Desarrollo de un sistema criptográfico probablemente seguro de clave pública estilo Rabin tradicional

Por J. Areitio

El Prof. Dr. Javier Areitio Bertolín es Catedrático de la Facultad de Ingeniería (ESIDE) y Director del Grupo de Investigación Redes y Sistemas de la Universidad de Deusto.

jareitio@eside.deusto.es

En el presente artículo se realiza la síntesis de un cripto-sistema asimétrico de clave pública siguiendo un enfoque estilo Rabin clásico. Resulta ser un sistema cuyo proceso de cifrado es más eficiente que el del sistema criptográfico RSA más utilizado hoy en día, aunque el proceso de descifrado sea de similar eficiencia en comparación con RSA. Así mismo se describen las técnicas CRT (Teorema del Resto Chino), EEA (Algoritmo Extendido de Euclides) y álgebra de Hill muy utilizados en Criptografía aplicada.

El cripto-sistema estilo Rabin clásico es el primer cripto-sistema de clave pública probablemente seguro. Al igual que el criptosistema RSA, la seguridad del sistema criptográfico estilo Rabin se basa en la dificultad de factorizar números grandes en primos:

(N = p.q).

Por tanto romper Rabin es al menos tan difícil como factorizar:

N = p.q.

En el cripto-sistema estilo Rabin, dado un mensaje "m" en texto en claro genera un criptograma "C" cuyo descifrado es ambiguo ya que genera cuatro posibles resultados todos ellos factibles de los cuales sólo uno es el correcto.

Para resolver esta ambigüedad se debe incluir cierta redundancia en "m" para que el receptor sea capaz de conocer cual de las cuatro soluciones es la original del emisor.

Los cripto-sistemas de clave pública necesitan publicar en un directorio de clave pública protegido (por ejemplo una Autoridad de Certificación) sus claves públicas de modo que dos partes que desean comunicarse puedan comenzar la comunicación cifrada aunque no se conozcan, así mismo pueden firmar sus mensajes cifrando con su clave secreta el resumen de dicho mensaje.

Necesidad de redundancia en el texto en claro a cifrar

El desarrollo que se realiza en este artículo es el de un sistema criptográfico estilo Rabin tradicional que como es asimétrico nos permite realizar un conjunto muy variado de operaciones criptográficas como cifrar, firmar digitalmente, realizar funciones unidireccionales, etc. Los cripto-sistemas estilo Rabin son computacionalmente seguros contra ataques de texto en claro elegido bajo la hipótesis de que el módulo N = p.q no pueda ser factorizado. Como se verá la función de cifrado no es inyectiva, de modo que el descifrado no puede hacerse de una manera no ambigua. De hecho, siempre van a existir cuatro posibles textos en claro que pueden ser el cifrado de cualquier texto cifrado dado. En general no existirá forma de distinguir cual de los cuatro posibles textos descifrados es el correcto, a menos que el texto en claro de partida contenga alguna redundancia para eliminar tres de los cuatro posibles valores generados en el descifrado. En el descifrado de este tipo de sistema criptográfico será necesario determinar la raíz cuadrada de "t" mod N, donde N=p.q (además se cumple que p = q = 3 mod 4), dos raíces cuadradas de t mod p son:

$$\{+t^{(p+1)/4} \bmod p\ ,\ -t^{(p+1)/4} \bmod p\}$$

y dos raíces de t mod q son:

$$\{+t^{(q+1)/4} \bmod q\ ,\ -t^{(q+1)/4} \bmod q\}.$$

Descripción del sistema criptográfico estilo Rabin

Veamos los pasos a seguir:

1) Proceso de generación de las claves pública y privada del receptor. Se parte de seleccionar en secreto dos números primos distintos "p" y "q" congruentes 3 módulo 4 (es decir p = q = 3 mod 4), por ejemplo sean p = 127, q = 131, donde: p = q = 3 mod 4. Se calcula su producto: N = (p . q) = 16637. Se elige aleatoriamente un valor "B" perteneciente al intervalo cerrado y acotado [0, N-1], por ejemplo B = 12345. La clave pública del receptor es (B, N) y la clave secreta del receptor es (p, q).

2) Proceso para cifrar en el emisor con la clave pública del receptor. Si el mensaje en texto en claro que el emisor desea enviar cifrado al receptor es m = 4410 ("m" debe estar comprendido en el intervalo de posibles números enteros positivos [0, N-1]), entonces el mensaje cifrado ó criptograma "C" a enviar al receptor se calcula utilizando la clave pública del receptor (B, N) y la expresión: C = m (m + B) mod N = 4633.

3) Proceso de descifrado en el receptor con la clave secreta del receptor. El receptor recibe el criptograma "C" del emisor y con su clave secreta (p, q) descifra el criptograma (ó texto cifrado) "C" utilizando la siguiente expresión: m = (s – B/2) mod N, donde:

$$s = \sqrt{t} \bmod N,$$

con:

$$t = (B^2/4 + C) \bmod N;$$

para calcular "s" se determinan previamente:

$$\sqrt{t} \bmod p = t^{(p+1)/4} \bmod p,$$

así como:

$$\sqrt{t} \bmod q = t^{(q+1)/4} \bmod q$$

Por tanto, primero calculamos:

$$t = (B \wedge 2/4 + C) \bmod N = 1500$$

a continuación los dos valores:

$$\sqrt{t} \bmod p = 1500^{(p+1)/4} = \{+22y\text{-}22 \bmod 127\}$$

y:

$$\sqrt{t} \bmod q = 1500^{(q+1)/4} \bmod q = \{+37 \text{ y } -37 \bmod 131\}$$

Utilizando el teorema del resto chino se calcula:

$$s = \sqrt{t} \bmod N = \{+3705 \text{ y } -3705 \text{ ó } +14373 \text{ y } -14373 \bmod 16637\},$$

por tanto:

$$m = (s - B/2) \bmod N =$$

{5851, 15078, 16519, 4410}
Donde dado las dos congruencias:
x = 22 mod 127, x = 37 mod 131
se calcula: x = 22 + 127u,
entonces: 22 + 127u = 37 mod 131
por tanto: 127u = 15 mod 131
es decir : u = 15/127 mod 131

Aplicación práctica del cripto-sitema estilo Rabin

1) Proceso de generación de clave pública y privada. Sean p = 7, q = 11, por tanto N = (p.q) = 77. Sea B = 9. La clave pública es (B, N) y la clave privada es (p, q).

2) Proceso de cifrado en el emisor. Sea el mensaje a cifrar por el emisor m = 2, el texto cifrado será:

C = m (m + B) mod N = 22.

3) Proceso de descifrado en el receptor. El receptor con el criptograma "C" y su clave secreta (p, q) descifra el texto recibido utilizando:

$$m = \sqrt{(B^2/4 + C)} - B/2 \mod N = \sqrt{(1 + C)} - B/2 \mod N = \sqrt{(1 + 22)} - 43 \mod 77,$$

ya que:

$(B^2/4) \mod 77 = 4/4 = 1.$

Para encontrar la raíz cuadrada de 23 módulo N = 77 primero calculamos las raíces cuadradas de 23 modulo p = 7 y modulo q = 11, ya que 7 y 11 son congruentes a 3 modulo 4 por tanto las raíces cuadradas de 23 modulo 7 son:

$23^{(7+1)/4} \mod 7 = 4$

y las raíces cuadradas de 23 modulo 11 son:

$23^{(11+1)/4} \mod 11 = 1.$

Utilizando el teorema del resto chino se calculan las cuatro raíces de 23 modulo 77 resultando:

{+10, -10, +32, -32}.

Por último los cuatro posibles textos en claro descifrados son:

(10 – 43) mod 77 =
44, (67 – 43) mod 77 =
24, (32 – 43) mod 77 =
66, (45 – 43) mod 77 = 2.

Teorema del Resto Chino: CRT. Casos prácticos.

Para poder realizar los cálculos de un cripto-sistema estilo Rabin clásico y de otros cripto-sistemas asimétricos similares es necesario aplicar el Teorema del Resto Chino ó CRT (Chinese Remainder Theorem) que dice que dado N = (m1 . m2) donde el máximo común divisor mcd(m1, m2) = 1 se puede obtener "x" mod N conociendo las dos congruencias: {x = a1 mod m1 ; x = a2 mod m2}. Veamos algunos casos prácticos con números:

Caso 1

Dado:
{x = 4 mod 7; x = 3 mod 5}
calcular: x = a mod 35,
donde: 35 = (7 . 5).

Para ello planteamos: x = 4 + 7u, así como: x = 3 mod 5, entonces sustituyendo la primera en la segunda: 4 + 7u = 3 mod 5, de este modo: 7u mod 5 = 2u = 3 – 4 = 4 mod 5, así: u = 4/2 mod 5 = 2 mod 5, ya que: 2 ^ -1 . 2 = 1 mod 5, es decir: 2 ^ - 1 mod 5 = 8. Por tanto: x = 4 + 7u = (4 + 7 . 2) mod 35 = 18 mod 35, con lo que:

x = 18 mod 35.

Caso 2

Dado:
{x = 3 mod 7; x = 7 mod 13}
determinar: x = a mod 91
donde: 91 = (13 . 7).

El resultado es x = 59 mod 91.

Caso 3

Conocidos:
{x = 7 mod 11 ; x = 6 modo 13}
hallar: x = a mod 143
donde: 143 = (13 . 11).

Sea: r = 6 . 11 . u + 7 . 13 . v
donde:
u = 11 ^ -1 mod 13 = 6 mod 13;
v = 13 ^ -1 mod 11 = 6 mod 11;
entonces:

x = 6 . 11 . 6 + 7 . 13 . 6 =
6 (66 + 91) = 6 . 157 =
6 . 14 = 84 mod 143,

luego el resultado es:

x = 84 mod 143.

Caso 4

Dado:
{x = a1 mod p ; x = a2 mod q}
determinar: x = a mod n;
donde: n = (p . q),
ademas: mcd(p, q) = 1.

La fórmula que permite calcular "a" es: a = (a1b1q + a2b2p) mod n
donde:
b1 = q ^ -1 mod p, b2 = p ^ -1 mod q

Veamos un caso numérico, sea:
{x = 5 mod 7 ; x = 6 mod 11}
determinar x = a mod 77
donde 77 = (7 . 11).

El valor de:
a = (5 . 2 . 11 + 6 . 8 . 7) mod 77
= 446 mod 77 = 61 mod 77
en este caso:
p = 7, q = 11, n = 77, a1 = 5, a2 = 6,
b = 7 ^ -1 mod 11 = 8,
b1 = 11 ^ -1 mod 7 = 2.

Algoritmo de Gauss. Generalización del CTR para sistemas de más de dos congruencias

Si los números enteros n1, n2, n3, . . . , nk son primos entre si (es decir su máximo común divisor es la unidad), entonces el sistema de congruencias simultaneas:
{x = a1 mod n1, x = a2 mod n2,..., x = ak mod nk} tienen una única solución módulo n = (n1 . n2 .... nk). La solución "x" aplicando el algoritmo de Gauss es:

$$x = \sum_{i=1}^{k} a_i . N_i . M_i \mod n,$$

donde: $N_i = (n/n_i) \mod n_i$,
además: $M_i = N_i \mod^{-1} n_i$
Veamos un caso práctico: dado el par de congruencias {x = 3 mod 7, x = 7 mod 13} calcular x = a mod 91 donde: 91 = (7 . 13). Aplicando el teorema de Gauss:
x = (a1. N1 .M1 + a2. N2. M2) mod n
= (3.13.6) + (7 .7 .15) mod 91 = 59
con: M1 = N1 ^ -1 mod 7 =
13 ^ -1 mod 7 = 6;
M2 = N2 ^ -1mod 13 =
7 ^ -1 mod 13 = 15;

N1 = 91/7 mod 7 = 13;
N2 = 91/13 mod 13 = 7.
Por tanto: x=59 mod 91

Examinemos otro caso: dadas las tres siguientes congruencias: {x=1 mod 4, x =47 mod 81 y x = 14 mod 25} tras aplicar el algoritmo de Gauss se llega al siguiente resultado: x = 6689 mod 8100, donde 8100 = (4 . 81 . 25).

Figura 1. Pasos del Algoritmo EEA aplicado a los valores: a = 4864 y b = 3458 con a > b. El resultado es: d = mcd (a,b) = 38 = (4864)(32) + (3458)(-45)

q	r	x	y	a	b	x_2	x1	y2	y1
-	-	-	-	4864	3458	1	0	0	1
1	1406	1	-1	3458	1406	0	1	1	-1
2	646	-2	3	1406	646	1	-2	-1	3
2	114	5	-7	646	114	-2	5	3	-7
5	76	-27	38	114	76	5	-27	-7	38
1	38	32	-45	76	38	-27	32	38	-45
2	0	-91	128	38	0	32	-91	-45	128

Figura 2. Pasos del Algoritmo EEA aplicado a los valores: a = 21 y b = 16 con a > b. El resultado es: d = mcd (21,16) = 1 = (21)(-3) + (16)(4)

q	r	x	y	a	b	x_2	x_1	y_2	y_1
-	-	-	-	21	16	1	0	0	1
1	5	1	-1	16	5	0	1	1	-1
3	1	-3	4	5	1	1	-3	-1	4
5	0	11	-21	1	0	-3	11	4	-21

Figura 3. Puntos de la curva elíptica $y^2 = (x^3 + x + 1)$ sobre Z_{23}. Expresiones para sumar puntos distintos e iguales.

OBTENCION PUNTOS DE UNA CURVA ELIPTICA PARA CRIPTOGRAFIA:

Dada la curva elíptica $y^2 = (x^3 + ax + b) \bmod p$ donde a = 1, b = 1, p = 23, se cumple la condición $(4a^3 + 27b^2) \bmod 23 = 8$ (distinto de cero). El conjunto de puntos de esta curva es de cardinalidad 28 : {[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, 3), [11, 20), [12, 4), [12, 19), [13, 7), [13, 16), [17, 3), [17, 20), [18, 3), [18, 20), [19, 5), [19, 18), O} donde O es el "punto en el infinito. Se cumple: P + [- P) = O con P = (x, y) ; - P = (x, - y).

FORMULAS DE SUMA:

P(x1, y1) + Q(x2, y2) = (x3, y3) donde x3 = d^2 – x1 – x2; y3 = d(x1 – x3) – y1; { d = (y2 - y1) / (x2 – x1) si P distinto de Q ; d = (3x1^2 + a) / (2y1) si P = Q}. Ejemplo: P(3, 10) + Q(9, 7) = (17, 20) ya que d = - 1/2 mod 23 = 11 con 2^-1 mod 23 = 12.

P(3, 10) + P(3, 10) = 2P = (7, 12) donde d = (3(3^2)+1) / 20) = 4^-1 mod 23 = 6; x3 = (6^2 – 6) mod 23 = 7; y3 = (6(3-7) – 10) mod 23 = - 34 mod 23 = 12.

Algoritmo de Euclides extendido: EEA. Casos practicos

El Algoritmo de Euclides Extendido ó EEA (Extended Euclidean Algorithm) nos permite no sólo determinar el máximo común divisor (mcd) "d" de dos número enteros "a" y "b" sino también nos calcula dos enteros "x" e "y" tales que verifican la expresión:

(ax + by) = d = mcd (a, b)

El algoritmo se puede escribir de la siguiente forma:

1) La entrada: Son dos números enteros no negativos "a" y "b" donde "a" es mayor o igual a "b".

2) La salida: Por una parte el máximo común divisor d=mcd (a, b). Por otra parte dos números enteros "x" e "y" tales que verifican la expresión: (ax + by) = d. El procedimiento es el siguiente:

a) Si b = 0 entonces d←a, x←1, y←0, devolver: (d, x, y)
b) Cargar x2←1, x1←0, y2←0, y1←1
c) Mientras b > 0 "b" mayor que cero) hacer:

c.1) q← Redondeo hacia abajo del cociente (a/b),
r ←(a – qb), x←(x2 – qx1),
y←(y2 – qy1)

c.2) a←b, b←r, x2← x1, x1← x, y2← y1, y1← y.

d) Cargar d←a, x←x2, y←y2, devolver: (d, x, y)

La figura 1 muestra el esquema de pasos seguido para el cálculo del EEA con los valores concretos:

a = 4864, b = 3458

El resultado es doble, por una parte d = mcd (4864, 3458) = 38. Y por otra parte x = 32, y = - 45 verificando la expresión:

(4864)(32) + (3458)(- 45) = 38.

Examinemos algunos casos prácticos para verificar su cumplimiento:

(a) (21)(-3)+(16)(4)=1, ver figura 2.
(b) (101)(-31)+(36)(87) =1.
(c) (131)(- 37)+(48)(101) = 1.
(d) (10)(57) + (7)(- 81) = 3.
(e) (93)(221) + (367)(- 56) = 1.
(f) (7)(3) + (10)(- 2) = 1.
(g) (23)(- 9) + (8)(26) = 1.
(h) (120)(- 9) + (47)(23) = 1, donde – 9 = 120 ^ -1 mod 23.
(i) (81)(94) + (-23)(331) = 1.
(j) (15)(963) + (22)(-657) = {9, - 9}.

El EEA se puede reformular sobre polinomios, de modo que dados dos polinomios:

g(x) = x^10+x^9+x^8+x^6+x^5+ x^4+1
h(x) = x^9+x^6+x^5+x^3+ x^2+1

definidos sobre Z2[x] se llega a que el máximo común divisor es:

mcd(g(x), h(x))= x ^ 3 + x + 1

y además se verifica que: **(x^4)(g(x)) + (x^5+x^4+x^3+x^2+x+1)(h(x)) = (x^3 + x + 1) = mcd(g(x), h(x)).**

Algebra de Hill para la sintesis de cifradores de secreto compartido

El álgebra de Hill permite el desarrollo de cifradores simétricos de clave secreta o lo que es lo mismo de secreto compartido. Examinemos un caso práctico. Supongamos que se elige un alfabeto formado por 26 letras de la A a la Z ({A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z}), para representar los mensajes de texto en claro y los criptogramas o mensajes cifrados. Asignamos a cada carácter alfabético un número entero del 0 al 25, así por ejemplo la A es el cero, la B el uno, la C el dos hasta la Z que es el 25. Se selecciona la clave secreta de este sistema criptográfico que será una matriz cuadrada Z (que tenga matriz inversa, es decir su determinante que sea distinto de cero) de dimensiones "d" filas por "d" columnas formada por números enteros, donde "d" representa el número de caracteres que se cifrarán cada vez (por ejemplo si d = 2, se trabajara con "di-gramas" es decir con grupos de dos letras, si fuese 3 tri-gramas, etc.). Así mismo, la clave secreta compartida entre emisor y receptor debe ser una cadena de (d . d) caracteres, es decir que tenga raíz cuadrada exacta (por ejemplo si trabajamos con n-gramas

(con n = 8) la clave secreta será de 64 caracteres). Por ejemplo, si trabajamos con di-gramas una clave secreta posible sería "DDCF" y expresada en notación matricial sustituyendo las letras por número fila a fila nos queda: $Z = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}$ y su matriz inversa será: $Z^{-1} = \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix}$ donde se verifica que:

$$(Z \cdot Z^{-1}) = \begin{pmatrix} 105 & 78 \\ 130 & 79 \end{pmatrix} \bmod 26 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} =$$

= Matriz identidad

En este contexto, la operación de cifrado de un mensaje en claro M (cuyo número de caracteres debe ser múltiplo de "d") con la clave secreta Z se puede representar como el texto cifrado o criptograma:

C = (M . Z) mod 26

Análogamente la operación de descifrado de un criptograma C en el texto en claro M se realizará utilizando la clave inversa de Z, es decir Z^{-1} empleando la expresión de producto matricial: $M = Z^{-1}$. C mod 26.

Supongamos que deseamos cifrar el texto en claro **M = HELP** formado por cuatro letras utilizando di-gramas (con d=2) y sea la clave secreta: $Z = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}$. Lo primero dividimos el texto en claro M en grupos de dos letras lo cual nos dará dos matrices columna de dos elementos cada una:

$$M1 = \begin{pmatrix} H \\ E \end{pmatrix} = \begin{pmatrix} 7 \\ 4 \end{pmatrix} \quad \text{y} \quad M2 = \begin{pmatrix} L \\ P \end{pmatrix} = \begin{pmatrix} 11 \\ 15 \end{pmatrix}$$

y aplicamos la expresión de cifrado a cada di-grama, lo cual nos permite obtener dos criptogramas:

$$C1 = Z.M1 \mod 26 = \begin{pmatrix} 33 \\ 34 \end{pmatrix} \bmod 26 = \begin{pmatrix} 7 \\ 8 \end{pmatrix} = \begin{pmatrix} H \\ I \end{pmatrix}$$

y por otra parte:

$$C2 = Z.M2 \bmod 26 = \begin{pmatrix} 0 \\ 19 \end{pmatrix} = \begin{pmatrix} A \\ T \end{pmatrix}$$

Por tanto el criptograma total C, está formado por la concatenación de los dos criptogramas parciales C1 y C2, es decir C = HIAT.

El proceso de descifrado en el receptor se realizará a partir del criptograma C = HIAT (=7, 8, 0, 19) dividido en di-gramas C1 y C2. Las dos expresiones matemáticas utilizadas serán:

$M1 = Z^{-1}.C1 \bmod 26 = \begin{pmatrix} 7 \\ 4 \end{pmatrix} = \begin{pmatrix} H \\ E \end{pmatrix}$

y

$M2 = Z^{-1}.C2 \bmod 26 = \begin{pmatrix} 11 \\ 15 \end{pmatrix} = \begin{pmatrix} L \\ P \end{pmatrix}$

Por tanto el texto en claro descifrado M será la concatenación de los dos textos en claro M1 y M2, es decir M = HELP = (7, 4, 11, 15). La inversión de una matriz Z requiere que la misma sea cuadrada y se obtiene dividiendo la adjunta de la traspuesta por el determinante de la matriz Z en cuestión. La traspuesta se obtiene cambiando filas por columnas y la adjunta consiste en sustituir cada elemento por su adjunto, es decir quitando la fila y columna donde se encuentra y obtener el determinante de lo que quede cuyo signo coincide con la paridad de la suma de los subíndices fila y columna donde se ubica así el elemento z como 4+5=9 es impar tendrá signo menos si es par signo positivo. El cálculo del inverso de 17 modulo 9108 es:

17 ^ -1 mod 9108 = 6965.

El orden de un elemento "a" (ord(a)) de un conjunto finito Zn es el menor entero positivo "t" que verifica a ^ t = 1 mod n. En el caso de Z21 los ordenes de cada elemento uno de los 12 posibles elementos son:

{ord(1)=1, ord(2)= 6, ord(4) = 3, ord(5) =6, ord(8)= 2, ord(10)= 6, ord(11)=6, ord(13)=2, ord(16)= 3, ord(17)=6, ord(19)=6, ord(20)=2}

El número de ordenes de elementos de Z21 se obtiene como el producto de los factores menos uno que forman 21, así 21 = 7.3, luego $\Phi = (7-1)(3-1) = 12$, será el número de órdenes de elementos de Z21. Si el orden de un elemento "a" coincide con Φ entonces se dice que ese elemento es un generador ó elemento primitivo de Zn. Si Zn tiene un generador, se dice que es cíclico. Vemos que Z21 no lo tiene.

Consideraciones finales

Las TIC (Tecnologías de la Información y las Comunicaciones) ofrecen oportunidades de negocio en continuo crecimiento a partir de productos de gran impacto en la productividad de cualquier economía, tanto a nivel micro como global. Pero la digitalización de empresas y administraciones crea también un tejido donde las organizaciones productivas, las instituciones y los ciudadanos pueden comunicarse con mucha mayor eficacia y rapidez. El impacto de esta situación afecta a todos los ámbitos desde la selección de proveedores o personalización de productos hasta el acceso a la formación o a la salud.

En este contexto la seguridad de la información que engloba entre otras disciplinas a la criptografía aplicada es de importancia máxima a tenor del creciente aumento del número y variedad de amenazas, vulnerabilidades y ataques a todos los recursos presentes en la sociedad de la información, substracto que soporta las operaciones en la sociedad del siglo veintiuno. La criptografía aplicada va dando solución a muchos problemas planteados en la sociedad actual donde los usuarios demandan privacidad, anonimato, integridad de la información, autenticidad de mensajes y canales de comunicación, no repudio, etc.

La economía mundial esta sufriendo un conjunto de transformaciones debido al paso de la era industrial a la de información. La utilización de las TIC esta pasando de un mercado de profesionales a un mercado de masas y a la aparición continuada de nuevas aplicaciones en todos los ámbitos de la sociedad. La criptografía, "clave" de la seguridad de la información en este nuevo milenio debe presidir todo diseño, producto, reingeniería de sistemas ya desarrollados, etc. con vistas a poder satisfacer las necesidades de todo

tipo de personas físicas y jurídicas (empresas, organizaciones). Los efectos de las TIC van más allá de los indicadores económicos al uso, ya que están afectando de un modo profundo a todos los sectores de la actividad humana: a la generación, adquisición y aplicación del conocimiento; a la forma de organización, producción y hacer negocio de las empresas; a la calidad de vida y bienestar de las personas; al modo de relacionarse entre sí y de los poderes públicos con los ciudadanos. En este contexto la ingeniería de seguridad con la criptografía aplicada como uno de sus aliados más relevantes debe impregnar y penetrar en cada uno de los procesos que existan o que se vayan a poner en funcionamiento. Las TIC poseen un gran poder de penetración en todos los sectores empresariales y en todas las actividades de la sociedad, su papel es crucial en modo creciente en la configuración de la sociedad futura, por tanto nos debe hacer pensar en la necesidad imperiosa de integrar los planteamientos criptográficos embebidos de la criptografía y seguridad de la información si no queremos vernos desprotegidos y esclavos de dichas TIC.

Bibliografía

- Areitio, J. "Diseño, Síntesis y Monitorización de Cripto-sistemas Simétricos". REE. Nº 595. Junio 2004.
- Anderson, R.J. "Security Engineering: Building Dependable Distributed Systems". Wiley & Sons 2001.
- Katzenbeisser, S. "User's Guide to Cryptography and Standards". Artech House Publishers. 2004.
- Spillman, "Classical and Contemporary Cryptology". Pearson E. 2004.
- Rhee, M.Y. "Internet Security: Cryptographic Algorithms and Protocols". John Wiley and Sons. 2003.