Desarrollo de mecanismos criptográficos asimétricos no convencionales

Por Javier y Gloria Areitio

El Dr. J. Areitio Bertolín (jareitio@eside.deusto.es) es Director del Grupo de Investigación Redes y Sistemas y Catedrático de la Facultad de Ingeniería de la Universidad de Deusto.

La Dra.G.Areitio Bertolin (ebparbeg@bs.ehu.es) es profesora del Laboratorio de Informática Aplicada de la Universidad del País Vasco (UPV / EHU)

En el presente artículo se sintetizan y analizan cinco mecanismos criptográficos de clave pública ó asimétricos (estilos E-G sobre GF(2 ^ 4), B-G, E-G sobre Zp, M-H y C-R) con diferentes niveles de seguridad, necesidades de potencia de computación y usabilidad. Todos ellos permiten múltiples funciones como realizar operaciones de cifrado, firma electrónica convencional y a ciegas, funciones unidireccionales tipo resumen (ó hash) y otras operaciones más sofisticadas.

Criptografia aplicada e ingenieria de seguridad de la informacion

El conjunto de requisitos de seguridad de la información va creciendo día a día. Entre los requisitos de seguridad más importantes que se pueden identificar actualmente se pueden indicar los siguientes:

(1) Ocultar la información, por ejemplo el contenido de los mensajes (servicio de confidencialidad), la identidad y ubicación geográfica de los usuarios (servicio de anonimato), la existencia de información en documentos o transmitiéndose en un canal de comunicaciones (utilizando técnicas de esteganografía, watermarks, canales subliminares, etc.); ó contra el análisis del tráfico incluso cifrado utilizando técnicas de relleno de tráfico para impedir inferencia de información por estadísticas de volumen de tráfico.

(2) Autenticación de la información.

(3) Controlar el acceso a la información (utilizando tres niveles):

- N1 con lo que se sabe, con contraseñas, frases de paso, etc.
- N2 con lo que se lleva, una tarjeta inteligente, una llave ó token hardware criptográfico USB, etc.
- N3 con lo que se es, características biométricas, huella dactilar, retina y/o iris (peligroso ya que puede facilitar datos íntimos de la persona (enfermedades, adicción a drogas, etc.), forma-volumen de la mano, etc.).

(4) El no repudio de las acciones realizadas por el emisor (envío de mensajes), receptor (recepción de mensajes), contenido de mensajes, fecha-hora implicadas, etc.

(5) Identificación y autenticación de entidades y usuarios.

(6) Capacidad de probar hechos relacionados con la información, por ejemplo, el conocimiento de un fragmento de información sin revelar (por ejemplo una contraseña) con tecnología Z-K utilizado en la identificación de entidades.

(7) Acordar un fragmento de información, por ejemplo un contrato digital.

Numerosas aplicaciones como el voto electrónico por Internet, los sistemas de pago digital, la protección de la privacidad personal, el problema de la piratería del software, las bases de datos distribuidas o la protección de la propiedad intelectual digital conducen a nuevos y más complejos requisitos de seguridad. Muchos de ellos aún están por identificar.

Uno de los problemas fundamentales de la seguridad de la información es la distinción entre información buena y mala, por ejemplo entre software (o ficheros adjuntos de Correo Electrónico) buenos o maliciosos ó entre tráfico de red bueno o malo con gusanos-virus, ataques DoS, etc. (por ejemplo utilizando cortafuegos multi-nivel (de filtrado de paquetes, inspección de estado, de nivel de aplicación con proxies ó agentes de protocolo de la capa de aplicación (http, ftp, h.323, smtp, etc.)) ó IDS-IPS-IMS (Sistemas de detección, prevención y gestión de intrusiones). Este problema de distinguir (por ejemplo para decidir si un fragmento de software satisface una especificación dada) esta pendiente por resolver y por tanto generalmente puede no tener una solución clara.

En contraposición, la criptografía se emplea generalmente para resolver problemas bien definidos con una solución clara (salvo por el hecho de que normalmente la seguridad no puede probarse de forma rigurosa). La potencia de la criptografía generalmente se desencadena sólo cuando se encuentra bien definido un problema. Por tanto, formalizar los problemas de seguridad de la información y determinar si existe una solución criptográfica es una parte importante de la investigación criptográfica. De hecho alguna de las más importantes y quizás más fascinantes contribuciones en investigación criptográfica son a veces soluciones paradójicas a ciertos problemas de seguridad por los que a primera vista no parecen existir soluciones. La criptografía clave de la seguridad en el nuevo milenio va siendo cada vez más una disciplina crucial para la sociedad de la información emergente. Si bien la seguridad de la información en el pasado parecía a veces un obstáculo caro en proyectos de TIC, gracias a la criptografía se percibe cada vez más una tecnología factible y fundamental para el desarrollo del siglo veintiuno.

La figura 1 nuestra los puntos de una curva elíptica de ecuación:

$$y^2 = (x^3 - 2x^2) \bmod 5$$

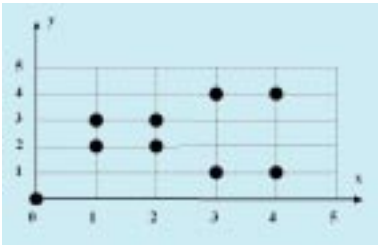

Fig. 1.- Representación gráfica de los puntos de la curva elíptica: y= (x - 2x) mod 5 sobre el campo finito Z. El conjunto completo de puntos es de diez elementos e incluye al punto en el infinito O. Estos puntos son: {(0, 0), (1,2), (1,3), (2,2), (2,3), (3,1), (3,4), (4,1), (4,4), O}.

definida sobre el campo finito GF(5)=Z5. El conjunto completo de puntos es de diez elementos e incluye al punto en el infinito O, estos puntos son:

{(0, 0), (1, 2), (1, 3), (2, 2), (2, 3), (3, 1), (3, 4), (4, 1), (4, 4), O}

Las figuras 2 y 3 representan gráficamente al mecanismo estilo D-H

(Diffie-Hellman) que permite distribuir entre dos o tres entidades un secreto compartido "z", para ello se utiliza una base de exponenciación "g" que debe ser primitivo módulo "p" (por ejemplo, si g=1 no sirve, ya que 1 ^ x mod p=1; si p=195 con g=14 no vale ya que 14 no es primitivo módulo 195 y la operación:

14 ^ x mod 195=14 ó 1

si p=181 con g=2 es válida ya que 2 es primitivo módulo p=181.

Dados dos números primos:
p= 86.759.222.313.428.390.812.218.077.095.850.708.048.977 y
q=108.488.104.853.637.470.612.961.399.842.972.948.409.834.611.525.790.577.216.753,
su producto es:
n=(p.q)=9.412.343.607.359.262.946.971.172.136.294.514.357.357.528.981.378.983.082.541.347.532.211.942.640.121.301.590.698.634.089.611.468.911.681.

Desarrollo de un criptosistema asimétrico de clave pública, estilo E-G generalizado sobre un campo finito GF(2^4)

El presente sistema criptográfico de tipo asimétrico, por tanto de clave pública estilo E-G (El Gamal) normalmente se describe sobre un campo finito Zp pero también se puede definir sobre los puntos de una curva elíptica sobre un campo finito Zp e incluso se puede generalizar y este es el objetivo de este apartado sobre un campo finito GF(2 ^ m).

En todos los casos se cumple que:

- Por eficiencia, las operaciones son relativamente fáciles.
- Por seguridad, el problema del logaritmo discreto no debe ser factible computacionalmente. Veamos como se describe un cripto-sistema estilo E-G generalizado sobre un campo finito GF(2 ^ m) en donde m=4.

Fig. 2.- Esquema de un mecanismo de distribución de una clave secreta "z" compartida, estilo D-H (Diffie-Hellman), entre dos entidades finales (entidad emisora E y entidad receptora R) utilizando un canal de comunicaciones no confidencial pero autenticado.

Proceso de generación de claves (pública y privada)

La entidad receptora selecciona un grupo multiplicativo cíclico G de orden "n" con elemento generador "g" del campo finito GF(2 ^ m) cuyos elementos se representan por polinomios sobre GF(2) de grado menor que m = 4 y donde la multiplicación se realiza módulo un polinomio irreducible, por ejemplo:

f(x) = (x ^ 4 + x + 1)

Por convenio un elemento,

(a3x ^ 3 + a2x ^ 2 + a1x + a0)

se representa por medio de una cadena binaria (a3 a2 a1 a0). El grupo G tiene orden n = 15 y el elemento generador es g = (0010). 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 = 7 y calcula la operación g ^ a = g ^ 7 = (1011). La clave pública del receptor es g ^ a = (1011) junto con g = (0010) y el polinomio f(x) que define la operación de multiplicación en G. Dado el polinomio f(x) = (x ^ 4 + x + 1) se pueden generar todos los elementos del campo haciendo f(g) = 0, es decir g ^ 4 + g + 1 = 0 se obtiene g ^ 4 = (g+1), donde la operación de suma es módulo 2; por tanto los elementos son los indicados a continuación:

g ^ 0=1=(0001),
g ^ 1=g=(0010),
g ^ 2=(0100),
g ^ 3=(1000),
g ^ 4=g+1=(0011),
g ^ 5=g ^ 2+g=(0110),
g ^ 6=g ^ 3+g ^ 2=(1100),
g ^ 7=g ^ 3+g+1=(1011),
g ^ 8=g ^ 2+1 =(0101),
g ^ 9=g ^ 3+g=(1010),
g ^ 10=g ^ 2+g+1=(0111),
g ^ 11=g ^ 3+g ^ 2+g=(1110),
g ^ 12=g ^ 3+g ^ 2+g+1=(1111),
g ^ 13=g ^ 3+g ^ 2+1=(1101),
g ^ 14=g ^ 3+1=(1001),
g ^ 15=g+g+1 =1=g ^ 0,

esto significa que es un grupo cíclico de orden n = 15 ya que g ^ 15 = g ^ 0 = 1.

Así mismo g ^ 77 = g ^ 2 ya que 77 entre n=15, tiene por resto 2.

Además, g ^ -2 = g ^ 13 ya que (– 2 + 15 = 13) en donde n = 15.

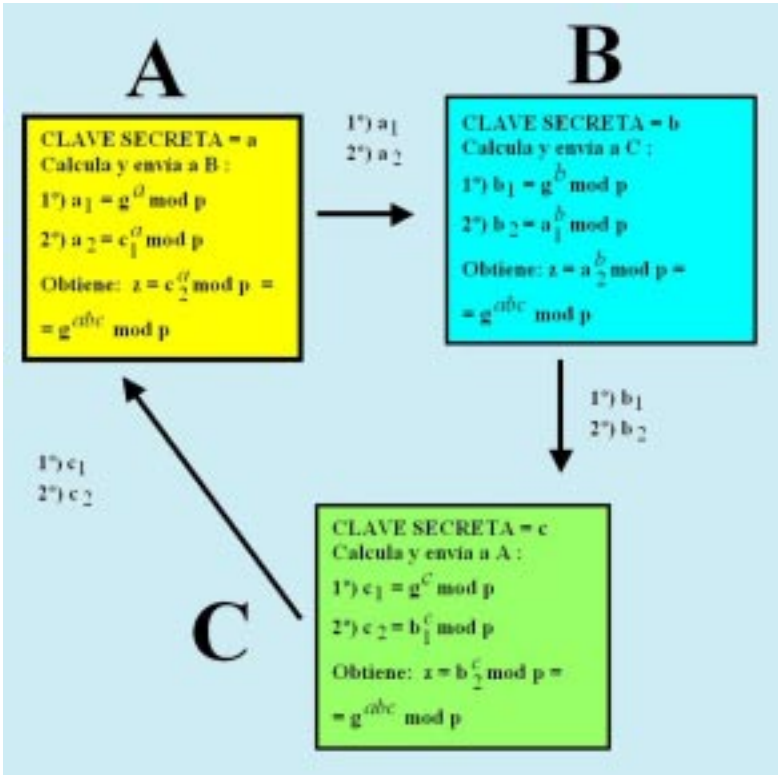

Fig. 3.- Protocolo estilo D-H (Diffie-Hellman) para distribuir una clave secreta "z" entre tres partes que se comunican: A, B y C.

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 4 bits), por ejemplo: m = (1100). El emisor selecciona un número entero aleatorio de un solo uso "k" (que pertenezca al intervalo cerrado [1, n-1]), por ejemplo k = 11 y realiza los siguientes cálculos:

v = g ^ k = g ^ 11 = (1110);

w = m.(g ^ a) ^ k = m . (g ^ a) ^ 11 = (1100).(0100) = g ^ 6.g ^ 2 = g ^ 8 = (0101).

Por tanto el criptograma o texto cifrado que envía el emisor al receptor es:

(v, w) = ((1110), (0101)).

Proceso de descifrado en el receptor

El receptor recibe el criptograma y con su clave privada recupera el mensaje en texto en claro realizando las siguientes operaciones de descifrado:

m = ((v ^ -a).w) = (1101).(0101) = g ^ 13.g ^ 8 = g ^ 21 = g ^ 6 = (1100), donde v ^ a = (1110) ^ 7 = (0100) = g ^ 2, además g ^ -2 = g ^ (-2 + 15) = g ^ 13 = (1101).

Síntesis de un criptosistema asimétrico probabilístico estilo B-G basado en un generador pseudoaleatorio BBS

El presente sistema criptográfico de tipo asimétrico y probabilístico, por tanto de clave pública, estilo B-G (Blum-Goldwasser) se basa en un generador de números pseudoaleatorio estilo BBS (Blum-Blum-Shub).

Este cripto-sistema es el más eficiente de los cripto-sistemas de cifrado probabilístico y es comparable al esquema RSA en términos de velocidad y expansión del mensaje. Es semánticamente seguro ya que el texto cifrado no fuga ningún tipo de información parcial. Se asume la no resolución del problema de la factorización de números enteros. Veamos como se describe.

Proceso de generación de claves pública y privada

La entidad receptora selecciona dos números primos aleatorios grandes y distintos "p" y "q" congruentes con 3 módulo 4, es decir p = q = 3 mod 4, por ejemplo p = 499, q = 547 y calcula su producto y lo llama "n":

n = (p . q) = 272953

También calcula dos números enteros "a" y "b" que satisfacen:

ap + bq = 1,

en este caso a = - 57, b = 52. La clave pública del receptor es n = 272953. La clave privada del receptor esta formada por cuatro valores: (p, q, a, b).

Proceso de cifrado en el emisor

El emisor calcula dos números "k" y "h" tales que "k" es el logaritmo en base 2 con redondeo hacia abajo de "n" y "h" es el logaritmo en base 2 con redondeo hacia abajo de "k", en este caso k = |log2 n| = 18, h = |log2 k| = 4. El emisor representa el mensaje en claro que va a enviar cifrado al receptor como una cadena de "t" bloques:

m1 m2 . . . mt,

en este caso t = 5 donde la longitud de cada bloque coincide con "h", en este caso h = 4. Por tanto el mensaje en claro a cifrar es: m1 = 1001, m2 = 1100, m3 = 0001, m4 = 0000, m5 = 1100.

El emisor selecciona un residuo cuadrático aleatorio "x0", esto se realiza seleccionando un número entero aleatorio "r", por ejemplo r = 399 y calculando: x0 = r ^ 2 mod n = 399 ^ 2 mod 272953 = 159201. A continuación se calcula desde i = 0 hasta i = t + 1 = 6 la operación:

xi = xi-1 ^ 2 mod n,

en este caso:

Para i = 1 se calcula: x1 = x0 ^ 2 mod n = 180539, donde "p1" son

los 4 bits menos significativos (LSB) de su representación binaria, en este caso p1=1011;

para i=2 se calcula: x2 = x1 ^ 2 mod n = 193932, donde "p2" son los 4 bits menos significativos (LSB) de su representación binaria, en este caso p2=1100;

para i=3 se calcula: x3 = x2 ^ 2 mod n = 245613, donde "p3" son los 4 bits menos significativos (LSB) de su representación binaria, en este caso p3=1101;

para i=4 se calcula: x4 = x3 ^ 2 mod n = 130286, donde "p4" son los 4 bits menos significativos (LSB) de su representación binaria, en este caso p4=1110;

para i=5 se calcula: x5 = x4 ^ 2 mod n = 40632, donde "p5" son los 4 bits menos significativos (LSB) de su representación binaria, en este caso p5=1000;

para i=6 se calcula: x6 = x5 ^ 2 mod n = 139680.

Desde i=1 hasta i=t=5 se calcula la suma módulo 2: ci = (pi + mi). En este caso: c1 = 0010, c2 = 0000, c3 = 1100, c4 = 1110, c5 = 0100. Por tanto, el criptograma o texto cifrado que envía el emisor al receptor es:

c=(c1,c2,c3,c4,c5,x6)=(0010, 0000,1100,1110,0100,139680).

Proceso de descifrado en el receptor

El receptor recibe el criptograma "c" y con su clave privada (p, q, a, b) obtiene el mensaje en claro del emisor. Para ello el receptor calcula:

d1=((p + 1)/4) ^ 6 mod (p-1)= 463;
d2=((q +1)/ 4) ^ 6 mod (q-1) = 337;
u = x6 ^ 463 mod p = 20;
v = x6 ^ 337 mod q=24;
x0 = (vap + ubp) mod n = 159201.

El receptor con "x0" construye desde i=1 a i=5 los "xi" y los "pi" y recupera los bloques de mensaje en claro "mi" utilizando la expresión:

mi = (ci + pi),

donde "pi" son los valores calculados en el receptor y los "ci" son los valores recibidos en el criptograma.

Desarrollo de un criptosistema asimétrico de clave pública tipo E-G sobre un campo finito Zp

Proceso de generación de claves pública y privada

El receptor selecciona un número primo grande, por ejemplo p = 2357 y un elemento generador "g" del grupo multiplicativo módulo "p" que se denota mediante GF(p) = Zp por ejemplo g = 2. Selecciona un número entero aleatorio denominado su clave privada "a" en el intervalo cerrado [1, -2], por ejemplo a=1751. Realiza el cálculo: g ^ a mod p =2 ^ 1751 mod 2357= 1185.

La clave privada del receptor es "a" y la clave pública del receptor esta formada por los tres valores siguientes: (p, g, g ^ 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 = 2035, el emisor selecciona un número entero aleatorio de un solo uso comprendido en el intervalo cerrado [1, p-2], por ejemplo k = 1520 y calcula dos valores:

v=a ^ k mod p=2 ^ 1520 mod 2357 = 1430;
w=(m.(g ^ a) ^ k)=(2035.1185 ^ 1520) mod 2357 = 697.

El criptograma o texto cifrado que envía el emisor al receptor esta formado por dos valores: (v = 1430, w = 697).

Proceso de descifrado en el receptor

El receptor recibe el criptograma y con su clave privada "a" lo descifra realizando las dos operaciones siguientes: v ^ (p-1-a) mod 2357= 1430 ^ 605 mod 2357=872, por tanto el mensaje descifrado es:

m = (v ^ (p-1-a) . w) mod p = 872 . 697 mod 2357 = 2035.

Desarrollo de un criptosistema asimétrico de clave pública basado en mochilas estilo M-H

El presente sistema criptográfico de tipo asimétrico, por tanto de clave pública estilo M-H (Merkle-Hellman) esta basado en el problema de la suma de subconjuntos supercrecientes que es NP-completo. Una secuencia de números enteros (b1, b2, . . . , bn) es supercreciente si se cumple que:

$$bi > \sum_{j=1}^{i-1} b_j$$

para cada "i" perteneciente al intervalo [2, n]. A continuación, veamos su arquitectura:

Proceso de generación de la clave pública y privada en el receptor

Se selecciona un entero "n", por ejemplo n = 6 como parámetro del sistema común. El receptor elige una secuencia supercreciente de "n" elementos, por ejemplo (12, 17, 33, 74, 157, 316) y un módulo "M" tal que M > (b1 + b2 + . . . + bn), por ejemplo M = 737. Selecciona un entero aleatorio W, tal que pertenece al intervalo [1, M-1] y verifica que el máximo común divisor mcd (W, M) = 1, por ejemplo W = 635. Selecciona una permutación aleatoria de enteros del uno a "n", por ejemplo: $\pi(1)=3$, $\pi(2)=6$, $\pi(3)=1$, $\pi(4)=2$, $\pi(5)=5$, $\pi(6)=4$

La clave pública del receptor se calcula realizando la operación:

ai = (W . b$_{\pi(i)}$) mod M

para todo "i" de 1 a "n", en este caso se obtiene el conjunto de valores: (319, 196, 250, 477, 200, 559) que se denomina "mochila pública". La clave privada-secreta del receptor es: (π, M, W, (12, 17, 33, 74, 157, 316)) donde (12, 17, 33, 74, 157, 316) se denomina mochila privada.

Proceso de cifrado en el emisor

El emisor desea enviar cifrado al receptor un mensaje en texto en

claro m = (101101), para ello realiza la siguiente operación para obtener el criptograma:
c=(m1.a1+m2 . a2+. . . +mn. an)= 319+250+477+559 = 1605, valor que envía como texto cifrado al receptor.

Proceso de descifrado en el receptor

El receptor recibe el criptograma y calcula:

d=(W ^ -1.c) mod M= 136.

El receptor resuelve el problema de la suma de subconjuntos supercreciente encontrando los enteros binarios {r1, r2, . . , rn} tales que:
d=(r1 . b1 + r2 . b2 +...+ rn . bn)
donde los "bi" son los elementos de la mochila privada, en este caso:
136=12.r1+17.r2+33.r3+74.r4+ 157.r5+316.r6, por tanto:
136=12+17+33+74, con lo cual:

r1=r2=r3=r4=1, r5=r6=0

Por tanto el mensaje descifrado se obtiene utilizando: mi = $r_{\pi(i)}$, donde "i" va desde 1 a "n". En este caso aplicando la permutación se obtiene el mensaje en claro:
m1=r3=1, m2=r6=0, m3=r1=1, m4=r2=1, m5=r5=0, m6=r4=1.

Síntesis de un criptosistema asimétrico de clave pública basado en mochilas estilo C-R

El presente sistema criptográfico asimétrico estilo C-R (Chor-Rivest) esta basado en mochilas y utiliza aritmética basada en campos finitos para calcular logaritmos discretos. Es uno de los pocos cripto-sistemas de mochilas que aún no ha sido roto y por lo tanto con posibilidades de utilización. Veamos su arquitectura:

Generación de las claves pública y privada-secreta en el receptor

[1] Se selecciona un campo finito GF(p ^ h) con "p" mayor o igual a "h", de característica "p", por ejemplo GF(7 ^ 4) donde p = 7, h = 4.

[2] Se selecciona un polinomio aleatorio irreducible f(x) de grado "h" sobre Zp, por ejemplo:
f(x)=x ^ 4+3x ^ 3+5x ^ 2+6x+2
de grado h = 4 sobre Z7. Los elementos del campo GF(p ^ h) se representan como polinomios en Zp[x] de grado menor que "h" con multiplicación realizada módulo f(x).

[3] Se selecciona un elemento primitivo aleatorio g(x) del campo GF(p ^ h), por ejemplo,

g(x) = 3x ^ 3 + 3x ^ 2 + 6.

[4] Para cada elemento "i" del campo Zp se calcula el logaritmos discreto: ai = $\log_{g(x)}(x + i)$. Así:

a0 = $\log_{g(x)}(x+0)$ = 1028,
a1 = $\log_{g(x)}(x+1)$ = 1935,
a2 = $\log_{g(x)}(x+2)$ = 2054,
a3 = $\log_{g(x)}(x+3)$ = 1008,
a4 = $\log_{g(x)}(x+4)$ = 379,
a5 = $\log_{g(x)}(x+5)$ = 1780,
a6 = $\log_{g(x)}(x6)$ = 223.

[5] Se selecciona una permutación aleatoria π de números enteros entre cero y (p-1), por ejemplo:

π(0) = 6,
π(1) = 4,
π(2) = 0,
π(3) = 2,
π(4) = 1,
π(5) = 5,
π(6) = 3.

[6] Se selecciona un número entero aleatorio "d" perteneciente al intervalo cerrado [0, (p ^ h-2)], por ejemplo d=1702.

[7] Se calcula:
ci = ($a_{\pi(i)}$ + d) mod (p ^ h - 1)
donde "i" pertenece al intervalo cerrado [0, (p-1)]. En este caso:
c0 = (a6 + d) mod 2400 = 1925,
c1 = (a4 + d) mod 2400 = 2081,
c2 = (a0 + d) mod 2400 = 330,
c3 = (a2 + d) mod 2400 = 1356,
c4 = (a1 + d) mod 2400 = 1237,
c5 = (a5 + d) mod 2400 = 1082,
c6 = (a3 + d) mod 2400 = 310.

[8] La clave pública del receptor es:
((c0,c1,c2,c3,c4,c5,c6), p=7, h=4).

[9] La clave privada del receptor es:

(f(x), g(x), π , d).

Proceso de cifrado en el emisor

[1] El emisor obtiene la clave pública del receptor de alguna autoridad confiable.

[2] Representa el mensaje "m" en claro, (por ejemplo: m = 22 = 10110) a enviar al receptor cifrado como una cadena binaria de longitud z = $\log_2$ (p! / (h! (p-h)!) = 5 bits donde p! representa el factorial de "p" cuyo valor se calcula realizando el producto p! = (1 . 2 . 3 . . . p).

[3] Transformar la representación binaria en 5 bits del mensaje en claro "m" en una cadena binaria "M" de longitud "p" que presenta exactamente "h" bits a uno utilizando el siguiente algoritmo: Cargar en L el valor de "h", repetir desde i=1 hasta "p": Si m≥[((p-i) !) / (L ! . (p-i-L) !)] entonces hacer:
{ $M_{(i-1)}$ = 1 ;
m = m - [((p-i) !) / (L ! . (p-i-L) !)] ;
L=L-1 }
en caso contrario hacer:
{ $M_{(i-1)}$ = 0 }.

La operación:
X [(p !) /(L ! . (p - L) !)] = 1 si L = 0 para p ≥ 0. Si p = 0 el resultado es X = 0 para L 1. En este caso:
M = 1011001.

[4] Calcular:

$c = \sum_{i=0}^{p-1} Mi \cdot ci \bmod (p \hat{} h - 1) =$
(c0 + c2 + c3 + c6) mod 2400 = 1521.

[5] Enviar al receptor el criptograma o texto cifrado c = 1521.

Proceso de descifrado en el receptor a partir del criptograma recibido y su clave privada

[1] Calcula:
r = (c – hd) mod (p ^ h -1) = 1913.

[2] Calcula:
u(x) = g(x) ^ r mod f(x) = x ^ 3 + 3x ^ 2 + 2x + 5.

[3] Calcula: s(x) = u(x) + f(x) = x ^ 4 + 4x ^ 3 + x ^ 2 + x.

[4] Se factoriza:

$s(x) = \prod_{j=1}^{h} (x+tj) =$
x(x+2)(x+3) (x+6), por tanto:
t1 = 0, t2 =2, t3=3, t4=6.

[5] Los componentes de M a uno tienen índices $\pi^{-1}(tj)$ con "j" en el intervalo [1, h], en este caso: $\pi^{-1}(0)=2$, $\pi^{-1}(2) = 3$, $\pi^{-1}(3) = 6$, $\pi^{-1}(6) = 0$, los restantes componentes son cero; por tanto:

M = 1011001.

Para recuperar "m" a partir de M se utiliza el algoritmo: m = 0, L = h, repetir desde i = 1 hasta "p":
Si $M_{(i-1)} = 1$, entonces:
m = (m + [((p-i) !) / (L ! . (p-i-L) !)]), L = (L-1). En este caso se recupera el texto en claro m = 22.

Transformación de un mensaje m de z bits a una cadena M de p bits con h unos

Veamos los pasos que el algoritmo antes descrito genera. Sea el mensaje en claro a transmitir de "z" bits m = 22 con z = 5 bits, donde su representación binaria es m = 22 = 10110. El cálculo de "z" se realiza con la expresión:
$z = \log_2 (p ! / (h ! (p-h) !) = 5$ bits.
Proceso: L = h = 4, desde i=1 hasta i=p=7, hacer:
Si m≥[((p-i) !) / (L ! . (p-i-L) !)], entonces hacer:
{ $M_{(i-1)} = 1$;
m = m - [((p-i) !) / (L ! . (p-i-L) !)] ; L=L-1 } en caso contrario hacer:
{ $M_{(i-1)} = 0$}.
Para i=1 se tiene m=22≥15, luego M_0=1, m = 22-15=7, L=3.
Para i=2 se tiene m=7≤ 0 luego M_1= 0.
Para i=3 se tiene m=7≥ 4, luego M_2= 1, m = 7-4=3, L=2.
Para i=4 se tiene m=3≥3, luego M_3=1, m= 3-3=0, L=1.
Para i=5 se tiene m=0≤ 2, luego M= 0.
Para i=6 se tiene m=0≤ 1, luego M= 0.
Para i=7 se tiene m=0≥0, luego M=1, por tanto:
M= M_0 M_1 M_2 M_3 M_4 M_5 M_6= 1011001 con h=4 unos y de longitud p=7 bits.

Transformación de una cadena M de p bits con h unos en un mensaje m de z bits

Dada la cadena binaria:

M = 1011001

veamos los pasos que el algoritmo antes descrito genera para obtener el mensaje en claro a transmitir de "z" bits m = 22 con z = 5 bits, donde su representación binaria es m = 22 = 10110. El cálculo de "z" se realiza con la expresión:
$z = \log_2 (p ! / (h ! (p-h) !) = 5$ bits.
Proceso: m = 0, L = h = 4, desde i = 1 hasta i = p = 7 hacer:
Si $M_{(i-1)} = 1$ entonces hacer:
{m= m + [((p-i) !) / (L ! . (p-i-L)i)] ; L = L-1 } en caso contrario no hacer nada. En este caso:
Para i = 1 se tiene M_0 = 1, luego m = 15, L = 3.
Para i = 2, M_1= 0, luego nada.
Para i = 3, se tiene M_2=1, luego m = 15 + 4 = 19, L = 2.
Para i =4, se tiene M_3 = 1, luego m = 19 + 3 = 22, L = 1.
Para i =5, M_4= 0, luego nada.
Para i =6, M_5= 0, luego nada.
Para i =7, se tiene M = 1, luego m = 22 + 0 = 22, L = 0.
Por tanto al final m = 22.

Bibliografía

- Areitio, J. "Análisis y Desarrollo de Cripto-sistemas Probabilísticos". Rev. Española de Electrónica. Nº 586.
- Schmeh, K. "Cryptography and Public Key Infrastructure on the Internet". John Wiley & Sons Ltd. 2003.❑