Enseignement Libre
Introduction à la Cryptographie
2008/2009

UNIVERSITÉ de Cergy-Pontoise

Examen du 27 Avril 2009

Exercice 1 : Quel est le nombre de clés possibles dans un chiffrement

1. par décalage ?
2. affine ?
3. par substitution ?

Exercice 2 : Montrer qu'en entier est divisible pas 9 si, et seulement si, la somme de ses chiffres est divisible par neuf.

Exercice 3 : Dans la Chine ancienne, les régiments comptaient 1000 soldats. Pour savoir si un régiment était complet, on faisait aligner les hommes par rangs de 7, puis par rangs de 11 et enfin par rangs de 13. Si, dans les trois cas, il manquait 1 homme pour que dernier rang soit rempli, on en déduisait que le régiment était complet. Justifier de façon précise cette méthode (on énoncera le théorème utilisé et on donnera le système de congruences associé au problème ainsi que la solution de ce système).

Exercice 4 :

1. On considère le couple $(35, 5)$. Vérifier que c'est une clé publique valide pour le RSA. Quelle est la clé privée associée ?
2. On code les lettres de l'alphabet à l'aide du tableau suivant :

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	6	8	9	11	12	13	16	17	18
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
19	22	23	24	26	27	29	31	32	33	33	33	33

   et le chiffrement s'effectue lettre par lettre. Décoder la phrase :
   "IAMEUSEBEUAQXEMALE"
3. Expliquer pourquoi la méthode utilisée affaiblit le RSA.

Exercice 5 : Dans cet exercice, le RSA est utilisé pour la signature.

1. Calculer le module N et l'entier $\varphi(N)$ associés aux nombres premiers $P = 17$ et $Q = 23$.
2. Parmi ces deux exposants publics, $E = 11$ et $E = 13$, lequel permet d'utiliser le RSA ? Calculer l'exposant privé associé D. Préciser les clés publique et privée d'Alice pour la signature.
3. Alice veut signer le message $m = 100$. Qu'envoie-t-elle à Bob ?
4. Comment Bob effectue-t-il la vérification ?