NOM : GROUPE :

Exercice 3.

Dans les deux premiers chiffrements, une lettre est représentée par son rang dans l'alphabet en partant de 0.

1. On considère la fonction de **chiffrement affine** suivante : 3

$$\begin{array}{rccc} E_k: & \mathbb{Z}/26\mathbb{Z} & \longrightarrow & \mathbb{Z}/26\mathbb{Z} \\ & m_i & \longmapsto & c_i = 21m_i + 5 \end{array}$$

(a) Chiffrer le message "LN".

$L \xmapsto{\text{rang}} 11 \xmapsto{E_k} 21 \times 11 + 5 \equiv 2 \mod 26 \longmapsto C$

$N \longmapsto 13 \longmapsto 21 \times 13 + 5 \equiv 18 \mod 26 \longmapsto S$ 1

Le chiffré de "LN" est donc "CS".

(b) Déchiffrer le message "AJO".

$c_i \equiv 21 m_i + 5 \iff m_i \equiv 21^{-1}(c_i - 5) \mod 26.$

A l'aide de l'algorithme d'Euclide étendu, on trouve : $21^{-1} \equiv 5 \mod 26$

On en déduit la fonction de déchiffrement :

$$\begin{array}{rccc} D_k: & \mathbb{Z}/26\mathbb{Z} & \longrightarrow & \mathbb{Z}/26\mathbb{Z} \\ & c_i & \longmapsto & 5(c_i - 5) = 5c_i + 1 \end{array}$$ 1

Par suite, on a :

$A \xmapsto{\text{rang}} 0 \xmapsto{D_k} 5 \times 0 + 1 \equiv 1 \mod 26 \longmapsto B$

$J \longmapsto 9 \longmapsto 5 \times 9 + 1 \equiv 20 \mod 26 \longmapsto U$ 1

$O \longmapsto 14 \longmapsto 5 \times 14 + 1 \equiv 19 \mod 26 \longmapsto T$

D'où le message clair "BUT".

3

2. On considère la fonction de **chiffrement de Hill** suivante :

$$\begin{array}{rccc} E_k : & (\mathbb{Z}/26\mathbb{Z})^2 & \longrightarrow & (\mathbb{Z}/26\mathbb{Z})^2 \\ & \begin{pmatrix} m_i \\ m_{i+1} \end{pmatrix} & \longmapsto & \begin{pmatrix} c_i \\ c_{i+1} \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 1 & 5 \end{pmatrix} \begin{pmatrix} m_i \\ m_{i+1} \end{pmatrix} \end{array}$$

(a) Chiffrer le message "LN".

$$LN \mapsto \begin{pmatrix} 11 \\ 13 \end{pmatrix} \xmapsto{E_k} \begin{pmatrix} 2 & 3 \\ 1 & 5 \end{pmatrix} \begin{pmatrix} 11 \\ 13 \end{pmatrix} = \begin{pmatrix} 9 \\ 24 \end{pmatrix} \longmapsto JY$$

1

(b) Déchiffrer le message "DVAX".

On calcule d'abord l'inverse de $A = \begin{pmatrix} 2 & 3 \\ 1 & 5 \end{pmatrix}$ modulo 26 :

$$A^{-1} = \det(A)^{-1} \times \mathrm{com}(A)^t = 7^{-1} \times \begin{pmatrix} 5 & -1 \\ -3 & 2 \end{pmatrix}^t = 15 \begin{pmatrix} 5 & -3 \\ -1 & 2 \end{pmatrix} \equiv \begin{pmatrix} 23 & 7 \\ 11 & 4 \end{pmatrix}$$

On en déduit la fonction de déchiffrement :

$$\begin{array}{rccc} D_k : & \mathbb{Z}/26\mathbb{Z} & \longrightarrow & \mathbb{Z}/26\mathbb{Z} \\ & \begin{pmatrix} c_i \\ c_{i+1} \end{pmatrix} & \longmapsto & \begin{pmatrix} 23 & 7 \\ 11 & 4 \end{pmatrix} \begin{pmatrix} c_i \\ c_{i+1} \end{pmatrix} \end{array}$$

1

Par suite, on a :

$$DV \mapsto \begin{pmatrix} 3 \\ 21 \end{pmatrix} \xmapsto{D_k} \begin{pmatrix} 23 & 7 \\ 11 & 4 \end{pmatrix} \begin{pmatrix} 3 \\ 21 \end{pmatrix} = \begin{pmatrix} 8 \\ 13 \end{pmatrix} \longmapsto IN$$

$$AX \mapsto \begin{pmatrix} 0 \\ 23 \end{pmatrix} \mapsto \begin{pmatrix} 23 & 7 \\ 11 & 4 \end{pmatrix} \begin{pmatrix} 0 \\ 23 \end{pmatrix} = \begin{pmatrix} 5 \\ 23 \end{pmatrix} \mapsto FO$$

1

D'où le message clair "INFO"

3. On considère la fonction de **chiffrement RSA** suivante : 4

$$\begin{array}{rccc} E_k : & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ & m_i & \longmapsto & c_i = m_i^e \end{array}$$

avec $n = pq = 11 \times 13$ et $e = 7$

(a) Déterminer la clé privée (d, n) où d est l'inverse de e modulo $\varphi(n)$.

- on calcule d'abord $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1) = 120$. 0,5
- A l'aide de l'algo d'Euclide étendu entre 120 et 7, on obtient :

$$7^{-1} \equiv -17 \equiv 103 \mod 120$$ (une seule étape suffit !)

1

- On en déduit la clé privée $(103, 143)$.

(b) Déchiffrer le message "123".

La fonction de déchiffrement est :

$$\begin{array}{rccc} D_k : & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ & c_i & \longmapsto & c_i^d \end{array}$$ 0,5

Pour calculer, de manière efficace (indispensable ici), on utilise l'exponentiation rapide :

- $123^{103} = 123^{2^6 + 2^5 + 2^2 + 2^1 + 1}$ 1
- $123^2 \equiv 114$

$123^{2^2} \equiv 114^2 \equiv 126$

$123^{2^3} \equiv 126^2 \equiv 3$

$123^{2^4} \equiv 3^2 \equiv 9$

$123^{2^5} \equiv 9^2 \equiv 81$

$123^{2^6} \equiv 81^2 \equiv 126$

On en déduit :

$$123^{103} \equiv 126 \times 81 \times 126 \times 114 \times 123$$
$$\equiv 85$$

D'où le message clair "85". 1