Master 1 deuxième session. M7 Cryptographie

Examen du 14 mars 2008

Exercice 1

Alice et Bob veulent échanger une clé à l'aide du procédé de Anshel-Anshel-Goldfeld avec le groupe symétrique S_5.
Ils rendent publiques les mots $a_1 = (12)(34); a_2 = (13)(25); b_1 = (14)(23); b_2 = (15)(23)$.
Alice choisit le mot $X = a_1 a_2^2$ qu'elle garde secret et Bob choisit le mot $Y = b_1 b_2^2$ qu'il garde secret aussi.
En suivant la procédure de cet échange, trouver les données qu' Alice envoie à Bob et les données que Bob envoie à Alice. Faire les calculs que fait Alice pour trouver le mot échangé et les calculs que Bob fait pour trouver le mot échangé. Mettre en évidence que c'est le même mot.

Exercice 2

En utilisant le système cryptographique RSA, Bob a publié la clef publique (n,e) et forgé sa clef secrète de déchiffrement d.
1) Comment Alice , connaissant n et e, doit-elle chiffrer le message en clair P, pour l'envoyer à Bob?
2) Quel calcul Bob doit-il faire pour retrouver P?
3) On note φ l'indicateur d'Euler. Justifier le fait que le calcul précédent permet bien de déchiffrer le message envoyé par Alice.
4) Sachant que $n = 11413$ et que $1 \leq e < n$, vous trouvez par hasard (ci-dessous) la table des calculs effectués par Alice pour chiffrer le message $P = 9726$.
Quelle est la valeur de la clef publique e utilisée par Alice?
5) Sachant que $\varphi(n) = 11200$, expliquer pourquoi la valeur de e trouvée à la question 4) ne doit être divisible par aucun des entiers 2, 5, ou 7 .
6) Déduire des résultats précédents la valeur de d, sachant que $1 \leq d < \varphi(n)$.
7) En général, si n et $\varphi(n)$ sont connus, comment peut-on trouver les deux facteurs premiers p et q de n?
8) Indiquer comment Bob peut utiliser très simplement sa clef secrète d pour signer un message en clair x qu'il envoie à Alice, et comment Alice vérifiera la validité de la signature.
Quelqu'un peut-il envoyer un message en se faisant passer pour Bob?

i	e_i	z		
11	1	$1^2 \times 9726$	=	9726
10	1	$9726^2 \times 9726$	=	2659
9	0	2659^2	=	5634
8	1	$5634^2 \times 9726$	=	9167
7	1	$9167^2 \times 9726$	=	4958
6	1	$4958^2 \times 9726$	=	7783
5	0	7783^2	=	6298
4	0	6298^2	=	4629
3	1	$4629^2 \times 9726$	=	10185
2	1	$10185^2 \times 9726$	=	105
1	0	105^2	=	11025
0	1	$11025^2 \times 9726$	=	5761