Novembre 2014

NOM :
Prénom :
Groupe :

Examen

Cryptographie

La qualité de la rédaction ainsi que la propreté de la copie seront pris en compte dans l'évaluation.

Exercice 1

40 min

Première partie. Questions de cours

1. Qu'est qu'une clef dans un codage affine ? 1

2. Est-il possible de trouver un codage affine f tel que $f(20) \equiv 5\ [26]$ et $f(7) \equiv 3\ [26]$? Justifier. 1.5

Deuxième partie. On sait qu'un codage affine donne le message XQGOJNI. On va chercher à décrypter ce message. On pose $f(x) \equiv ax + b\ [26]$.

1. On sait que les premières lettres du texte claire sont AX.

   (a) Donner le système de deux équations qui traduisent les données de l'énoncé. 1

   (b) Résoudre le système précédent. 1

   (c) Donner l'expression de f. 0.5

2. (a) Déterminer l'inverse de 11 modulo 26. 1

(b) En déduire une expression de f^{-1} la fonction de décryptage. 0.5

(c) Conclure. 1

Exercice 2

30 min

On considère la matrice $M = \begin{pmatrix} 3 & -4 \\ 1 & 5 \end{pmatrix}$ modulo 26.

1. (a) Déterminer l'inverse de 19 modulo 26. 1

(b) En déduire M^{-1} la matrice inverse de M modulo 26. 1.5

2. Crypter, avec la méthode de Hill, le message HULK avec M comme clef. 1

3. Avec la méthode Hill de clef M, on a obtenue le message CUMUBL. Décrypter ce message. 1.5

Exercice 3

50 min

Première partie. Question de cours.

1. Que signifie RSA ? 0.5

2. Quelle est la clef de décryptage associée à la clef de cryptage $(11103, 19)$? Justifier. 2

Deuxième partie. On considère la méthode RSA avec $n = 4141$.

1. Donner la valeur de p et q tel que $n = pq$ et φ.

2. Vérifier que 3 est l'inverse de 2667 modulo φ. 0.5

3. On a crypté un message avec la clef $(n, 2667)$ et on a obtenu 1844-3738-1568-754.
   (a) Montrer $1844^2 \equiv 575\ [n]$. En déduire 1844^3 modulo n. 1

   (b) De la même manière calculer 3738^3 modulo n en détaillant les calculs. 1

   (c) De même pour 1568^3 modulo n. 1

   (d) De même pour 754^3 modulo n. 1

   (e) Décrypter le message. 0.5

A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25