Síntesis y análisis de criptosistemas asimétricos

Prof. Dr. Javier Areitio Bertolín
Director del Grupo de Investigación Redes y Sistemas. Catedrático de la Facultad de Ingeniería. ESIDE. Universidad de Deusto
jareitio@eside.deusto.es

En el presente artículo se aborda el análisis y síntesis de una tecnología criptográfica catalogada como asimétrica o de clave pública que asigna a cada dispositivo de una red dos claves una pública (que se sitúa en una Autoridad de Certificación para general conocimiento) y otra secreta-privada (que nadie debería conocer).

Los criptosistemas asimétricos permiten desarrollar mecanismos para cifrado (con vistas a garantizar la confidencialidad) y firma digital (con vistas a garantizar la integridad y autenticación); el no repudio sólo se puede garantizar incluyendo entre emisor y receptor una tercera parte confiable TTP, denominada fedatario ó notario electrónico que se encargue de tomar pruebas o evidencias de las identidades de los que se comunican, contenido, sellado temporal, etc. Los criptosistemas asimétricos que se abordan en este artículo son: Mochilas M-H, D-H, RSA, ElGamal y Rabin.

Criptosistema asimétrico basado en mochilas M-H (Merkle-Hellman).

Cada entidad que desea comunicarse debe disponer de dos mochilas o claves una secreta y otra que se hace pública. Supongamos que un emisor desea enviar un mensaje cifrado (o criptograma) a un receptor. Los pasos a seguir son:

1) El receptor dispone de una mochila o clave secreta MS de longitud "n" formada por un conjunto de "n" valores:

MS = (s1,s2,s3, . , sn)

2) El receptor elige en secreto el módulo "p" de la aritmética modular finita "p" debe ser mayor que la suma de todos los elementos de la mochila secreta.

3) El receptor crea una mochila pública MP multiplicando en secreto en aritmética módulo "p" cada valor de la mochila secreta por un valor secreto "a" que tenga inverso,

a·a ^ (-1) = 1 mod p,

MP =

= a·s1 mod p,a·s2 mod p,., a·sn mod p

4) Si un emisor desea enviar al receptor anterior un mensaje de "n" bits expresado en binario cifrado,

M = (10101 . . .101)

deberá realizar el producto interno de M con la mochila pública de receptor en cuestión MP:

C = M*MP

5) Por su parte el receptor para descifrar el criptograma recibido C y obtener el mensaje original M deberá realizar el producto:

M = C·a ^ (-1) mod p

y comparando con su mochila secreta MS extraer el mensaje binario M.

Propiedades que deben cumplir las mochilas Secreta y Publica M-H y los parámetros *a* y *p*.

1) La mochila secreta,

MS = (b1, b2, . .., bn)

debe ser super-creciente, es decir cada término debe ser mayor que la suma de los anteriores, esto es,

bi > (bi-1 + ... + b1) con i = 1,2,.,n,

(dicho de otra forma, debe estar formada por valores crecientes y cada valor no debe obtenerse sumando una combinación de los anteriores). Por ejemplo la mochila secreta:

MS1 = (3,6,11,30,*50*,105)

no es super-creciente,

50 = 3 + 6 + 11 + 30

La mochila secreta:

MS2 = (7,9,21,121,1,750)

tampoco es super-creciente pues los valores no son crecientes.

En cambio:

MS3 = (3,8,12,25,50,121)

si es super-creciente. Así mismo:

MS4 = (1,2,4,8,16,32,64,128,.,1024)

es super-creciente.

2) El tamaño o longitud de la mochila secreta MS no debe ser múltiplo de 8 bits si se trabaja en ASCII donde el número de bits de la representación ASCII de los mensajes vale 8. Si se trabaja con sextetos no debe ser múltiplo de seis, etc.

3) La longitud de la mochila MS debe ser grande para resistir ataques por fuerza bruta.

4) Los valores que forman la mochila MS deben ser suficientemente elevados para dificultar ataques por fuerza bruta.

5) Para que la mochila sea mas segura, los dos primeros valores de la mochila pública MP "s1" y "s2" deben cumplir: mcd (s1, p) distinto de mcd (s2, p) y a su vez distintos de la unidad (es decir, el módulo "p" no debe tener factores comunes con s1 y s2; no se debe cumplir la primalidad entre ellos) para evitar un ataque de Shamir-Zippel con lo cual la mochila es mas segura.

6) Los valores "a" y "p" deben ser primos, es decir, se debe cumplir:

mcd(a,p) = 1

Es decir si se elige,

p = 198 = 2·3 ^ 2·11

entonces el valor menor de "a" vale 5 y su cuadrado 25.

7) El mínimo valor de "p" se obtiene como el mínimo mayor de la suma de valores de la mochila secreta MS, es decir, "p" igual a la suma de elementos de la mochila secreta mas una unidad.

Densidad de una mochila. Tasa de información de una mochila.

Dada una mochila,

A = (a1, ... ,an)

se define la densidad de una mochila "d" como el cociente entre el número de elementos de la mochila y el tamaño en bits del mas grande de ellos. Es decir: d = n /N donde N es el máximo de los logaritmos en base 2 de los números "ai". Las mochilas M-H suelen tener densidad menor de la unidad.

Así mismo, se define la tasa de información de una mochila R como el cociente entre el logaritmo en base

2 del número de posibles mensajes en claro dividido entre el logaritmo en base 2 del número posible de mensajes cifrados. Para la mochila M-H R vale la unidad.

Síntesis de una mochila publica de longitud nueve supercreciente

Dada una mochila secreta MS se puede obtener la mochila pública MP:

1) Supongamos que la mochila secreta de un receptor es:

MS=(2,5,9,21,45,103,215,450,946)

2) Supongamos que los parámetros a=1289 y p=2003. Por tanto:

a ^ (-1)=317

3) La mochila pública será:

MP=(2·1289,5·1289,9·1289, 21·1289,45·1289,103·1289, 215·1289,450·1289,946·1289)= (575,436,1586,1030,1921,569, 721,1183,1570).

4) Si tenemos como mensaje,

M=101100111

el criptograma a enviar será:

C=M*MP=

=575+1586+1030+721+1183+1570=

=6665

El receptor descifrará el mensaje a partir del criptograma C y a ^ (-1) utilizando:

M=C·a ^ (-1) mod p=

=6665·317 mod 2003=1643

este valor comparando con la MS permite recuperar M=101100111.

Calculo del producto interno para obtener el criptograma con mochilas

Conocido el mensaje M y mochila pública MP determinar el mensaje cifrado:

1) Sea la mochila pública de longitud cuatro:

MP=(3,7,50,157)

2) Sea el mensaje en binario de longitud medio byte:

M=(1010)

3) El criptograma es:

C=M*MP=(3,7,50,157)*(1010)=

=3+50=53

Al resultado no se le aplica el módulo p.

Determinación del mensaje descifrado en texto en claro utilizando mochilas

Se trata de obtener el mensaje en claro conociendo el criptograma, el inverso de "a" módulo p (es decir, el co-primo de a módulo p), el módulo p y la mochila secreta MS:

1) Supongamos que el criptograma vale C = 3155.

2) El parámetro a ^ (-1)=325 y el módulo de la aritmética modular finita vale p =2503. Por tanto,

a=1987

3)El mensaje descifrado,

M=C·a ^ (-1) mod p=

=3155·325 mod 2503=1648

4) Supongamos que la mochila secreta es de longitud 9 vale:

MS=(7,211,1,4,998,18,43,78, 435).

5) Como la longitud de MS es nueve el número de bits de M será 9. Se compara M=1648 con MS y se comienza restando 1648 del valor mayor de MS, en este caso 998 obteniendo 650 que se resta por el valor inmediato mas grande que es 435 el resultado es 215. Se resta del inmediato inferior mas grande que es 211 se obtiene 4. Se resta del valor de MS 4 y se llega a cero. Por tanto:

M=1648=010110001

ya que se ha restado de 211, 4, 998 y 435 (valores a "1") el resto a cero.

Criptosistema D-H (Diffie-Hellman) para intercambiar un secreto compartido o clave de sesión simétrica

El criptosistema D-H permite que el emisor A y el receptor B separados a través de una red puedan acordar una clave privada ó secreto compartido S de sesión utilizando un protocolo de dos envíos (uno de A a B y otro de B a A).

Es necesario que A y B custodien en secreto cada uno una clave personal no transferible. El secreto del emisor A se llama X y el secreto del receptor B se llama Y.

Tanto A como B utilizan dos números primos grandes en secreto denominados "g" y "n", este segundo se utiliza como módulo para la aritmética modular finita que permite realizar los cálculos de exponenciación.

El procedimiento es el siguiente:

1) El emisor A envía al receptor B el valor: g^x mod n.

2) El receptor B calcula con la información recibida:

$(g^x \bmod n)^y = g^{xy} \bmod n =$

=Clave común de sesión=S

3) El receptor B envía al emisor A el valor: g^y mod n.

4) El emisor A calcula con el valor recibido de B:

$(g^y \bmod n)^x = g^{xy} \bmod n =$

=Clave común de sesión=S.

Criptosistema asimétrico RSA (Rivest – Shamir – Adleman)

Desarrollado en 1977 por Ronald Rivest, Adi Shamir y Leonard Adleman. Utiliza dos claves una pública y otra secreta. El sistema es robusto cuando se utilizan claves de 1024 o 2048 bits. La seguridad de RSA se basa en lo complicado de encontrar la clave privada a partir de la pública es decir la factorización del módulo "n" en sus dos factores primos. Entre sus aplicaciones es de destacar el protocolo de seguridad PGP.

Cada entidad que desea comunicarse debe disponer de dos claves una secreta-privada "d" y otra que se hace pública "e". Supongamos que un emisor desea enviar un mensaje cifrado (o criptograma C) a un receptor. Los pasos a seguir son:

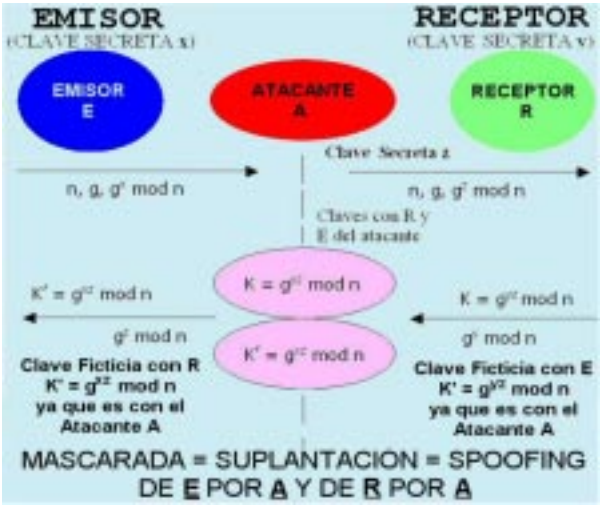


Figura 1.-Esquema de un ataque "Man – in – the – Middle" a la Técnica de DH (Diffie-Hellman)

Figura 3. Resumen de la generación de claves y procesos de cifrado y descifrado con el criptosistema RSA

1) Seleccionar dos primos grandes *p* y *q* en secreto. Calcular y hacer público (por ejemplo en una Autoridad de Certificación, tablón de anuncios electrónico, páginas amarillas, etc) el resultado: $n = p*q$.
2) Calcular $j(n) = (p-1)*(q-1)$. Seleccionar y hacer público la clave pública "*e*" tal que: $mcd(e,j(n)) = 1$ son primos entre sí, donde el valor de "*e*" esta comprendido *entre* $1 < e < j(n)$.
3) Calcular en secreto la clave secreta:

$$d = e^{-1} \bmod j(n)$$

donde, $e \cdot e^{-1} = 1 \bmod j(n)$.
4) Clave pública del receptor: *(e, n)* y la Clave privada del receptor: *(d, n)*.
5) Para cifrar un mensaje M:

$$C = M^e \bmod n$$

donde "*e*" clave pública del receptor.

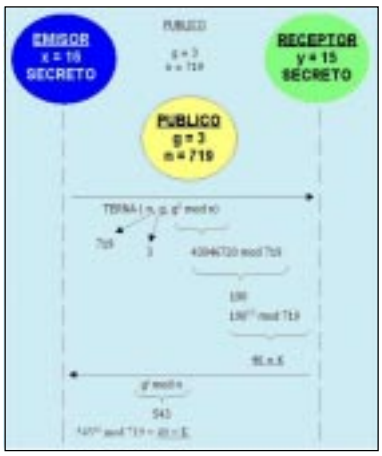


Figura 2. Esquema de un Intercambio del secreto compartido K basado en DH (Diffie–Hellman).

6) Para firmar digitalmente el resumen-hash de un mensaje denominado M: $F = M^d \bmod n$, donde "*d*" es la clave secreta del emisor.
7) Para descifrar un criptograma C en el receptor: $M = C^d \bmod n$, donde "*d*" es la clave secreta del receptor.
8) Para comprobar la validez de una firma electrónica "*F*" recibida en el receptor:
$V = F^e \bmod n$, donde "*e*" es la clave pública del emisor y *V* es el resumen o hash del mensaje en claro recibido.

Aplicación del criptosistema RSA

CASO–1

Dados p=7, q=17, determinar la clave pública y privada RSA del receptor. Hallar el criptograma C para el mensaje M = 19 enviado por el emisor.

El proceso es:
(1) Seleccionar p∧q: (p=7, q=17).
(2) Calcular: n=p*q=7 *17=119.
(3)Calcular:
φ(n)=(p–1)*(q–1)=6*16=96.
(4) Seleccionar e tal que sea el menor entre:

mcd (e,φ (n))=1
con, 1<e<φ (n)=>e=5.

(5) Calcular d como el coprimo de "e" módulo φ (n):
d=e^{-1} mod φ (n), de forma que,
d*e=1 mod j (n) =>d=77.
(6) La clave pública es: (e, n) y clave secreta-privada es: (d, n).
(7) Cifrar: C=M^e mod n.
(8) Descifrar: M=C^d mod n. En este caso: M=19→C=66.

CASO-2

Determinar la clave privada RSA *(e,n)* conocido p=53, q=61, d=791. Hallar la clave pública RSA *(d,n)*, con d=791, p=53;

q=61→n= 53*61 =3233
f(n)=52 *60=3120 →
e=d^{-1} mod f (n)=71.

Clave Privada (e, n) = (71, 3233).
Clave Publica (d, n) = (791, 3233).

CASO-3

Determinar el criptograma del mensaje en claro: M=ES SECRETO, como p=11 y q=17 por tanto n=87. Así φ(n)=φ (187)=10*16=160; d=7; donde mcd (7,160)=1. Por tanto: e=23; 23*7=161=1 (mod 160).

Clave Pública (23, 187)=(e, n). Para cifrar el texto en claro sustituimos las letras por los siguientes códigos: A=01; B=02; C=03; D=04; E=05; F=06..; R=19; S=20; T= 21.. blanco=00. Texto en claro codificado en números: 05200020050319052116. El texto subdividido en bloques queda 05 20 00 20 05 03 19 05 21 16.
Texto a cifrar: p y q primos; n=p*q, φ(n)=(p-1)*(q-1), "d" ha de ser primo con φ(n)=(p-1)*(q-1). "

e" es entero menor que "n" tal que e*d=1 (mod φ(n)). Clave pública (e, n). Ciframos el texto subdividiendo en bloques M$_i$.

Texto Cifrado

C1 = 05 ^ 23 (mod 187) = 180;
C2 = 20 ^ 23 (mod 187) = 113;
C3 = 00 ^ 23 (mod 187) = 000;
C4 = 20 ^ 23 (mod 187) = 113;
C5 = 05 ^ 23 (mod 187) = 180;
C6 = 03 ^ 23 (mod 187) = 181;
C7 = 19 ^ 23 (mod 187) = 094;
C8 = 05 ^ 23 (mod 187) = 098;
C9 = 21 ^ 23 (mod 187) = 098;
C10=16 ^ 23 (mod 187) = 169;

Resultado final del criptograma: 180 113 000 113 180 181 094 180 098 169.

Receptor recupera el mensaje descifrando:

M1 = 180 ^ 7 (mod 187) = 05;
M2 = 113 ^ 7 (mod 187) = 20;
M3 = 000 ^ 7 (mod 187) = 00;
M4 = 113 ^ 7 (mod 187) = 20;
M5 = 180 ^ 7 (mod 187) = 05;
M6 = 181 ^ 7 (mod 187) = 03;
M7 = 094 ^ 7 (mod 187) = 19;
M8 = 180 ^ 7 (mod 187) = 05.

Criptosistema asimétrico basado en Elgamal

Cada entidad que desea comunicarse debe disponer de dos claves una secreta-privada "x_B" y otra que se hace pública "y_B".

Supongamos que un emisor desea enviar un mensaje cifrado (o criptograma) a un receptor. Los pasos a seguir son:

1) Se selecciona un número primo p.
2) Se selecciona un elemento primitivo o raíz primitiva a.
3) El receptor selecciona un número secreto x_B.
4) El receptor pública su clave pública $y_B = a^{xB} \bmod p$.
5) El par de claves "Secreta – Pública" del receptor es : (x_B, y_B).
6) El emisor selecciona un número aleatorio de un solo uso: $k_1 (0 \le k_1 \le (p-1))$ y calcula $k = y_B^{k1} \bmod p$.
7) Si el emisor desea cifrar el mensaje M realizará dos operaciones: $C_1 = a^{k1} \bmod p$ y $C_2 = k \cdot M \bmod p$ y envía al receptor el par de valores: (C_1, C_2). Como se observa, el criptograma ocupa el doble de RSA.
8) El receptor extrae K: $K = C_1^{xB} \bmod p$.
9) El receptor extrae M: $M = C_2 \cdot K^{-1} \bmod p$, donde K^{-1} es la inversa de K módulo p.

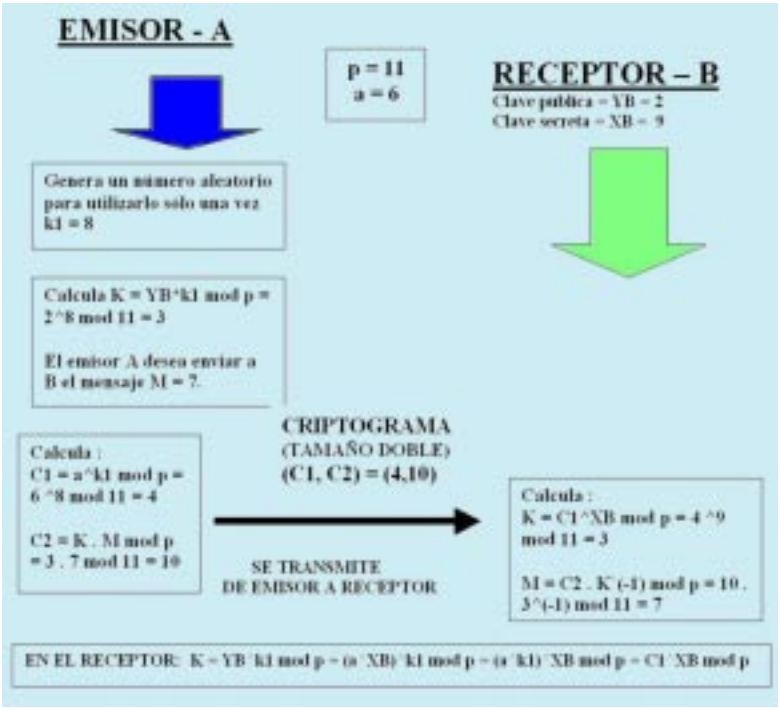
Determinacion de un criptograma Elgamal a partir de un mensaje en claro

Si se elige como número primo *p = 97* y la raíz primitiva es: *a = 5.* Sea el mensaje a cifrar: *M = 3* (se desea enviar al receptor). Se pide:

(a) Calcular las claves "publica – privada" del receptor, si clave secreta es => $x_B = 58$.
(b) ¿Cuál es la clave K del emisor, si el emisor selecciona $K_1 = 36$?
(c) ¿Qué envía el emisor por la línea de transmisión? (¿(C_1, C_2)?)..
(d) ¿Cómo se descifra en el receptor (determinar K y el texto en claro)?.

El proceso es el siguiente:

1) Las claves del receptor son:
$x_B = 58 \rightarrow$ Secreta;
$y_B = a^{XB} \bmod p = 5^{58} \bmod 97 = 44 \rightarrow$ Pública.
2) El emisor calcula la clave:
$K = y_B^{K1} \bmod p = 44^{36} \bmod 97 = 75$.
3) El emisor envía al medio de transmisión el par:
$C_1 = a^{K1} \bmod p = 5^{36} \bmod 97 = 50$;
$C_2 = K*M \bmod p = 75*3 \bmod 97 = 31$.
4) El receptor descifra:
(a) $K = C_1^{XB} \bmod p = 50^{58} \bmod 97 = 75$.
(b) Inversa de K => $K*K^{-1} = 1 \bmod 97$ => $75*K^{-1} = 1 \bmod 97$ => $K^{-1} = 22$.
(c) $M = C_2 * K^{-1} \bmod p = 31 \cdot 22 \bmod 97 = 3$ (=3) c.q.d.



Criptosistema probabilístico asimétrico de Rabin

Cada usuario elige dos números primos grandes (de 1024 bits de longitud) "p" y "q" cada uno igual a 3 módulo 4 (es decir cuando se dividen por 4 dan de resto 3) y forma el producto $n = p \cdot q$.

La clave pública es el número "n". La clave privada-secreta son los números "p" y "q". Para cifrar un mensaje M se forma el texto cifrado $C = M \wedge 2 \bmod n$.

Para descifrar conocido el criptograma C se utilizan las siguientes fórmulas que permiten obtener las cuatro raíces cuadradas módulo "n" de C:

1) "a" y "b" cumplen con: $a.p + b.q = 1$;
$r = c \wedge (p+1)/4 \bmod p$;
$s = c \wedge (q+1)/4 \bmod q$;
$x = (a \cdot p \cdot s + b \cdot q \cdot r) \bmod n$;
$y = (a \cdot p \cdot s - b \cdot q \cdot r) \bmod n$
2) Las cuatro raíces cuadradas son:
M1 = x; M2 = - x ; M3 y; M4 = -y

Figura 4. Esquema de un Proceso de Cifrado y Descifrado utilizando un Sistema Criptográfico basado en ElGamal.

Una de las cuatro raíces es M, una segunda raíz es n – M y las otras dos son valores negativos de cada una. El criptosistema de clave pública de Rabin también puede formularse de otra forma:

1) Dada una clave pública "n" (por ejemplo 77) y un valor "b" entre 0 y (n-1) (por ejemplo b=9 con 0<=9<=76).

2) Dada una clave secreta-privada "p" y "q" (por ejemplo p=7 y q=11 donde n=p·q=7.11=77) y donde p=7=3 mod 4 y q=11=3 mod 4.

3) Para cifrar el mensaje M=2 se utiliza el criptograma:

C=(M ^ 2+b· M) mod n=
=(2 ^ 2+9. 2) mod 77=22

4) Para descifrar el criptograma C= 22, el receptor calculará:

M=([(b ^ 2/4)+C]1/2-b/2) mod n
=([(81/4)+22] ^ 1/2 - 9/2) mod 77
=([1 + 22] ^ 1/2 - 43) mod 77
=[23] ^ 1/2 -43) mod 77.

Como 23 ^ 1/2 mod 77 tiene cuatro raíces ± 10 mod 77 y ± 32 mod 77; Los cuatro resultados que obtendríamos son:

10–43 mod 77=44;
–10– 43 mod 77=24;
32–43 mod 77=66;
–32–43 mod 77=2;

Fig. 5.- Esquema del Mecanismo de Firma Electrónica y Cifrado basado en ElGamal.

de los cuales sólo el último es el válido para M=2). En lo anterior:

2 ^ (-1) mod 77=39 y
4 ^ (-1) mod 77=58. Así mismo
23 ^ (p+1/4) mod 7=23 ^ 2 mod 7=
= 2 ^ 2 mod 7=4;
23 ^ (q+1/4) mod 11=1

Aplicación del criptosistema de Rabin

Supongamos que p=7, q=11, por tanto n=77. Así mismo (–3)·7+ 2·11=1 por consiguiente a=–3 y b =2. Supongamos que se utilizan mensajes de tres bits cuyos bits se duplican hasta formar 6 bits, es decir hasta el número 63 en decimal. Supongamos que el dato a transmitir es 101 ó 5, en decimal su duplicación da 101101, es decir 45 en decimal. Para cifrar se aplica: C=M ^ 2 mod 77=23. Para descifrar:

r=23 ^ 2 mod 7=4,
S=23 ^ 3 mod 11=1;
x=((-3)·7·1+2·11· 4) mod 77=67;
y=((-3)·7·1–2·11·4) mod 77=45;

Estas son dos de las cuatro raíces cuadradas y las otras dos son (– x mod 77)=10 y (–y mod 77)= 32 En binario las cuatro raíces cuadradas son en decimal:

67=1000011; 45=101101
10=001010; 32=100000

Por tanto el valor 45 tiene la redundancia requerida de modo que es el resultado correcto.

Problemática del uso repetido del valor aleatorio k1 en Elgamal

Dado un mensaje M1 el criptograma es:
(C1, C2)=(a ^ k1 mod p, (K ·M1) mod p). Dado otro mensaje M2 con el mismo valor de k1 su criptograma es: (C1', C2')=(C1, (K ·M2) mod p). Por tanto: C1'=C1 y C2'/C2=M2/M1 y M2=M·C2'· C2 ^ (-1). Si k1=8, p=11, a=6, clave pública del receptor YB=2, entonces si M1=7 el criptograma es (C1=4, C2=10) y si M2=5 entonces con el mismo k1 el criptograma es (C1'=4, C2'=4) con lo que se puede recuperar M2 utilizando:

M2=M1·C2'.C2 ^ (-1)=7·4·10 ^ (-1)=5.

La simbología A ^ (-1) significa elevar el valor A a la (-1), es decir calcular el inverso multiplicativo de A.

Aspectos Finales

Nuestro grupo de investigación ha implementado estos mecanismos criptográficos con valores mucho mas grandes en comparación con los utilizados en los ejemplos del presente artículo. Así mismo se han sometido a criptoanálisis variados y ataques de diversas formas obteniendo resultados negativos, lo cual demuestra que los desarrollos criptográficos asimétricos sintetizados han sido muy satisfactorios. La obtención de números primos elevados es fundamental en esta área; un número primo muy elevado es [2 ^ 6972593)– 1], es decir 2 elevado a 6972593 menos una unidad. Utilizando RSA con p=99103 y q=80177, la clave pública e=2968833449 y la privada d=5144067833, el cifrado de M=1905140400 da como resultado C=6774683355. Con D-H, si la clave secreta del emisor es x=5 y la del receptor vale y=7, sabiendo n=17 y g=3 la clave común será K=10.

Bibliografía

- Areitio, J. "Desarrollo de un Criptosistema Probabilístico". Revista Española Electrónica. nº 586. Sept.2003.
- Ferguson, N. & Schneier "Practical Cryptography" J.Wiley & Sons. 2003.
- Mao, W. "Modern Cryptography: Theory and Practice". Prentice-Hall. PTR. 2003.
- Menezes, A.J., Van Oorschot, P.C. and Vanstone, S.A. "Handbook of Applied Cryptography". CRC Press. FL. 1997.
- Schmeh, K. "Cryptography and Public Key Infrastructure on the Internet". John Wiley & Sons Ltd. 2003. ❑