

Durée : 2h

EPREUVE DE CRYPTOGRAPHIE

Exercice 1: Questions de cours (4pts)

- 1) Définir : Cryptographie; cryptanalyse; chiffrement; fonction de hachage
- 2) Quelle est la différence fondamentale entre la signature numérique et la signature manuscrite?
- 3) Pourquoi dans la pratique préfère-t-on signer le haché d'un document?
- 4) Citez 4 services de sécurité.

Exercice 2: Chiffrement affine (6pts)

- 1) Le texte suivant a été obtenu par chiffrement affine avec la clef « K »

NOCE	CKQO	BCCO	ZVKS
QXOX	DNOV	KMSB	MEVK
DSYX	NOVK	PKEC	COWY
XXKS	O		

Déchiffrez-le!

- 2) Le texte suivant a été obtenu par chiffrement affine avec une clef inconnue:

QF XTSJQ XJSXNGNQNXJ QJX JHTQNJWX FZC WJLQJX
IJ XJHZWNYJ

Déterminer la clef utilisée et le texte clair correspondant.

Exercice 3: Chiffrement de Vigenère (3pts)

L'application du chiffrement de Vigenère au texte clair:

LA VIE EST BELLE

Donne le texte chiffré :

XA CIH IET MEOPQ

Déterminez la clef utilisée.

Exercice 4: Chiffrement RSA (5pts)

1) Définir le sigle **RSA**

2) On prend $p=97$, $q=23$ et $e=7$

Déterminez la clef publique (n,e) et la clef privée d .

3) Chiffrer $M=104$

Exercice 5: Programmation C (2pts)

Vous disposez d'une fonction « chiffrement » qui prend en entrée un caractère et retourne le chiffré de celui-ci par la méthode de Jules César.

Char chiffrement (char c)

Écrire une fonction « chiffrement_fichier » qui prend en entrée deux fichiers, effectue le chiffrement du contenu du premier fichier et écrit le résultat dans le second. Elle retourne 2 en cas d'erreur et 1 si l'opération s'est bien effectuée.