CRIPTOGRAFIA-DE-LA-CLAU-PUBLICA.pdf

mariabarnils

Criptografia i Seguretat

3º Grado en Ingeniería de Datos

Escuela de Ingeniería
Universidad Autónoma de Barcelona

Maria Barnils Sagués

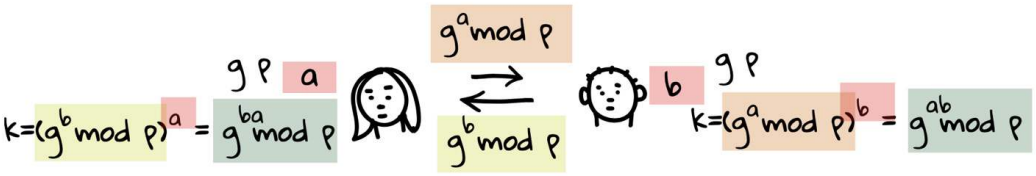
T5: CRIPTOGRAFIA DE LA CLAU PÚBLICA

Intercanvi de claus de Diffie-Hellman

L'algorisme d'intercanvi de claus de Diffie-Hellman permet que dos usuaris que es comuniquen per un canal insegur puguin aconseguir derivar una clau compartida de manera segura. D'aquesta manera, encara que un atacant estigui escoltant el canal, l'atacant no pot aconseguir conèixer la clau derivada pels usuaris.

Ara posarem un exemple del funcionament del algorisme:

1. Primer pas:
    a. La Maria escull un número primer 'p', per exemple 31.
    b. Després escull un nombre k inferior a p (10).
    c. El número k i el p li envia al Pedro sense por a que la resta el vegin.
    d. Ara la maria escull un número x menor a p y el manté en secret. I farà la següent operació: A = k^x (mod p) i enviarà el resultat al Pedro.
2. Segon pas:
    a. El Pedro escull un valor y menor a p.
    b. Fa la mateixa operació que la Maria per calcular el seu número B = k^y (mod p)
    c. Pedro li envia B a la Maria.
3. Tercer pas:
    a. Ara els dos tenen els valors de A i B, cada un farà la seva respectiva operació:
        i. Maria: B^x (mod 31)
        ii. Pedro: A^y (mod 31)
    b. El resultat de les dues operacions serà el mateix.



La principal vulnerabilitat d'aquest protocol és el que es coneix com a atacs de 'Man in the middle' (MiTM). Aquest ataca es basa en que una tercera persona fa de missatger entre el emissor i el receptor de tal manera que aconsegueix tota la informació dels dos i pot generar la clau privada.

Xifres de clau pública

Habitualment els algorismes de xifrat de clau pública comprenen tres funcions bàsiques: la generació de claus, el xifrat i el desxifrat. L'algorisme de generació de claus retorna un parell de claus de criptografia asimètrica, [k_{pub},k_{priv}]; l'algorisme de xifrat rep un missatge m i una clau pública kpub i genera el missatge xifrat c; i l'algorisme de desxifrat rep un missatge xifrat c i una clau privada kpriv i permet recuperar el missatge original m.

$$missatge\ xifrat = E(k_{pub}, missatge\ original)$$

$$missatge\ original = E(missatge, xifrat, k_{priv})$$

- Xifratge basat en la factorització d'enters: RSA

L'RSA és un criptosistema de clau pública basat en el problema de la factorització d'enters. L'RSA es fa servir, principalment, en dos contextos: per xifrar dades de poca mida (normalment, per xifrar claus criptogràfiques) i en signatures digitals.

Primer de tot anem a explicar com es generen els parells de Claus a partir del RSA, el procés consta de 6 passos:

1. S'escullen dos nombres primers $p = 3\ i\ q = 11$
2. Es calcula el producte dels nombres primers $n = p * q = 3 * 11 = 33$
3. Es calcula la funció de Euler $\phi(n) = z = (p-1)(q-1) = 20$
4. S'escull un nombre primer k que no tingui divisors comuns amb z, en el nostre cas podríem triar un dels següents: 3, 7, 11, 13, 17 o 19. Ens quedem amb el nombre $k = 7$.
5. La clau pública serà el conjunt de nombres (n, k), és a dir $(33,7)$.
6. A continuació és calcula la clau privada que es fa escollint un valor j que verifiqui la següent equació: $k * j = 1(mod\ z)$. En el nostre cas la clau privada seria 3.

A continuació explicarem com es xifra un missatge:

Per tal de xifrar un missatge amb RSA, s'aplicarà l'algorisme de xifrat, que fa servir la clau pública del destinatari, la fórmula és molt senzilla, m és el missatge en clar, n i e son els dos valors de la clau pública $k_{pub} = (n, e)$ i c és el missatge xifrat:

$$c = m^e\ mod\ n$$

Quan el destinatari rebi el missatge xifrat, poder desxifrar-lo fent ús de la seva clau privada. També podem desxifrar els missatge utilitzant la fórmula inversa on d és la clau privada:

$$m = c^d\ mod\ n$$

- Xifratge basat en el logaritme discret: ElGamal

ElGamal és un criptosistema de clau pública basat en el problema del logaritme discret. En concret, ElGamal està basat en l'algorisme d'intercanvi de claus de Diffie-Hellman. Com amb l'anterior mètode de xifratge, també es creen Claus, s xifren missatges i després es desxifren.

Per la generació de claus:

1. Es tria un valor p un alfa a d'ordre q.
2. Es tria un valor aleatori d que es trobi dins del rang [2, p-2]. A partir d'aquest valor es calcula $\beta = \alpha^d\ mod\ p$.

3. La clau pública és $k_{pub} = (p, \alpha, \beta)$ i la clau privada és $k_{priv} = d$.

Per tal de xifrar un missatge m amb la clau pública es segueixen 3 passos:

1. Es tria un nombre aleatori h i es calcula $c_1 = \alpha^h mod\ p$
2. Es recupera la clau pública del receptor i es calcula $c_2 = m * \beta^h mod\ p$
3. S'envia el missatge xifrat (c_1, c_2)

Cal remarcar que aquest xifratge és expansiu, ja que per un missatge de mida m es generen textos xifrats de mida 2m. També és probabilístic, ja que per a una mateixa clau pública i un mateix missatge en clar, es poden generar múltiples textos xifrats, triant diferents valors aleatoris h durant el procés de xifrat.

Per desxifrar un text només s'ha d'aplicar la següent fórmula utilitzant la clau privada d:

$$m = \frac{c_2}{c_1^d}\ mod\ p$$