TD 1 : Arithmétique et chiffrement

Exercice 1. * Effectuez les divisions euclidiennes suivantes :

1. division de 43 par 12
2. division de 87 par 9

Exercice 2. *

1. Écrire les tables de multiplication dans $\mathbb{Z}/6\mathbb{Z}$ et $\mathbb{Z}/7\mathbb{Z}$.
2. (a) Résoudre dans $\mathbb{Z}/6\mathbb{Z}$ les équations :
   i. $5x = 4$
   ii. $2x = 4$
   iii. $2x = 5$
   (b) Mêmes questions dans $\mathbb{Z}/7\mathbb{Z}$.

Exercice 3. * Inverse
Calucler les inverses modulo 7 de :

- 3
- 4

Exercice 4. **

1. En utilisant l'algorithme d'Euclide étendu, calculez (s'il existe) l'inverse de 5 dans $\mathbb{Z}/26\mathbb{Z}$.
2. En utilisant l'algorithme d'Euclide étendu, calculez (s'il existe) l'inverse de 22 dans $\mathbb{Z}/79\mathbb{Z}$.
3. En utilisant l'algorithme d'Euclide étendu, calculez (s'il existe) l'inverse de 441 dans $\mathbb{Z}/777\mathbb{Z}$.

Exercice 5. * Restes Chinois
Trouver le plus petit entier positif x tel que (à la fois) :
$x \equiv 1 \mod 3$
$x \equiv 2 \mod 5$
$x \equiv 3 \mod 7$

Exercice 6. * Restes Chinois
Trouver le plus petit entier positif x tel que (à la fois) :
$x \equiv 3[17]$
$x \equiv 4[11]$
$x \equiv 5[6]$

Exercice 7. ** Fermat
Montrer que, quel que soit l'entier naturel n non nul, $n^5 - n$ est divisible par 30.

Cryptographie

Vocabulaire

- La *Cryptologie* est la science des messages secrets. Elle se décompose en deux disciplines :
  - ⋆ la *Cryptographie*, art de transformer un message clair en un message inintelligible par celui qui ne possède pas la clé de déchiffrement. Cependant, on utilise souvent le mot cryptographie comme synonyme de cryptologie.
  - ⋆ la *Cryptanalyse*, art d'analyser un message chiffré afin de le décrypter quand on ne possède pas la clé de déchiffrement.
- *Chiffre* : anciennement code secret, par extension désigne aussi un algorithme utilisé pour le chiffrement ;
- *Chiffrer* : transformer à l'aide d'une clé de chiffrement un message en clair en un message chiffré, incompréhensible si on ne dispose pas de la clé de déchiffrement correspondante ;
- *Déchiffrer* : retrouver à l'aide de la clé de déchiffrement correspondante le message en clair d'origine à partir d'un message précédemment chiffré à l'aide d'une clé de chiffrement ;
- *Clé de chiffrement* : méthode permettant de chiffrer un message en clair ;
- *Clé de déchiffrement* : méthode associée à une clé de chiffrement et permettant de déchiffrer un message précédemment chiffré ;
- *Décrypter* : retrouver le message en clair correspondant à un message chiffré sans posséder la clé de déchiffrement ni la clé de chiffrement ;
- *Chiffré* : message chiffré (incompréhensible si on ne dispose pas de la bonne clé de déchiffrement).

Consignes générales

- On écrit les messages en lettres majuscules et sans accents. Ceci a pour but de simplifier le chiffrement et le déchiffrement des messages.
- Lorsque les messages sont constitués de plusieurs mots ou de plusieurs phrases, on conserve les espaces entre les mots et les signes de ponctuation. Le résultat est de faciliter encore le déchiffrement.
- Ce n'est pas conforme à la réalité, puisque dans la vraie vie, on veut au contraire compliquer au maximum le cryptogramme, pour empêcher l'adversaire de le décrypter, si possible...
- Plus un cryptogramme est long, plus il est facile à décrypter, car l'adversaire dispose de plus d'indices. Ceci explique pourquoi, dans les exercices, les messages à décrypter seront significativement plus longs que les messages à chiffrer ou à déchiffrer.
- On utilise la correspondance ci-dessous entre les lettres de l'alphabet $\{A, B, C, \dots, Z\}$ et les nombres $\{0, 1, 2, \dots, 25\}$.

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

Chiffrement par décalage

- Un chiffrement par décalage consiste à décaler les lettres de l'alphabet d'une valeur fixe.
- Et bien sûr, si on dépasse Z, on reprend à partir de A.
- Autrement dit, on travaille « modulo 26 ».

Exercice 8 (Chiffre de César)**.** *
Les lettres de l'alphabet sont chiffrées à l'aide de la clé de chiffrement :

$$f : \begin{cases} \{0,1,\dots,25\} & \longrightarrow & \{0,1,\dots,25\} \\ x & \mapsto & f(x) = x+3 \mod 26 \end{cases}$$

Cette méthode est réputée avoir été utilisée par Jules César pour communiquer secrètement avec ses généraux pendant la guerre des Gaules, d'où son nom.

1. Chiffrer le message : ALLEZ-Y !
2. Quelle est la clé de déchiffrement du chiffre de César ?
3. Déchiffrer la réponse du général : RQ B YD !

Exercice 9 (Une faiblesse dangereuse)**.** *
Combien y-a-t-il de chiffrements par décalage différents ?

Exercice 10. * Classer des chiffrés
Alice a laissé ce petit fichier sur son bureau. Les onze messages qu'il contient sont bien trop courts pour être décryptés.

1. `CA CLWD AGQ XWTQ`
2. `QD KLE KADQ GWOEECA`
3. `TSIB NSNAINP WITTI BJZSII`
4. `GWOEECA HWONA WD DA NAOQ TAGNLTAT`
5. `VI BJZS WJNSJHHI VI DJNS`
6. `IHWJSI NH AFGZH NSNAINP`
7. `XWTQ WO KLE RQFTRNAI CR`
8. `NH DJNS WJAAIHWI NZIH`
9. `RXWOT KLE`
10. `SDFJNA WPRE KADQ DSEWQU`
11. `GJNG AFGZH OIVZIHG ZHZ`

- Saurez-vous classer ces messages en deux ensembles, correspondant à deux chiffrements distincts ? Puis, en réordonnant les premières lettres de l'ensemble le plus petit et les dernières lettres de l'ensemble le plus grand, vous découvrirez deux nombres secrets écrits en français.

Exercice 11. * AVJC

- Dans la cave d'un bâtiment de l'U.S. Navy, des brouillons de lettres, certaines chiffrées et d'autres en clair, ont été retrouvés dans un vieux carton. À l'aide la lettre de la figure 1, saurez-vous decrypter celle de la figure 2 ?

Le 26 avril 1942 à Washington D.C.,

À qui de droit,
J'ai fait des découvertes importantes sur la la cryptanalyse de la machine ENIGMA. J'ai utilisé mes connaissances en cryptographie antique pour protéger mes travaux des curieux, mais je n'ai aucun doute qu'un expert en cryptographie saura y accéder.

Elizebeth Smith Friedman.

Post-Scriptum : Portez ce vieux whisky au juge blond qui fume.

FIGURE 1 – Un brouillon en clair retrouvé dans la cave.

Oh 28 dyulo 1942 d Zdvklqjwrq G.F.,

D txl gh gurlw,
Pd ghfrxyhuwh sruwh vxu od vwuxfwxuh gh od pdfklqh HQLJPD. Hooh shuphw gh idluh ghv vxffhvvlrqv gh vxevwlwxwlrqv hw gh shupxwdwlrqv. M'dl dxvvl o'lpsuhvvlrq txh od vwuxfwxuh ghv phvvdjhv hfkdqjhv hvw vrxyhqw od phph, fh txh qrxv doorqv hvvdbhu g'hasorlwhu.

Holchehwk Vplwk Iulhgpdq.

Srvw-Vfulswxp : Sruwhc fh ylhxa zklvnb dx mxjh eorqg txl ixph.

FIGURE 2 – Un brouillon chiffré retrouvé dans la cave.

- Qui est Elizebeth Smith Friedman ?

Exercice 12. * Chiffrement allemand

- Dans le carton d'archives de la Seconde Guerre mondiale retrouvé dans la cave d'un bâtiment de l'US Navy qui contenait les brouillons des lettres de l'exercice précédent, il y avait aussi les deux lettres des figures 3 et 4. Saurez-vous décrypter celle de la figure 4 ?
- Pourquoi "chiffrement allemand" ?

Exercice 13. * Méli-mélo

- Le brouillon de lettre de la figure 5 a été trouvé dans la cave d'un bâtiment de l'U.S. Navy, dans le même carton d'archives que les messages des exercices précédents. Saurez-vous le décrypter ?

Le 27 avril 1942 à Bletchley Park,

À qui de droit,
Nous avons obtenu une machine ENIGMA et sommes en bonne voie pour en percer les secrets.

Alan Turing.

Post-Scriptum : Buvez de ce whisky que le patron juge fameux.

FIGURE 3 – Une lettre en clair retrouvée dans la cave.

DX AV VX VF AA GG FX DF DX VG XX XA VV AA AD DX AV GD AF DD DX AV VA FG AA FX DV,

AA FV GF DF AG AV AG FX FF DF GD,
FA AV FX AF DF FG FF GF FX AF AV GA FD FF GF GG AV DX DX AV GA, FD FF GF GA AA GG FF FD GA FX AV GF GA GA DF AA AG AV AF DD DF AX AX FX AV FX FV GF AV DX FV GF AV GA FA AV GA GA AA DA AV GA AV FD GG FF VA AV GA FG AA FX DX AV GA AA DX DX AV FA AA FD AG GA.

AA DX AA FD GD GF FX DF FD DA.

FG FF GA GD - GA AF FX DF FG GD GF FA : AD GF GG AV VD AG AV AF AV GV DD DF GA DV VA FV GF AV DX AV FG AA GD FX FF FD DG GF DA AV AX AA FA AV GF GX.

FIGURE 4 – Une lettre chiffrée retrouvée dans la cave.

92Leirav49l1aW2ànishnogt.CD.
iuAqrdde,toi
iaJ'ssaumeiruqareuéqAslemellsdanliutneissetdutaspsceénhouqtiopeseru rerndrclaatypylnalpseidus-ciff.eil

ziElteebimhSrFthmdie.an

FIGURE 5 – Un brouillon chiffré retrouvé dans la cave.