Complementos de Criptografia(Clave Asimétrica)

Extraído de Técnicas criptográficas de protección de datos ED: Alfaomega

Algoritmo RSA

Elaborado por Rivest, Shamir y Adelman en el MIT.
El texto se encripta en bloques , cada bloque tiene un valor binario menor que n.

Suponiendo M el texto plano

Para cifrar : $C = M^e \bmod n$
Para decifrar $M = C^d \bmod n = (M\hat{}e)\hat{}d \bmod n = M^{ed} \bmod n$

El valor de **n** es conocido por ambas partes. El emisor (y cualquiera) conoce **e** y sólo el receptor conoce **d.**

La clave privada consiste de { d,n } y la clave pública consiste de {e,n }

Ejemplo de creación de claves.

1. Elegir dos números primos p y q **(p=7 y q=17)**
2. Calcular n= p.q **(m= p.q = 7x17 = 119**
3. Calcular ø = (p-1)(q-1) **(ø = 96).**
4. Elegir un e que sea primo relativo de **ø (e = 5)**
5. Determinar d tal que 1 = d.e mod 96 **(d = 77)**

Se obtiene que KU = { 5, 119 } , KR = { 77, 119 }

Ejemplo de procedimiento
Supongamos que quiero transmitir el número 19 de forma tal que la transmisión sea confidencial.

Dado que : C = M^e mod n => **19**^5 mod 119 = 2476099 mod 119 = 66

Transmito 66 al receptor

M = C^d mod n => 66^77 mod n = 1.27....x10^140 mod 119 = **19.**

NOTA Es muy importante que Ud. repita los cálculos anteriores para acostumbrarse a los procedimientos

Intercambio de clave DIFFIE-HELLMAN.

Desarrollado con el propósito de evitar los problemas de ditribución de claves y de carencia de un sistema sencillo de firma digital:

El protocolo es el siguiente : (► leer complemento de Matematicas)

1. Dos usuarios A y B selecionan publicamente un grupo multiplicativo finito, G, de orden n y un elemento $\alpha \, \varepsilon$ G.
2. A genera un número aleatorio “a”, calcula α^a en G y lo transmite a B
3. B genera un número aleatorio “b”, calcula α^b en G y lo transmite a B
4. A recibe α^b y calcula $(\alpha^b)^a$ en G
5. B recibe α^a y calcula $(\alpha^a)^b$ en G

Para aclarar veamos un ejemplo

Sea “p” el número primo 53, G = Z^*_{53} y α = 2 un generador. Siguiendo los pasos anteriores se tiene

1. **A** elije a = 29, calcula $\alpha^a = 2^{29} \equiv 45 \pmod{53}$ y envia 45 a **B**.
2. **B** elije b = 19, calcula $= 2^{19} \equiv 12 \pmod{53}$ y envia 12 a **A**
3. **A** recibe 12 y calcula $12^{29} \equiv 21 \pmod{53}$
4. **B** recibe 45 y calcula $45^{19} \equiv 21 \pmod{53}$

Notemos que ahora tanto A como B comparten 21, una clave secreta (que podria ser la clave secreta que se busca distribuir).

Un escucha podrá capturar la información que circula por la red y por tanto conocer Z^*_{53} , 2, 45 y 12 pero no tendrá forma práctica de conocer 21.

Criptosistema RSA

(► leer complemento de Matematicas)

La implementación del modelo de Diffie-Hellman fue desarrollado por **R**ivest, **S**hamir y **Ad**leman . El protocolo, que permite el envio de mensajes de un usuario a otro, es como sigue :

1. Cada usuario elije dos números primos (actualmente no deberían tener menos de 200 dígitos para garantizar la seguridad) "p" y "q" y se calcula n = p.q.
   El grupo finito a utilizar será entonces Z^*_n .
   El orden de este grupo será $\Phi(n) = \Phi\ (p.q) = (p-1)(q-1)$

2. El usuario selecciona un entero positivo "e" tal que $0 < 1 < \Phi(n)$ y que además sea primo con el orden del grupo, es decir : mcd (e, $\Phi(n)$) = 1.
3. Se calcula el inverso de "e' en Z^*_n , "d" ;
   Se tiene entonces que $e.d \equiv 1$ (mod $\Phi(n)$), con $0 < d < \Phi(n)$

4. La clave pública del usuario es el par (n,e) y su clave privada es el número d .
   Evidentemente p , q y $\Phi(n)$ deben permanecer secretos.

Veamos un ejemplo completo del envio de un mensaje y su recuperación mediante RSA

Ejemplo

Supongamos que somos **A** deseamos enviar un mensaje confidencial al usuario **B**, **A** debe emplear la clave púbica de **B**, veamos como elaboró **B** su clave:

B elije dos números primos p_b= 281 y q_b = 167.

Calcula n_b = 281 . 167 = 46927 se pasa a trabajar entonces con el grupo Z^*_{46927} ,
El orden del grupo es $\Phi(46927)$ = 280 . 166 = 46480.
Se elije un número "e" , según el punto 3 anterior . e_b = 39423.
Comprobamos que mcd (39423,46480) = 1 [*se deja al lector comprobarlo*]
Corresponde ahora determinar el inverso de 39423 mod (46480) el número que se obtiene es d_b = 26767 [*Nuevamente debería ser comprobado por el lector*]

La clave pública de **B** será entonces (n_b,e_b) = (46927,39423).

Estamos ya en condiciones de ver como **A** envia su mensaje a **B**.

Suponemos que usamos un alfabeto de 26 caracteres por lo cual el mensaje debera ser cifrado en base 26. Por otro lado el número mayor manejable en nuestro ejemplo es n_b = 46927. Veamos entonces :

$26 \wedge 2 = 676$
$26 \wedge 3 = 17576$
$26 \wedge 4 = 456976$ excede el valor máximo permitido por lo cual nuestro mensaje no podrá tener mas de 3 letras (En caso de mensajes mas largos se deberá romper en bloques de 3 letras)

El mensaje a enviar sera : YES.

Somos el usuario **A**, nuestra clave pública es $(n_a, e_a) = (155011, 2347)$ y nuestra clave privada es $d_a = 151267$ (con $p_a = 409$ $q_a = 379$ $\Phi(n_a) = 154224$). Elaborada en forma similar a lo recien explicado.

Para enviar el mensaje debemos codificarlo en base 26.

$YES = Y \,.\, 26^2 + E \,.\, 26 + S = 24 \,.\, 26^2 + 4 \,.\, 26 + 18 =$ **16346** $= m$

Donde se uso la codificación normal (A = 0 , B = 1, C = 2 .....)

Debemos ahora encriptar m con la clave pública de B

$C = m^{e_b} \,(\mathrm{mod}\ n_b) = 16346^{39423}$ (mod 46927) = **21166**

21166 es el mensaje a enviar, pasándolo a texto (de ser necesario)

$C = 21166 = 1 \,.\, 26^3 + 5 \,.\, 26^2 + 8 \,.\, 26 + 2 =$ **BFIC** que se enviará a **B**

B al recibir el mensaje los codificará en base 26 recuperando C.

$BFIC = 1 \,.\, 26^3 + 5 \,.\, 26^2 + 8 \,.\, 26 + 2 = 21166 = C$

Para obtener el texto plano deberá emplear su clave privada solo conocida por él
$d_b = 26767$

$m = c^{d_b} \,(\mathrm{mod}\ n_b) = 21166^{26767}$ (mod 46927) = 16346

Decodificándolo se llega al texto original 'm'

$m = 16346 = 24 \,.\, 26^2 + 4 \,.\, 26 + 18 =$ **YES**

Aplicaciones especiales.

I . Lanzamiento de una moneda por Teléfono :

Alicia y Benito se han divorciado, viven en ciudades separadas y quieren decidir telefónicamente quien se queda con el Apunte de Cátedra de Seguridad.
Se dan varias posibilidades.

a. Alicia tira la moneda, Benito dice cara o ceca, Alicia le dice si acertó
b. Alicia tira la moneda. Le dice a Benito el resultado, Benito dice si acertó
c. Benito dice cara o ceca. Alicia tira la moneda y le dice a Benito si acertó.

Todas las posibilidades anteriores como también otras posibles se prestan a hacer trampa.

La solución sería un procedimiento tal que Alicia no pueda arrojar la moneda después de oir la elección de Benito y Benito no pueda conocer el resultado del lanzamiento antes de hacer su elección..... Parece un problema imposible.

Protocolo propuesto:

1. Alicia y Benito se ponen de acuerdo en la elección de una función unnidireccional con igual cantidad de pares e impares. f: X→ Y.
2. Alicia elige un número aleatorio x de X, calcula f(x) = y; enviándolo a Benito
3. Benito debe adivinar si es par o impar. Dice su supocisión a Alicia.
4. Alicia comunica a Benito el valor de x elegido, ambos comprueban que realmente f(x) = y.

El lector comprobará el funcionamiento del protocolo indicando su posible falla.

II . Secreto Dividido.

Supongamos que se tiene un secreto valioso y se no desea correr el riego de perderlo; por ello se puede pensar en hacer muchas copias, pero así se corre el riesgo que el secreto caiga en otras manos.
Para solucionar el problema dividimos el secreto en ‘t’ partes (llamadas sombras) de forma tal que se deba conocer ‘k’ partes para recuperar el secreto, mientras no es suficiente con k-1.

Un caso practico sería que el secreto S es la clave para acceder al control de una operación crucial. Para que la acción sea tomada se requiere el acuerdo de al menos k partes, no siendo necesario concenso de las otras partes.

Detalle :

El esquema se conoce con el nombre de *(k,t)-umbral*. El secreto se divide en 't' partes Ai, con i = 1.....t. con 1< k < t que satisfaga :

1. Cada parte A_i conoce la información a_i, que no es conocida por A_j.
2. El secreto S se puede obtener a partir de k cualquiera a_i .
3. El conocimiento de k-1 cualquiera a_i no es suficiente para recuperar el secreto.

Ejemplo : (► leer complemento de Matematicas)

Deseamos ocultar el número S = 123456. Elegimos k = 3 y t = 5.
Según el Teorema del Resto Chino para un sistema de 5 congruencias.

$$S = \sum_{i=1}^{5} a_i M_i N_i$$

Supongamos : $m_1 = 82$, $m_2=83$, $m_3=85$, $m_4 = 87$ y $m_5 = 89$

Estos números fueron elegidos de forma que verifiquen la hipótesis del teorema.

Dado que queremos que con 3 partes sea suficiente para obtener el secreto

Min(k=3) = 82 . 83 . 85 = 578510

Pero que con 2 no alcance

Max (k = 2) = 7743

Es decir el número secreto verifica la condición :

7743 < S < 578510

Obtenemos ahora los a_i correspondiente sabiendo que $S \equiv a_i \pmod{m_i}$

$123456 \equiv a_1 \pmod{82} \rightarrow a_1 = 46$ en forma similar se llega a

$a_2 = 35$, $a_3 = 36$, $a_4 = 3$, $a_5 = 13$. Que son los valores de conocimiento que se proporcionan a cada parte.

Probemos si el sistema funciona, Supongamos que A2, A3 y A4 se unen para determinar el valor de S.

S = a2 . M2 . N2 = a3 . M3 .N3 + a4 . M4 . N4 → Aplicando el Teorema del Resto chino

m = m2 . m3 . m4 = 613785

M2 = m/m2 = 613785 / 83 = 7395
M3 = 7221
M4 = 7055

Calculamos ahora los inversos

N2 tal que M2 . N2 ≡ 1 (mod m2) → 7395 . N2 ≡ 1 (mod 83) → N2 = 52
En forma similar

N3 = 21; N4 = 11

X = 35 . 7395 . 52 + 36 . 7221 . 21 + 3 . 7055 . 11 = 19150791

19150791 ≡ S (mod 613785) => **S = 123456.**

Se deja al lector comprobar que es lo que ocurre si solo dos de las partes se unen para obtener el resultado.

Problemas de CriptografIa. Esta es la parte a entregar del TP

1. Alicia y Benito utilizan un grupo Z^*_{13} y eligen como generador del mismo = 4 . Determinar que número secreto se intercambiarán por el método de intercambio de claves de Deffie – Hellman si Alicia elige como numero aleatorio 5 y Benito 2.

2. Romper el código del problema anterior si se sabe que los números que se intercambian Alicia y Benito son 3 y 10 respectivamente.

3. Benito utiliza un sistema criptográfico RSA con la clave pública (n_e,e_B) = (2947,179). Determinar que enviará a Alicia si el mensaje es M = "MANDA DINERO" . Usar el alfabeto A-Z codificado 0-25 con 26 = punto y 27 = espacio.

4. El director de una empresa establece un premio si al menos 3 de sus 5 empleados se ponen de acuerdo compartiendo información en un esquema (3,5)- umbral donde la información secreta es la cantidad del premio. Los módulos empleados son $m1 = 97$, $m2= 98$, $m3 = 99$, $m4 = 101$, $m5 = 103$. Desarrollar el esquema correspondiente si el premio son $ 500000. Determinar que ocurre si E2, E3 y E4 combinan sus sombras, ¿y si lo hacen E2 y E5?