Criptografia i Seguretat [104355]

Activitats RSA i DH

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

   Recordem que si un nombre m es pot factoritzar en potències de nombres primers com $m = p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_n^{e_n}$, llavors $\phi(m) = \prod_{i=1}^{n}(p_i^{e_i} - p_i^{e_i-1})$.

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?

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.
   2. Calculeu el xifratge del missatge $m = 15$ que B vol enviar a A.
   3. Desxifreu el missatge rebut per A de B.

   Resultat: clau privades: $A : 877$, $B : 73$, $C : 239$. $E_{PK_A}(m) = 108$.

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 $p = 7001$, $\alpha = 101$, $a = 68$ i $b = 98$.

   Descriviu el protocol i calculeu la clau privada que comparteixen.

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] n_d =140030234401607803777917438251378213819219721524651118808434275263655395469528598704536324499566494098557043742549996566558639071657539815043385431186640932840798807785896997249571231108794361593482827908287632293375666323685398351507895710615198985712283304233326023055012524211849836100106559378736370665769