Enseignement Libre
Introduction à la Cryptographie
2008/2009

UNIVERSITÉ de Cergy-Pontoise

Examen du 4 Juin 2009 : deuxième session

Exercice 1 : On considère le chiffrement affine avec la clé $(a, b) = (11, 3)$.

1. Chiffrer la phrase : Vive la cryptographie.
2. Donner la fonction de déchiffrement.
3. Déchiffrer la phrase : OBQKVZBKDRV

Exercice 2 : Un problème de lunaisons
Considérons le cycle de Meton (235 lunaisons), le cycle de 81 lunaisons, et le cycle de $235 \times 81 = 19035$ lunaisons. Déterminer quelle lune du cycle de 19035 lunaisons correspond à la troisième lune du cycle de Meton et à la septième lune du cycle de 81 lunaisons.

Exercice 3 : Supposons qu'Alice souhaite envoyer le même message à Bob, Eve et Charlie à l'aide du chiffrement RSA. Les clés publiques de Bob, Eve et Charlie sont respectivement $(55, 3)$, $(51, 3)$ et $(46, 3)$. Elle envoie 25 à Bob, 44 à Eve et 42 à Charlie.

1. Résoudre le système de congruences :

$$\begin{cases} x \equiv 25 & \mod 55 \\ x \equiv 44 & \mod 51 \\ x \equiv 42 & \mod 46 \end{cases}$$

2. En déduire le message M envoyé par Alice sans utiliser les clés privées de Bob, Eve et Charlie.

Exercice 4 : Dans un cryptosystème utilisant le RSA, déterminer les clés secrètes ansi que les messages envoyés pour les clés publiques (n, e) et le message crytpé $C = M^e \mod n$ dans chacun des cas suivants :

1. $n = 35$, $e = 5$, $C = 10$.
2. $n = 265$, $e = 139$, $C = 10$.
3. $n = 667$, $e = 493$, $C = 10$.
4. $n = 1763$, $e = 611$, $C = 2$.