TP : Cryptosystèmes Classiques

1 Chiffrement par substitution

Notons $\mathbb{Z}_{26} = \mathbb{Z}/26\mathbb{Z}$ l'anneau quotient représentant les 26 lettres de l'alphabet.
Soit $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$ et $\mathcal{K}$ l'ensemble des permutations sur l'ensemble des lettres de l'alphabet. Pour chaque permutation $\pi \in \mathcal{K}$, $\forall x,\ y \in \mathbb{Z}_{26}$, on définit le système de chiffrement par substitution par :

$$e_K(x) = \pi(x)$$

$$d_K(y) = \pi^{-1}(y)$$

où π^{-1} est la permutation réciproque de π.

1.1 Cas particulier du chiffrement par décalage

Exercice : Chiffrement par décalage

Soit $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$. $\forall K,\ x,\ y \in \mathbb{Z}_{26}$, on définit :

$$e_K(x) = x + K \mod 26$$

$$d_K(y) = y - K \mod 26$$

Ce cryptosystème est aussi appelé chiffrement de César, car jules César l'utilisait (avec la clé $K = 3$ et l'alphabet romain).

1. Montrer que le système de chiffrement par décalage est un cas particulier du système de chiffrement par substitution.
2. Que vaut $-K \mod 26$? Vérifier que le chiffrement par décalage forme bien un cryptosystème.
3. Quelle est la taille de l'espace des clés $\mathcal{K}$? Que pensez vous de la sécurité de ce cryptosystème ?

1.2 Cas particulier du chiffrement affine

Exercice : Chiffrement affine

Soit $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$ et $\mathcal{K}$ l'ensemble des éléments (a, b) de $\mathbb{Z}_{26} \times \mathbb{Z}_{26}$ tels que $a \in \mathbb{Z}_{26}^{\times}$. $\forall K = (a, b) \in \mathcal{K}$, $\forall x,\ y \in \mathbb{Z}_{26}$, on définit le système de chiffrement affine par :

$$e_K(x) = ax + b \mod 26$$

$$d_K(y) = a^{-1}(y - b) \mod 26$$

1. Implémenter en C le système de chiffrement affine.
2. La fonction indicatrice d'Euler est la fonction $\phi : \mathbb{N}^* \to \mathbb{N}^*$ qui à un entier m associe le nombre d'entiers positifs inférieurs à m et premiers avec m. Soit p un nombre premier. Que vaut $\phi(p)$? Soit $e > 0$. Que vaut $\phi(p^e)$? Soit $m = \prod_{i=1}^{n} p_i^{e_i}$. En utilisant le théorème chinois, donner la fomule donnant $\phi(m)$.

3. En utilisant la fonction indicatrice d'Euler, calculer $|\mathcal{K}|$ où $\mathcal{K}$ est défini comme l'ensemble des éléments (a, b) de $\mathbb{Z}_{26} \times \mathbb{Z}_{26}$ tels que $a \in \mathbb{Z}_{26}^{\times}$. Que pensez vous de la sécurité de ce cryptosystème ?

4. Retrouver le message clair correspondant au chiffré suivant :

```
char cipher[9][25] = {"KQEREJEBCPPCJCRKIEACUZ",
                      "BKRVPKRBCIBQCARBJCVFCUP",
                      "KRIOFKPACUZQEPBKRXPEII",
                      "EABDKPBCPFCDCCAFIEABDKP",
                      "BCPFEQPKAZBKRHAIBKAPCC",
                      "IBURCCDKDCCJCIDFUIXPAFF",
                      "ERBICZDFKABICBBENEFCUP",
                      "JCVKABPCYDCCDPKBCOCPERK",
                      "IVKSCPICBRKIJPKABI"};
```

Pour y parvenir, on pourra procéder comme suit :

a) en utilisant un corpus, calculer la table des fréquences d'apparition des caractères puis classer cette table par ordre décroissant de valeur ;

b) calculer la table des fréquences d'apparition des caractères chiffré puis classer cette table par ordre décroissant de valeurs ;

c) implémenter l'algorithme d'Euclide étendu ;

d) en observant que $e_K(x) = ax + b$ peut conduire à un système de deux équations à deux inconnues (a et b), et que pour être légale, une clé $K = (a, b)$ doit satisfaire $\gcd(a, 26) = 1$, retrouver la clé K puis le message clair.

1.3 Cryptanalyse du chiffrement par substitution

Exercice : Chiffrement par substitution

Notons $\mathbb{Z}_{26} = \mathbb{Z}/26\mathbb{Z}$ l'anneau quotient représentant les 26 lettres de l'alphabet.
Soit $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$ et $\mathcal{K}$ l'ensemble des permutations sur l'ensemble des lettres de l'alphabet. Pour chaque permutation $\pi \in \mathcal{K}$, $\forall x, y \in \mathbb{Z}_{26}$, on définit le système de chiffrement par substitution par :

$$e_K(x) = \pi(x)$$

$$d_K(y) = \pi^{-1}(y)$$

où π^{-1} est la permutation réciproque de π.

1. Implémenter en C le système de chiffrement par substitution. Quelle est la taille de l'espace des clés $\mathcal{K}$? Que pensez-vous de la sécurité de ce cryptosystème ?

2. Retrouver le message clair correspondant au chiffré suivant :

```
char cipher[11][24] = {"EMGLOSUDCGDNCUSWYSFHNSF",
                       "CYKDPUMLWGYICOXYSIPJCK",
                       "QPKUGKMGOLICGINCGACKSNI",
                       "SACYKZSCKXECJCKSHYSXCG",
                       "OIDPKZCNKSHICGIWYGKKGKG",
                       "OLDSILKGOIUSIGLEDSPWZU",
                       "GFZCCNDGYYSFUSZCNXEOJNC",
                       "GYEOWEUPXEZGACGNFGLKNS",
                       "ACIGOIYCKXCJUCIUZCFZCCN",
                       "DGYYSFEUEKUZCSOCFZCCNC",
                       "IACZEJNCSHFZEJZEGMXCYHC"};
```

Pour y parvenir, on pourra procéder comme suit :

a) en utilisant un corpus, calculer les tables des fréquences d'apparition des caractères, des digrammes et des trigrammes puis classer ces tables par ordre décroissant de valeur

b) calculer les tables des fréquences d'apparition des caractères, des digrammes et des trigrammes dans le chiffré puis classer ces tables par ordre décroissant de valeurs

d) en déduire une méthode (interactive) permettant de retrouver le message clair.