Département d'Informatique
Faculté des sciences
Université de Batna

Master I : CSSI

Introduction à la cryptographie

Contrôle final
06/07/11
Durée : 1H30

Questions de cours :

1. Quel est l'inconvénient de l'algorithme El-Gamal par rapport à RSA ?
2. Quelles sont les propriétés qui doivent être assurées par un protocole Zero-knowledge ?

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

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

On considère ici le chiffrement des 26 caractères seulement et seules les clés qui modifient le texte sont prises en considération.

Exercice 2 :

1. Sachant que le message a été chiffré par la méthode de Vigenère, en utilisant le mot-clef CRYPTO, quel est le message en clair obtenu en déchiffrant le cryptogramme suivant : RRPIBSNUCRKMRKM ?

2. Quel est le résultat du codage du bloc 11010111 par la structure de Feistel en utilisant la clé 1100 et la fonction f=XOR ?

Exercice 3 :

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	34	34	34

et le chiffrement s'effectue lettre par lettre. Décoder la phrase :
"IAMEUSEBEUAQXEMALE"

3. La sécurité est-elle assurée par cette méthode de chiffrement ? Pourquoi ?