Chapitre I : exercices + solutions

MOHAMED MEJRI

Groupe LSFM
Département d'Informatique et de Génie Logiciel
Université LAVAL
Québec, Canada

Chiffrement affine

Rappel :

- **Théorème d'Euler** : si $pgcd(a, n) = 1$ alors $a^{\phi(n)} \equiv 1 \; mod \; n$
- Fonction d'Euler $\phi(n) = |\{k|0 < k < n$ et $pgcd(k, n) = 1\}|$: (le nombre d'entiers k, $0 < k < n$, premiers avec n)
- si p est premier alors $\phi(p) = p - 1$
- si p et q sont premiers alors $\phi(p \times q) = (p - 1) \times (q - 1)$
- L'inverse d'un élément a dans $\mathbb{Z}_n$ est a^{-1} tel que $(a \times a^{-1}) \equiv 1 \; mod \; n$
- l'inverse de a n'existe dans $\mathbb{Z}_n$ que si et seulement si $pgcd(a, n) = 1$
- Donc d'après le théorème d'Euler, l'inverse de a, quand cela existe, est $a^{\phi(n)-1} \; mod \; n$ puisque $a \times a^{\phi(n)-1} \equiv 1 \; mod \; n$
- Exemple : l'inverse de 3 dans $\mathbb{Z}_{26}$ est $3^{11} \; mod \; 26 = 9$ puisque $\phi(26) = \phi(2 \times 13) = 1 \times 12 = 12$

Chiffrement affine

➾ Question : Trouver m tel que : $e_k(m) = WNIIR\ PRAIK$ avec $k = (3, 1)$.

➾ Solution : Puis que l'inverse de 3 dans $\mathbb{Z}_{26}$ est 9 ($9 * 3 \equiv 1\ mod\ 26$), donc :

$$d_k(y) = 9(y - 1) mod\ 26$$

$$\begin{array}{lll}
d_k(W) = (22(W) - 1) * 9\ mod\ 26 = 7 & \mapsto & H \\
d_k(N) = (13(N) - 1) * 9\ mod\ 26 = 4 & \mapsto & E \\
d_k(I) = (8(I) - 1) * 9\ mod\ 26 = 11 & \mapsto & L \\
d_k(I) = (8(I) - 1) * 9\ mod\ 26 = 11 & \mapsto & L \\
d_k(R) = (17(R) - 1) * 9\ mod\ 26 = 14 & \mapsto & O \\
d_k(P) = (15(P) - 1) * 9\ mod\ 26 = 22 & \mapsto & W \\
d_k(R) = (17(R) - 1) * 9\ mod\ 26 = 14 & \mapsto & O \\
d_k(A) = (0(A) - 1) * 9\ mod\ 26 = 15 & \mapsto & R \\
d_k(I) = (8(I) - 1) * 9\ mod\ 26 = 11 & \mapsto & L \\
d_k(K) = (10(K) - 1) * 9\ mod\ 26 = 3 & \mapsto & D
\end{array}$$

$$d_k(WNIIR\ PRAIK) = HELLO\ WORLD$$

UNIVERSITÉ LAVAL

Chiffrement par substitution

➩ Question : Trouver m tel que : $e_\pi(m) = QSNQRFRSRFLK$ avec π est celle donnée dans l'acétate 20.

➩ Solution :

$$
\begin{array}{lclcl}
\pi^{-1}(16(Q)) & = & 18 & \mapsto & S \\
\pi^{-1}(18(S)) & = & 20 & \mapsto & U \\
\pi^{-1}(13(N)) & = & 1 & \mapsto & B \\
\pi^{-1}(16(Q)) & = & 18 & \mapsto & S \\
\pi^{-1}(17(R)) & = & 19 & \mapsto & T \\
\pi^{-1}(5(F)) & = & 1 & \mapsto & I \\
\pi^{-1}(17(R)) & = & 19 & \mapsto & T \\
\pi^{-1}(18(S)) & = & 20 & \mapsto & U \\
\pi^{-1}(17(R)) & = & 19 & \mapsto & T \\
\pi^{-1}(5(F)) & = & 1 & \mapsto & I \\
\pi^{-1}(11(L)) & = & 14 & \mapsto & O \\
\pi^{-1}(10(K)) & = & 13 & \mapsto & N
\end{array}
$$

$$d_k(VEFCCPBJBKR) = SUBSTITUTION$$

Carré de Polybe

➩ Question : La plus fameuse victime de la cryptanalyse est :

44211 21324 15522 11215

Trouver son nom sachant qu'il a été crypté avec le carré de Polybe en utilisant "CRYPTANALYSE" comme clé.

➩ Solution : Le carré de Polybe avec "CRYPTANALYSE" comme clé est :

	1	2	3	4	5
1	C	R	Y	P	T
2	A	N	L	S	E
3	B	D	F	G	H
4	I	J	K	M	O
5	Q	U	V	X	Z

$$d_k(44211\ 21324\ 15522\ 11215) = MARY\ STUART$$

Chiffrement par permutation

- **Question :** En statistique, pour critiquer la notion de "moyenne", on dit : lecqiu aiutal etenad nusuof tersel eipdsd snafnu gireso nesnet yomnne rtebse nei
  Retrouver le message en clair correspondant sachant qu'il a été crypté avec le chiffrement par permutation en utilisant 3 2 1 comme clé.
- **Solution :** $\pi = (3\ \ 2\ \ 1)$ donc $\pi(1) = 3; \pi(2) = 2\ \ \pi(3) = 1$ et $\pi^{-1}(1) = 3; \pi^{-1}(2) = 2\ \ \pi^{-1}(3) = 1$. On déduit que :

$$
\begin{array}{rl}
& d_k(lecqiuaiutaletenadnusuofterslee ipdsdsnafnugiresonosnetyomnnertebsenei) \\
= & d_k(lec)d_k(qiu)d_k(aiu)d_k(tal)d_k(ete)d_k(nad)d_k(nus)d_k(uof)d_k(ter)d_k(sel)d_k(eip)d_k(dsd) \\
& d_k(sna)d_k(fnu)d_k(gir)d_k(eso)dd_k(nes)d_k(net)d_k(yom)d_k(nne)d_k(rte)d_k(bse)d_k(nei) \\
= & celuiquialatetedansunfouretlespiedsdansunfrigosesentenmoyennetresbien
\end{array}
$$

Résultat : celui qui a la tête dans un four et les pieds dans un frigo se sent en moyenne très bien.

Chiffrement de Hill

Question : Le plus petit entier x tel que les trois nombres x, x^2 et x^3 épuisent tous les chiffres $(0, 1, ..., 9)$ est : $YUNCNAQBEVTE$
Retrouver cet entier sachant qu'il a été écrit en toutes lettres et crypté avec le chiffrement de Hill en utilisant la matrice

$$K = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$$

Solution : L'inverse de K dans $\mathbb{Z}_{26}$ est :

$$K^{-1} = \begin{pmatrix} 18 & 17 \\ 17 & 18 \end{pmatrix}$$

$$\begin{array}{lcl}
(Y, U)K^{-1} & = & (24, 20)K^{-1} = (18, 14) = (S, O) \\
(N, C)K^{-1} & = & (I, X) \\
(N, A)K^{-1} & = & (A, N) \\
(Q, B)K^{-1} & = & (T, E) \\
(E, V)K^{-1} & = & (N, E) \\
(T, E)K^{-1} & = & (U, F)
\end{array}$$

Réponse : SOIXANTE NEUF : $(69, 69^2 = 4761, 69^3 = 328509)$