Cantidad de bits que se necesita comunicar para transferir una firma o un mensaje cifrado.

(4) Determinismo del cifrado. Existen cripto-sistemas determinísticos que para un mismo mensaje en claro el texto cifrado siempre es el mismo (RSA tradicional), en cambio otros cripto-sistema (denominados probabilísticos o semánticamente seguros) para un mismo texto en claro producen textos cifrados ó criptogramas diferentes a lo largo del tiempo (no fugando información alguna a un hipotético adversario, atacante o cripto-analista que revise el texto cifrado).

Desarrollo de un criptosistema asimétrico de clave pública estilo E-G generalizado sobre un campo finito GF(3⁴)

El presente sistema criptográfico de tipo asimétrico, por tanto de clave pública estilo E-G (El Gamal) normalmente se describe sobre un campo GF(p) pero también se puede definir sobre los puntos de una curva elíptica sobre un campo finito GF(p) e incluso se puede generalizar y este es el objetivo de este apartado sobre un campo finito no binario GF(3^4). En todos los casos se cumple:

- Eficiencia, las operaciones son relativamente fáciles.
- Seguridad, el problema del logaritmo discreto no debe ser factible compu-tacionalmente. Veamos como se describe un cripto-sistema estilo E-G generalizado sobre un campo finito GF(3^4).

Proceso de generación de claves (pública y privada) en la entidad receptora

La entidad receptora selecciona un grupo multiplicativo cíclico G de orden "n" con elemento generador "g" del campo finito GF(3^4) cuyos elementos se representan por polinomios sobre GF(3) de grado menor que m = 4 y donde la multiplicación se realiza módulo un polinomio irreducible, por ejemplo:

$f(x) = (x^4 + x + 2)$.

Por convenio un elemento:

$(a_3x^3 + a_2x^2 + a_1x + a_0)$

se representa por medio de una cadena ternaria $(a_3\ a_2\ a_1\ a_0)$. El grupo G tiene orden n = 80 y un elemento generador es g = (0010) = α . El receptor selecciona un número entero aleatorio comprendido en el intervalo cerrado [1, n-1], entre 1 y (n-1) que corresponde con la clave privada "a", por ejemplo: a = 3 y calcula la operación $g^a = g^3 = \alpha^3$. La clave pública del receptor es g^a = (1000) junto con g = (0010) = α y el polinomio f(x) que define la operación de multiplicación en G. Dado el polinomio generador $f(x) = (x^4+x+2)$ se pueden obtener todos los elementos del campo haciendo $f(\alpha) = 0$, es decir:

$(\alpha^4 + \alpha + 2) = 0$ y,

se obtiene:

$\alpha^4 = (-\alpha - 2) = (2\alpha+1)$,

donde la operación de suma es módulo 3.

Por tanto los elementos del campo de Galois con extensión óptima GF(3^4) que se muestran en la figura 1, constituyen un grupo cíclico de orden n = 80 ya que $\alpha^{80} = \alpha^0 = 1 = (0001)$.

Proceso de cifrado en el emisor

El emisor desea enviar cifrado al receptor un mensaje de texto en claro (que debe ser un elemento de G de la forma cadena de cuatro dígitos ternarios), por ejemplo:
$m = (1100) = \alpha^{55}$.

El emisor selecciona un número entero aleatorio de un solo uso "k" (que pertenezca al intervalo cerrado [1, n-1]), por ejemplo k = 5 y realiza los siguientes cálculos:
$v = g^k = g^5 = \alpha^5 = (0210)$;
$w = [m.(g^a)^k] = m.(g^a)^5 = \alpha^{55}.\alpha^{15} = \alpha^{70} = (1122)$.

Por tanto el criptograma o texto cifrado que envía el emisor al receptor es: (v, w) = ((0210), (1122)).

Proceso de descifrado en el receptor

El receptor recibe el criptograma y con su clave privada a = 3 recupera el mensaje en texto en claro realizando las siguientes operaciones de descifrado:
$m = [(v)^{-a}.w] = (\alpha^5)^{-3}.\alpha^{70} = \alpha^{-15}.\alpha^{70} = \alpha^{55} = (1100)$.

Desarrollo de un criptosistema asimétrico de clave pública estilo E-G sobre un campo finito GF(p)

Proceso de generación de claves pública y privada del receptor

El receptor selecciona un número primo, grande, por ejemplo p = 97 (ó bien p = 23) y un elemento generador o raíz primitiva "a" del grupo multiplicativo módulo "p" que se denota mediante GF(p) = Zp por ejemplo a = 5 (ó bien a = 11, tal que las sucesivas potencias de 11 módulo 23 desde 2 a 22 generen todos los elementos no nulos de GF(23): $11^2 = 6$, $11^3 = 20$, . . . , $11^{21} = 21$, $11^{22} = 1$). El receptor B selecciona un número entero aleatorio secreto denominado su clave privada "x_B" en el intervalo cerrado [1, p-2], por ejemplo $x_B = 58$ (ó bien $x_B = 6$). Realiza el cálculo:
$y_B = a^{x_B} \bmod p = 5^{58} \bmod 97 = 44$ (ó bien $y_B = 11^6 \bmod 23 = 9$). La clave privada del receptor es "x_B" y la clave pública del receptor es y_B (junto con "p" y "a").

Proceso de cifrado en el emisor

El emisor desea enviar cifrado al receptor un texto en claro en la forma de un número entero comprendido en el intervalo cerrado [0, p-1], por ejemplo sea el mensaje m = 3 (ó

PARAMETROS DEL SISTEMA Y CLAVES :

Dados dos primos "p", "q" donde "q" divide a (p – 1),
p = 29, q = 7
Sea "g" un generador del subgrupo cíclico de orden "q" en Zp → g = 16
Sea la clave secreta del firmante un valor aleatorio entre 1 y (q-1) → x = 3
Sea la clave pública del firmante:
$y = g^x \bmod p = 16^3 \bmod 29 = 7$

FIRMA DEL HASH DE UN MENSAJE (r,s):

Sea el mensaje "m" y su hash: h(m) comprendido entre uno y (q-1)
h(m) = 5
El firmante genera un valor aleatorio "k" comprendido entre uno y (q-1) → k = 6
calcula: $r = (g^k \bmod p) \bmod q = (16^6 \bmod 29) \bmod 7 = 20 \bmod 7 = 6$
$s = k^{-1}[h(m) + x \,.\, r] \bmod q = 6[5 + 3 \,.\, 6] \bmod 7 = 5$
El mensaje firmado es la terna (m, r, s)

VERIFICACION DE LA FIRMA :

Verifica si "r" y "s" están comprendidos entre uno y (q-1)
calcula: $w = s^{-1} \bmod q = 5^{-1} \bmod 7 = 3$
$u_1 = w \,.\, h(m) \bmod q = 3 \,.\, 5 \bmod 7 = 1$
$u_2 = r \,.\, w \bmod q = 6 \,.\, 3 \bmod 7 = 4$
La firma digital se acepta si se verifica la igualdad siguiente con la clave pública del firmante "y":
$(g^{u_1} \,.\, y^{u_2} \bmod p) \bmod q = r$
$(16^1 \,.\, 7^4 \bmod 29) \bmod 7 = 20 \bmod 7 = 6$ → FIRMA CORRECTA

Fig. 2.- Firma digital estilo DSA basado en logaritmos discretos sobre GF(p).

bien m = 10), el emisor A selecciona un número entero aleatorio de un solo uso comprendido en el intervalo cerrado [1, p-2], por ejemplo k = 36 (ó k = 3) y calcula:
$K = y_B^k \bmod p = 44^{36} \bmod 97 = 75$
(ó bien $K = 9^k \bmod 23 = 16$),
así mismo determina dos valores:
$C_1 = a^k \bmod p = 5^{36} \bmod 97 = 50$
(ó bien $C_1 = 11^3 \bmod 23 = 20$);
$C_2 = (K.m) \bmod p = 75 .3 \bmod 97 = 31$
(ó bien $C_2 = 16 . 10 \bmod 23 = 22$).

El criptograma o texto cifrado que envía el emisor al receptor esta formado por dos valores: ($C_1 = 50$, $C_2 = 31$) ó bien ($C_1 = 20$, $C_2 = 22$).

Proceso de descifrado en el receptor

El receptor recibe el criptograma y con su clave privada "x_B" lo descifra realizando las dos operaciones siguientes:
$K = C_1^{X_B} \bmod p = a^{kX_B} \bmod p = 50^{58} \bmod 97 = 75$
(ó bien $K = 20^6 \bmod 23 = 16$, donde la inversa de 16 mod 23 es 13);
$m = C_2.K^{-1} \bmod p = 31.22 \bmod 97 = 3$
(ó bien m = (22 . 13) mod 23 = 10), por tanto el mensaje descifrado es: m = 3 (ó bien m = 10).

Se cumple que $K.K^{-1} = 1 \bmod p$, en este caso, $K^{-1} \bmod 97 = 22$ (ó bien $K^{-1} \bmod 23 = 13$).

Desarrollo de un criptosistema estilo D-H convencional sobre GF(p) para el acuerdo de claves secretas

Los cripto-sistemas de clave pública o asimétricos pueden clasificarse atendiendo al tipo de problema matemático utilizado en:

(1) Logaritmo discreto: estilos D-H (Diffie-Hellman), El-Gamal, DSA (para firma electrónica), LUC, XTR, etc.

(2) Factorización de números enteros: estilos RSA, GQ, etc.

(3) Logaritmo discreto sobre curvas elípticas: estilos EC-DH, EC-DSA.

CRIPTOSISTEMA CS-A1 :

Dado un mensaje en claro de 6 bits $M = m_0\ m_1 = (1,1,1,\ 1,1,1)$
Dada una clave simétrica de sesión de 6 bits
$K = k_1 k_2 = (1,0,1,\ 1,1,1)$
El criptograma o mensaje cifrado C se obtiene de la siguiente forma:
1) Se define una función de 6 variables
$f(x_1, x_2, x_3, y_1, y_2, y_3) = (x_1.x_2.y_1.y_2\ ,\ x_2.x_3.y_3.y_1\ ,\ (x_1 + x_2).y_1.y_3)$
2) Se definen dos variables
$m_2 = m_0 + f(k_1\ ,\ m_1) = (1,1,1) + f((1,0,1)\ ,\ (1,1,1)) = (1,1,1) + (0,0,1) = (1,1,0)$
$m_3 = m_1 + f(k_2\ ,\ m_2) = (1,1,1) + f((0,1,1)\ ,\ (1,1,0)) = (1,1,1) + (0,0,0) = (1,1,1)$
$C = (m_2, m_3) = (1,1,0,\ 1,1,1)$

CRIPTOSISTEMA CS-A2 :

Dado un mensaje en claro de 6 bits $M = m_0\ m_1 = (1,0,1\ \ 0,1,1)$
Dada una clave simétrica de sesión de 12 elementos
$K = k_1 k_2\ k_3 k_4 = (1,2,3\ \ 2,1,3\ \ 3,2,1\ \ 2,3,1)$
El criptograma o mensaje cifrado C se obtiene de la siguiente forma:
1) Se define una función de permutación de los bits de m_i según la clave k_i utilizada
$f(k_1, m_1) = (\text{los bits 1, 2, y 3 de } m_1 \text{ en el orden 1, 2, 3}) = (0,1,1)$
2) Se definen 4 variables
$m_2 = m_0 + f(k_1\ ,\ m_1) = (1,0,1) + (0,1,1) = (1,1,0)$
$m_3 = m_1 + f(k_2\ ,\ m_2) = (0,1,1) + (1,1,0) = (1,0,1)$
$m_4 = m_2 + f(k_3\ ,\ m_3) = (1,1,0) + (1,0,1) = (0,1,1)$
$m_5 = m_3 + f(k_4\ ,\ m_4) = (1,0,1) + (1,1,0) = (0,1,1)$
$C = (m_4, m_5) = (1,1,0\ \ 1,1,1)$

Fig. 3.- Especificación de dos cripto-sistemas simétricos de clave secreta CS-A1y CS-A2.

(3) Retículos: estilo NTRU, etc..

(4) Suma de subconjuntos: estilo Mochilas, etc.

(5) Códigos de corrección de errores: estilo McEllice (presenta similitudes con retículos), etc..

La especificación de un criptosistema estilo D-H convencional es la siguiente:

• Proceso de establecimiento de parámetros generales del cripto-sistema. Dado un campo finito GF(p), por ejemplo p = 517 y sea el elemento generador ó raíz primitiva g = 23

• Proceso de generación de las claves pública y privada de la entidad emisora A y de la entidad receptora B. La entidad emisora A selecciona una clave secreta $n_A = 8$ y la entidad receptora B selecciona una clave secreta $n_B = 14$. La entidad emisora A calcula su clave pública:

$P_A = g^{n_A} \bmod p = 23^8 \bmod 517 = 56$ y la entidad receptora B calcula su clave pública:
$P_B = g^{n_B} \bmod p = 23^{14} \bmod 517 = 89$.
• Proceso de transferencia mutua entre A y B de sus claves públicas. La entidad A envía a B su clave pública $P_A = 56$ y la entidad B envía a la entidad A su clave pública $P_B = 89$
• Proceso de obtención local (en A y en B) de la clave secreta común de sesión compartida entre A y B utilizando lo recibido y su clave secreta-privada. La entidad A eleva lo recibido a su clave privada obtenido el secreto compartido entre A y B, es decir la clave común es:
$K = 89^8 \bmod 517 = 243$.
La entidad B hace lo mismo eleva lo recibido a su clave privada obteniendo:
$K = 56^{14} \bmod 517 = 243$.

Sintesis de un cripto-sistema de firma digital basado en curvas elípticas estilo ECDSA sobre GF(p)

La firma digital puede realizarse de forma eficiente en sistemas de poca potencia de computación y reducida capacidad de almacenamiento utilizando curvas elípticas. Una curva elíptica como:
$y^2 = (x^3 + x + 1) \bmod 23$ definida sobre GF(23) verifica que:
$(4a^3 + 27b^2) = 8$ (distinto de cero, donde "a" es el coeficiente de "x" y "b" es el término independiente) presenta los veinte ocho puntos siguientes:
{(0, 1), (0, 22), (1, 7), (1, 16), (3, 10), (3, 13), (4, 0), (5, 4), (5, 19), (6, 4), (6, 19), (7, 11), (7, 12), (9, 7), (9, 16), (11, 13), (11, 20), (12, 4), (12, 19), (13, 7), (13, 16), (17, 3), (17, 20), (18, 3), (18, 20), (19, 5), (19, 18), O}

O= Punto origen en el infinito (P + O = P). Una curva elíptica como $y^2 = (x^3 + x) \bmod 23$ definida sobre GF(23) verifica que $(4a^3 + 27b^2)$ es distinto de cero, donde "a" es el coeficiente de "x" y "b" es el término independiente) presenta los veinte cuatro puntos siguientes:
{(0, 0), (1, 5), (1, 18), (9, 5), (9, 18), (11, 10), (11, 13), (13, 5), (13, 18), (15, 3), (15, 20), (16, 8), (16, 15), (17, 10), (17, 13), (18, 10), (18, 13), (19, 1), (19, 22), (20, 4), (20, 19), (21, 6), (21, 17), O}. Siendo O el punto origen en el infinito (P+O= P).

La especificación de un cripto-sistema de firma digital basado en curvas elípticas estilo ECDSA sobre GF(p) es la siguiente:

Proceso de generación de la clave de la entidad firmante emisora

(a) Se selecciona una curva elíptica E definida sobre GF(p) = Z_p. El número de puntos de $E(Z_p)$ debe ser divisible por un número grande primo "n".
(b) Se selecciona un punto P de la curva $E(Z_p)$ de orden "n".
(c) Se selecciona un número entero impredecible estadísticamente único "d" en el intervalo cerrado [1, n-1].
(d) Se calcula el punto Q=(d . P).
(e) La clave pública de la entidad firmante emisora es (E, P, n, Q) y su clave privada es "d".

Proceso de generación de la firma en la entidad firmante emisora

Sea "h(m)" el hash (por ejemplo SHA1) del mensaje "m" a ser firmado. Las acciones son:
(a) Se selecciona un número entero único e impredecible "k" en el intervalo cerrado [1, n-1].
(b) Se calcula:
$(k \,.\, P) = (x_1, y_1)$; $r = x_1 \bmod n$.
Si "r" es cero se vuelve al paso anterior ya que por seguridad si r = 0 entonces la ecuación de firma $s = k^{-1}[h(m) + d \,.\, r] \bmod n$ no implica a la clave privada "d".
(c) Se calcula $k^{-1} \bmod n$.
(d) Se calcula $s = k^{-1}[h(m) + d.r] \bmod n$
(e) Si s = 0 volver al primer paso del proceso. Si s=0 entonces $s^{-1} \bmod n$ no existe y se requiere en el proceso de verificación de firma.

CRIPTOSISTEMA CS-A1 :

Ecuaciones de descifrado:
Dado el mensaje cifrado $C = (m_2, m_3)$ de 6 bits
Se descifra realizando las siguientes operaciones con la clave secreta $K = k_1 k_2$ compartida:
$m_1 = m_3 + f(k_2, m_2)$
$m_0 = m_2 + f(k_1, m_1)$
obteniendo el mensaje en claro $M = m_0 m_1$

CRIPTOSISTEMA CS-A2 :

Ecuaciones de descifrado:
Dado el mensaje cifrado $C = (m_4, m_5)$ de 6 bits
Se descifra realizando las siguientes operaciones con la clave secreta $K = k_1 k_2 k_3 k_4$ compartida:
$m_3 = m_5 + f(k_4, m_4)$
$m_2 = m_4 + f(k_3, m_3)$
$m_1 = m_3 + f(k_2, m_2)$
$m_0 = m_2 + f(k_1, m_1)$
obteniendo el mensaje en claro $M = m_0 m_1$

Fig. 4.- Especificación de las ecuaciones de descifrado de los cripto-sistemas simétricos de clave secreta CS-A1y CS-A2.

(d) La firma del mensaje "m" es el par de números enteros (r, s). El firmante envía (m, h( ), r, s).

Proceso de verificación de la firma si es o no valida en la entidad receptora.

El receptor recibe (r, s) y con la clave pública del firmante verifica su validez:

(a) Obtiene una copia de la clave pública de la entidad firmante emisora (E, P, n, Q).

(b) Verifica que "r" y "s" son enteros en el intervalo cerrado [1, n-1].

(c) Se calcula $w = s^{-1} \bmod n$ así como h(m). Se calcula $u_1 = [h(m).w] \bmod n$ así como $u_2 = (r \,.\, w) \bmod n$.

(d) Se calcula $(u_1.\, P + u_2.\, Q) = (x_0,\ y_0)$ así como $v = x_0 \bmod n$.

(e) Se acepta la firma como válida si y sólo si v = r.

La figura 2 muestra la especificación de la síntesis de un cripto-sistema para firma electrónica estilo DSA basado en logaritmos discretos sobre GF(p).

Algoritmos de Euclides utilizados en criptografia

El algoritmo no extendido de Euclides permite calcular el máximo común divisor de dos número enteros "a" y "b" con "a" mayor o igual que "b": d = mcd (a, b) donde $a \geq b$.

Su especificación en pseudo-código es:

```
Comienzo
mientras b distinto de cero, hacer
{r = a mod b) , a = b , b = r}
d = a
fin
```

Por ejemplo, si d = mcd (36, 30) eso supone que:
a = 36/30/6,
b = 30/6/0,
r = 6/0, por tanto
d = 6.
El mcd (2940, 2002) = 14.
El mcd (143, 88) = 11.

El algoritmo extendido de Euclides ó EEA (Extended Euclidean Algorithm) permite obtener inversos modulares (si d = 1, es decir x = a mod b) y se formula de la manera siguiente: Calcular x, y, d = mcd (a, b), donde a.x + b.y = d. Su especificación en pseudo-código es (ver fig. 5):

Figura 5

```
Comienzo.
si b = 0 hacer
{d = a , x = 1 , y = 0}
sino hacer
        {x2 = 1 , x1 = 1 , y2 = 1 , y1 = 1
                mientras b mayor que 0 hacer
                        {q = a / b (cociente entero) , r = a – qb , x = x2 - qx1 ,
                         y = y2 - qy1 , a = b, b = r , x2 = x1 , x1 = x, y2 = y1 ,
                         y1 = y }
        }
d = a , x = x2 , y = y2
fin.
```

Consideremos, por ejemplo:
p = 2847893757848938511,
q = 92734928626327511
su producto n(p.q) toma el valor:
= 264099224369484956639974579586676121
supongamos que e = 1009, entonces el inverso multiplicativo módulo φ de "e" donde $\varphi = (p - 1).(q - 1)$ es $d = e^{-1} \bmod \varphi$
= 57583577166785619240689887497036 89
Por otra parte, el inverso multiplicativo $3^{-1} \bmod 460 = 307$, así mismo el inverso multiplicativo $3^{-1} \bmod 40 = 27$ como se puede comprobar al aplicar el EEA:
d = mcd(3, 40) = a.x + b.y donde:
a = 3 / 40 / 3 / 1 ;
b = 40 / 3 / 1 / 0 ;
x_2 = 1 / 0 /1 / -13;
x_1 = 0 / 1 / -13 / 40;
y_2 = 0 / 1 / 0 / 1;
y_1 = 1 / 0 / 1 / -3;
q = 0 / 13 / 3;
r = 3 / 1 / 0;
x = 1 / -13 / 40;
y = 0 / 1 / -3, por tanto
d = 1, x = -13 mod 40 = 27 y = 1, consecuentemente
d = mcd(a,b) = 1 = ax + by = (3)(27) + (40)(1)

Si nos piden hallar dos números enteros "d" y "n" tales que (2002.d + 2940.n) = mcd (2002, 2940) entonces aplicando EEA se obtiene d = 47, n = - 32. La inversa multiplicativa de 223 módulo 660 es 367.

La factorización del valor n = = 264099224369484956639974579586676121 es:
p = 2847893757848938511,
q = 92734928626327511.

Las figuras 3 y 4 muestran las ecuaciones de cifrado y descifrado de un par de cripto-sistemas simétricos denominados CS-A1 y CS-A2, ambos se caracterizan por utilizar una única clave de sesión compartida entre las partes que se comunican. ❑

Bibliografía

Areitio, J. "Análisis y desarrollo de esquemas para la compartición e intercambio de secretos". Revista Española de Electrónica. Nº 601. Diciembre 2004.

Areitio, J. "Diseño, síntesis y monitorización de cripto-sistemas simétricos". Revista Española de Electrónica. Nº 595. Junio 2004.

Buchmann, J.A. "Introduction to Cryptography". 2nd Edition. Springer-Verlag. 2004.

Goldreich, O. "Foundations of Cryptography, Vol. 2, Basic Applications". Cambridge University Press. 2004.