Licence 3-MHT633 Université Bordeaux 1
2009/2010

Feuille 1 : Chiffrements anciens

Dans toute la feuille on utilise la numérotation des lettres de l'alphabet suivante :

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	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

Exercice 1. L'anneau $\mathbb{Z}/n\mathbb{Z}$

Soit n un entier naturel non nul.

1. Rappeler la définition de l'ensemble $\mathbb{Z}/n\mathbb{Z}$.
2. Donner la structure de groupe de $\mathbb{Z}/n\mathbb{Z}$. Est-il abélien ? Quel est son cardinal ?
3. Donner la structure d'anneau de $\mathbb{Z}/n\mathbb{Z}$? Est-il abélien ?
4. Caractériser les inversibles de $\mathbb{Z}/n\mathbb{Z}$.

Exercice 2. Chiffrement affine

Étant donnés deux entiers a et b, une lettre de l'alphabet est identifiée à un élément x de l'anneau $\mathbb{Z}/26\mathbb{Z}$ et est chiffrée en $ax + b$.

1. Montrez que la fonction de chiffrement est inversible ssi $a \mod 26 \in (\mathbb{Z}/26\mathbb{Z})^*$ et calculez son inverse. Précisez les données $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ de ce système de chiffrement. Quel est le cardinal de $\mathcal{K}$?
2. Un chiffrement affine dont vous ne connaissez pas la clé a chiffré le texte clair «hahaha» en «nonono». Retrouvez la clé. (Il s'agit d'une attaque à texte clair connu). Calculez la clé de déchiffrement.
3. Montrez que la composée de deux chiffrements affines est encore un chiffrement affine.
4. Montrez qu'un chiffrement par décalage est un cas particulier de chiffrement affine. Montrez qu'un chiffrement affine est un cas particulier de chiffrement de substitution.
5. Généralisez la définition d'un système de chiffrement affine sur l'anneau $A = \mathbb{Z}/m\mathbb{Z}$. Généralisez l'attaque précédente : que doit avoir en sa possession un attaquant pour calculer la clé ?

Exercice 3. Matrices à coefficients dans un anneau

Soit $(A, +, \cdot)$ un anneau commutatif et unitaire.

1. Montrez que l'ensemble des matrices à n lignes et n colonnes, à coefficients dans A, est un anneau pour l'addition et la multiplication des matrices. On le note $M_n(A)$.
2. Montrez que $M \in M_n(A)$ est inversible si et seulement si $\det(A)$ est inversible dans A.
3. Pour $n = 2$, montrez que $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est inversible dans $M_2(A)$ si et seulement si $ad - bc \in A^*$ et que dans ce cas
$$M^{-1} = (ad - bc)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$
4. On note $Gl_n(A)$ le groupe des matrices inversibles de $M_n(A)$. Montrez que l'ordre de $Gl_2(\mathbb{Z}/p\mathbb{Z})$ où p est un nombre premier est $(p^2 - 1)(p^2 - p)$. (indication :Cherchez quelles conditions les colonnes d'une matrice inversible doivent satisfaire).
5. Généralisation : montrez que
$$|Gl_n(\mathbb{Z}/p\mathbb{Z})| = (p^n - 1)(p^n - p)(p^n - p^2) \dots (p^n - p^{n-1}).$$

Exercice 4. Chiffrement de Hill

Soit $K \in Gl_n(A)$, on définit
$$\begin{aligned} e_K : A^n &\to A^n \\ x &\mapsto xK \end{aligned}$$

1. Montrez qu'on définit ainsi un système de chiffrement symétrique dont on précisera les données $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$.
2. Exemple numérique : «YIFZMA» est un texte chiffré par un chiffrement de Hill avec $n = 2$ et $A = \mathbb{Z}/26\mathbb{Z}$, de matrice $K = \begin{pmatrix} 9 & 13 \\ 2 & 3 \end{pmatrix}$. Retrouvez le clair.
3. Eve a volé la machine à chiffrer de Bob, qui utilise un chiffrement de Hill avec une matrice 2×2 sur $\mathbb{Z}/26\mathbb{Z}$. Elle tente une attaque à texte choisi : le texte clair «ba» est chiffré en «HC» et le texte clair «zz» est chiffré en «GT». Quelle est la clé ? Quelle est la clé de déchiffrement ? Que pensez-vous des choix de Eve ?
4. Généralisez l'attaque de Eve (à clair choisi) à un système de chiffrement de Hill quelconque.
5. Montrez que la composée de deux chiffrements de Hill est encore un chiffrement de Hill. Vous considèrerez le cas de matrices de même taille, puis de tailles différentes.

6. Montrez qu'un chiffrement par permutation est un cas particulier d'un chiffrement de Hill.
7. «GEZXDS» est un texte chiffré par un chiffrement de Hill de matrice 2×2. Le clair est «solved». Trouvez la clé. Calculez ensuite la clé de déchiffrement.

Exercice 5. Cryptanalyse par fréquences

Le but de l'exercice est de déchiffer le texte chiffré ci-dessous grâce à une analyse de fréquence. Le texte est en français. On utilisera la fait que la lettre la plus fréquente en français est le E, viennent ensuite S puis A.

$$\begin{array}{cccc} XGCLKPHEUL & GPFQYYWHST & YIYHFENYIG & HFYIGHQASY \\ DQWGTHGWYC & SLQWYLXYWC & EIISTQCGHQ & ETWTSIYLQA \\ SYW & & & \end{array}$$

1. On suppose que la lettre la plus fréquente dans le message clair est le E. Le message a t-il été chiffré par décalage ?
2. On suppose que le chiffrement est affine. Essayer de déchiffrer le message.
3. On veut maintenant adapter cette méthode à un chiffrement de Vigenère. Trouver la longueur de la clé utilisée pour chiffrer le message suivant.

$$\begin{array}{cccc} PVCIGHMSRO & RWMSWNOTQW & WYTEAOZLPV & CIGHMSMRLD \\ PAILUZMLNH & OEWOUWXCOU & MVXGUNNSXL & MJNUMKVLOF \\ QFMEIITJLS & NXXEAOZLPV & CIGHMETAWM & AWUPIVBMWM \\ KLPGILXVQL & MK & & \end{array}$$

4. Connaissant la longueur de la clé comment peut-on se ramener à un chifffrement par décalage ?

Exercice 6. chiffrement par substitution

Soit σ une permutation de $\mathbb{Z}/26\mathbb{Z}$. Chaque lettre de l'alphabet est identifiée à un élément x de $\mathbb{Z}/26\mathbb{Z}$ et est chiffré $\sigma(x)$.

1. Précisez les données $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ de ce système de chiffrement.
2. Quel est le cardinal de $\mathcal{K}$? Comparer avec le nombre de clés dans le cas du chiffrement affine et dans le cas du chiffrement par décalage. Dans le cas d'une attaque par recherche exhaustive de clé quel est le chiffrement le plus sûr ? Peut on généraliser l'attaque du chiffrement affine dans ce cas ?

3. L'application $x \to x^5$ définit elle une permutation de $\mathbb{Z}/31\mathbb{Z}$? Quels sont les d tels que l'application $x \to x^d$ définisse une permutation de $\mathbb{Z}/31\mathbb{Z}$? Dans ce cas quelle est la fonction de déchiffrement ?

Exercice 7. Clés involutives

Le but de l'exercice est de trouver des chiffrements dont la fonction de déchiffrement est la même que la fonction de chiffrement.

1. Si la fonction de chiffrement est involutive quelle est la clé de déchiffrement ?
2. On se place dans le cas d'un chiffrement par décalage sur l'alphabet $\mathbb{Z}/n\mathbb{Z}$. Trouver toutes les clés involutives (*i.e.* telles que la fonction de chiffrement est involutive). Traiter les cas $n = 26$ et $n = 29$.
3. Si le chiffrement est affine sur $\mathbb{Z}/n\mathbb{Z}$, caractériser les clés involutives. Préciser le nombre de clés involutives dans le cas où n est un nombre premier.
4. Si le chiffrement est un chiffrement par permutation de longueur n, combien y a-t-il de clés involutives.

   On rappelle qu'un chiffrement par permutation, de permutation $\sigma \in S_n$, envoie le message $x = (x_1, x_2, \ldots, x_n) \in (\mathbb{Z}/26\mathbb{Z})^n$ sur le message $(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$.