MASTER EII

Epreuve : CRYPTOGRAPHIE / M. BONNETON

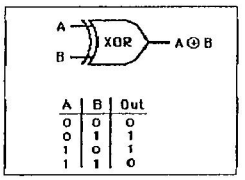
JUILLET 2014 Durée : 2 heures

Calculatrice graphique autorisée – Aucun document

Exercice 1 : L'armée de César comptait plus de 1000 hommes et moins de 3000. Lorsqu'il voulut la dénombrer par groupes de 9, il restait 5 soldats, par groupes de 13, il en restait 8. En revanche, il pouvait faire des groupes de 11 sans qu'il ne reste de soldats. Combien y avait-il d'hommes dans son armée ?

Exercice 2 : Lester Hill (mathématicien américain, 1891-1961) a publié en 1929 une méthode de chiffrement dite polygraphique. On commence par associer à chaque lettre de l'alphabet un nombre compris entre 0 et 25 (A=0, B=1, … , Z=25). On se donne une matrice $A = \begin{vmatrix} 2 & 5 \\ 1 & 3 \end{vmatrix}$

1. Vérifier que la matrice A permet de chiffrer correctement un message en clair et de la décoder.
2. Chiffrer le message « CODAGE »
3. Décoder le message « EELBZJ »



Exercice 3 : Compléter les réseaux de Feistel suivants :

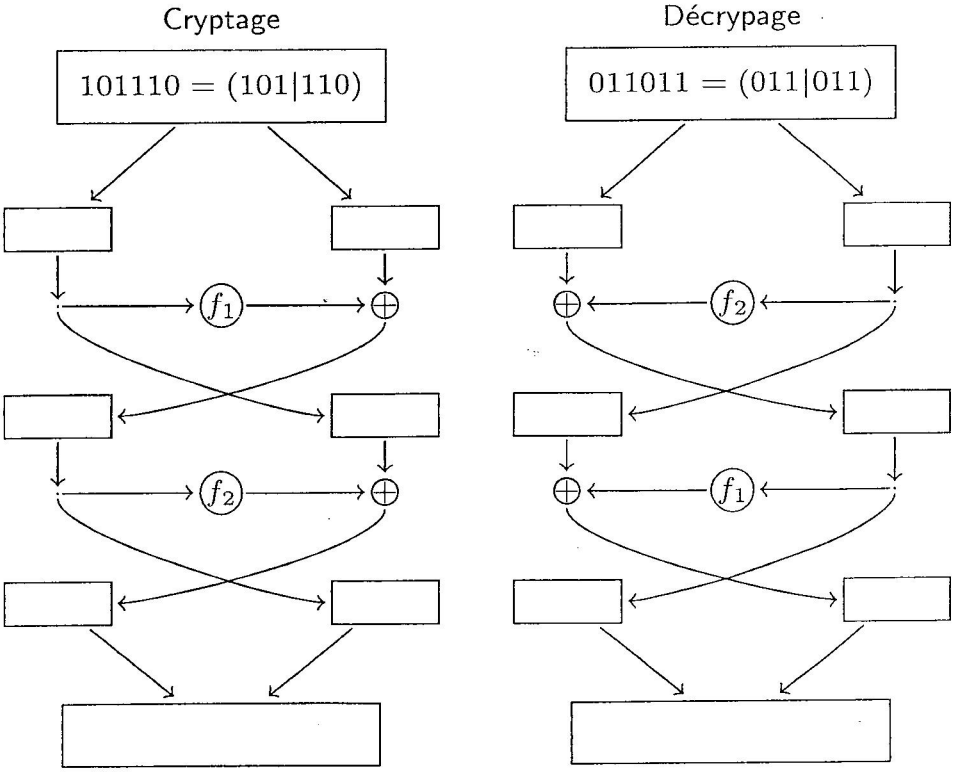
$w = 101110 \in \{0,1\}^6$

$f_1 : \{0,1\}^3 \to \{0,1\}^3$

$000 \to 101$
$001 \to 100$
$010 \to 111$
$100 \to 000$
$011 \to 001$
$101 \to 101$
$110 \to 010$
$111 \to 110$

$f_2 : \{0,1\}^3 \to \{0,1\}^3$

$000 \to 010$
$001 \to 001$
$010 \to 110$
$100 \to 111$
$011 \to 110$
$101 \to 011$
$110 \to 001$
$111 \to 100$



Exercice 4 : *ATTAQUE DU RSA SUR MODULE COMMUN*

Alice, Bob et Charlie, trois dangereux terroristes, préparent un double attentat contre la maison blanche. Pour communiquer à ses deux complices le message m contenant l'heure de l'attentat (format hhmm), Alice leur envoie les messages chiffrés : $m_1 = 4166 \equiv m^{e1} \bmod n$ et $m_2 = 5094 \equiv m^{e2} \bmod n$

En utilisant leurs clés RSA publiques respectives : (n , e_1) = (9313 , 5465) & (n , e_2) = (9313 , 7807)

Mais ces deux messages m_1 et m_2 sont interceptés ainsi que leurs clés publiques par les services du NCIS.

1/ En découvrant ces données, l'agent T. MC Guy s'écrit : « Mais ils ont pris le même module n et en plus les exposants de chiffrement publiques e_1 et e_2 sont premiers entre eux !!!! Quelle erreur !!! Je dois pouvoir déchiffrer ce message par une simple attaque sur module commun ! »

a/ Vérifiez que e_1 et e_2 sont premiers entre eux.

b/ Déterminez une identité de Bezout entre e_1 et e_2 : $e_1 \times d_1 + e_2 \times d_2 = 1$

c/ En partant de $m = m^1 = m^{e1 \times d1 + e2 \times d2} \bmod n$, montrer que l'on peut retrouver m à l'aide de m_1, m_2, d_1 et d_2.

d/ Sachant que $m_2^{-1} = 7940 \bmod n$, en déduire l'heure de l'attentat m.

2/ L'agent A. Sciuto marmonne : « C'est quoi cette attaque sur module commun ? Je suis sûre que ma calculatrice viendra à bout plus rapidement de la factorisation de n= 9313 !! »

a/ Déterminer la décomposition en facteurs premiers de 9313.

b/ En déduire la valeur de l'indicatrice d'Euler : $\phi(n)$

c/ Déterminer maintenant c_1 l'inverse de $e_1 \bmod \phi(n)$

d/ Retrouver l'heure de l'attentat m à partir de m_1 et d_1.

Rappels et aide :

- Pour montrer que deux nombres sont premiers entre eux, il faut calculer le PGCD des 2 nombres.
- Règles de calculs sur les puissances : $x^{ab+c} = x^{ab} \cdot x^c = (x^a)^b \cdot x^c = (x^b)^a \cdot x^c$
- $x^{-a} = (1/x)^a$
- $4166^{10} = 5798 \bmod 9313$ $\qquad$ $5094^{-7} = 7940^{7} = 4835 \bmod 9313$
- Indicatrice d'Euler : $\phi(n) = n\left(1-\frac{1}{p_1}\right)\ldots\left(1-\frac{1}{p_r}\right)$
- $4166^{5} = 1200 \bmod 9313$

Le théorème chinois des restes

Soit $m_1, m_2, \ldots, m_r$ une suite d'entiers positifs premiers entre eux deux à deux. Alors le système de congruences :

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \cdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

a une solution unique x modulo $M = m_1 \times m_2 \times \cdots \times m_r$:

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_r M_r y_r$$

avec

$$M_i = M/m_i \qquad y_i M_i \equiv 1 \pmod{m_i}$$

Le chiffre de Hill est à l'intersection de l'arithmétique et de l'algèbre linéaire. En remplaçant les lettres par des nombres (A-->0,...), on ne traite plus que des entiers compris entre 0 et 25. En outre, un nombre n est identifié avec tous les nombres n+26k, où k est un entier (en clair, si 1 représente B, 27,53,-25... aussi!). Quand les calculs faits par les combinaisons linéaires sortent des entiers de 0 à 25, on s'y ramène en prenant le reste dans la division par 26. On dit que l'on travaille dans $\mathbb{Z}/26\mathbb{Z}$.

Chaque groupe de 2 lettres, ou par identification de 2 nombres x_1,x_2, est représenté par un vecteur colonne $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$. Les relations de dépendance linéaire sont, comme souvent, représentés par une matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. On a, dans $\mathbb{Z}/26\mathbb{Z}$, la relation

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = A \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

où $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ est le bloc codé, et $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ est le bloc clair.

Une matrice carrée à coefficient dans $\mathbb{Z}/26\mathbb{Z}$ est inversible si et seulement si son déterminant est inversible modulo 26. De plus, lorsque $m = 2$, l'inverse est donné par la formule :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = (ad - bc)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

RAPPEL SUR LE RSA :

Alice		Bob
M		
		choisit p et q e premier avec $p-1$ et $q-1$
		calcule $n = p \times q$ d tel que $ed \equiv 1 \pmod{\varphi(n)}$
	$\longleftarrow$	envoie (n, e) à Alice
calcule $C = M^e \pmod{n}$ et l'envoie à Bob	$\longrightarrow$	
		calcule $C^d \pmod{n}$