Adrià Muro Gómez
1665191

Activitat sobre RSA i Diffie-Hellman

1. Per a un sistema de xifratge RSA amb p = 97 i q = 31, quantes claus públiques podem fer servir?

p = 97, q = 31

n = 97·31 = φ(3007) → (97-1)·(30-1) = 2880

Per trobar el nombre de claus públiques apliquem φ(2880) = 768. El nombre de claus públiques que podem utilitzar és 768.

2. Per un sistema de xifratge RSA amb p = 97 i q = 31, ens diuen que podem fer servir qualsevol de les següents claus públiques:

a) e = 24
b) e = 33
c) e = 45
d) e = 49

Quines d'elles són millors i perquè?

Comprovem si cada valor és vàlid:

- gcd(24, 2880) = 24
- gcd(33, 2880) = 3
- gcd(45, 2880) = 15
- gcd(49, 2880) =1

Només e = 49 és una clau pública vàlida. Les altres tenen gcd(e, φ(n)) != 1, i per tant, no es poden usar.

3. Els usuaris d'una xarxa que es comuniquen utilitzant el criptosistema RSA tenen les següents claus públiques:

	(n,e)
A	$PK_A = (979, 293)$
B	$PK_B = (299, 217)$
C	$PK_C = (407, 119)$
D	$PK_D = (n_d, 65537)^1$

1. **Calculeu les claus privades de A, B, C i D.**

A: $979 = 11 \cdot 89 \rightarrow \varphi(n) = 10 \cdot 88 = 880 \rightarrow e = 293 \rightarrow d = e^{-1} \bmod 880 = 877$

B: $299 = 13 \cdot 23 \rightarrow \varphi(n) = 12 \cdot 22 = 264 \rightarrow e = 217 \rightarrow d = e^{-1} \bmod 264 = 73$

C: $407 = 11 \cdot 37 \rightarrow \varphi(n) = 10 \cdot 36 = 360 \rightarrow e = 119 \rightarrow d = e^{-1} \bmod 360 = 239$

D: Impossible de calcular sense n_d

2. **Calculeu el xifratge del missatge m = 15 que B vol enviar a A.**

   $m = 15, e = 293, n = 979 \rightarrow c = m^e \bmod n = 15^{293} \bmod 979 = 108$

3. **Desxifreu el missatge rebut per A de B.**

   $c = 108, d = 877, n = 979 \rightarrow m = c^d \bmod n = 108^{877} \bmod 979 = 15$

4. Suposem que els usuaris A i B porten a terme una distribució de clau secreta utilitzant el protocol de Diffie-Hellman. Els valors que utilitzen són p = 7001, α = 101, a = 68 i b = 98. Descriviu el protocol i calculeu la clau privada que comparteixen.

1. Es defineix un nombre primer gran p=7001 i una arrel primitiva α=101
2. L'usuari A tria una clau privada a=68 i calcula la seva clau pública:
   $A=\alpha^a \bmod p = 101^{68} \bmod 7001 = 176$
3. L'usuari B tria una clau privada b=98 i calcula la seva clau pública:
   $B=\alpha^b \bmod p = 101^{98} \bmod 7001 = 2901$
4. A i B intercanvien les claus públiques A i B.
5. A calcula la clau secreta:
   $K=B^a \bmod p$
6. B calcula la mateixa clau secreta:
   $K=A^b \bmod p$

Càlcul de la clau compartida:

$K=B^a \bmod p = 2901^{68} \bmod 7001 = 2153$

2153 és la clau compartida, coincideix amb $K=A^b \bmod p$

5. El protocol de Diffie-Hellman és vulnerable enfront d'atacs d'impersonació. Descriviu quins passos es modificarien i quins s'afegirien en l'intercanvi de claus de l'exercici anterior per tal que un atacant aconseguís compartir una clau diferent amb cada usuari malgrat els usuaris pensessin que comparteixen una sola clau entre ells dos.

1. A envia la seva clau pública $A=\alpha^a \bmod p$, però l'atacant M la intercepta.

2. M genera la seva pròpia clau privada m_1 i calcula $M_1 = \alpha^{m1} \bmod p$, que envia a B com si fos A.

3. B respon amb la seva clau pública $B=\alpha^b \bmod p$, però M la intercepta.

4. M genera una altra clau privada m_2 i envia $M_2 = \alpha^{m2} \bmod p$ a A com si fos B.

5. Ara M pot calcular dues claus secretes:

    - Amb A: $K_{AM} = M^a_2 \bmod p$

    - Amb B: $K_{MB} = M^b_1 \bmod p$

6. M pot llegir, modificar i reenviar missatges entre A i B com si fos l'altre, sense que cap dels dos ho sàpiga.