Université de Lille 1 SCIENCES ET TECHNOLOGIES

L1 - SESI - 2015–2016

Arithmétique et Cryptographie

DS1 – Durée 2h
5 mars 2016

Toutes les réponses doivent être justifiées et vous soignerez votre rédaction.

Les documents son interdits, ainsi que les appareils électroniques (téléphones, ordinateurs portables, etc...). Seules les calculatrices sont autorisées.

Notez le numéro de votre groupe sur la copie.

1 Chiffre de César

Pour communiquer avec ses généraux, César utilisait un alphabet à 20 lettres (alphabet antique) :

```
A, B, C, D, E, F, G, H, I, L, M, N, O, P, Q, R, S, T, V, X
```

et le code qui porte aujourd'hui son nom.
Comme d'habitude, on associe à chaque lettre son rang dans l'alphabet : $A \leftrightarrow 0$, $B \leftrightarrow 1, \ldots, X \leftrightarrow 19$.

1. Précisez l'application de chiffrement du code de César, de déchiffrement ainsi que la taille de l'espace des clés.
2. Ce procédé est-il sûr ? Argumentez.

Pour apporter plus de sécurité, César décide d'utiliser le procédé suivant :
— Soit un caractère codé par $m \in \mathbb{Z}\,; 0 \leqslant m \leqslant 19$
— On multiplie m par 3.
— On ajoute 5 au résultat obtenu.
— On multiplie par 7 le résultat obtenu.
— le chiffré de m est le résultat de la dernière opération modulo 20.

3. Chiffrez le mot `BAC` à l'aide de ce procédé.
4. Quelle conjecture faites-vous sur ce procédé de chiffrement ? César a-t-il raison de l'utiliser ?
5. Démontrez la conjecture faite à la question précédente.

2 Chiffrement affine

On considère le chiffrement affine. L'alphabet des lettres à chiffrer est constitué des 26 lettres latines ainsi que de l'espace. L'alphabet comprend donc 27 caractères que nous coderons numériquement de façon usuelle $A \leftrightarrow 0$, $B \leftrightarrow 1$, $\ldots$, $Z \leftrightarrow 25$, l'espace étant codée 26. On rappelle que les clés sont des couples d'entiers $k = (a, b)$ et que le chiffrement d'un caractère de code m s'obtient en calculant $c = (am + b) \pmod{()n}$, n étant la taille de l'alphabet.

1. Chiffrez le mot constitué des trois premières lettres de votre nom avec la clé $k = (13, 8)$.
2. Est-ce que tout couple (a, b) peut servir de clé ? Si oui prouvez-le ! Si non, expliquez pourquoi à partir d'un exemple.
3. Dans le cas de notre alphabet de 27 caractères, quelle est la taille de l'espace des clés ?
4. Déchiffrez le message `XAAYBK` avec la clé $k = (17, 23)$.

Voici un message qui a été chiffré par le chiffrement affine (les passages à la ligne ne sont pas à prendre en considération, ils ne sont là que pour éviter de tout placer sur une seule ligne) :

```
JSIKSHEXT ZXRZXMZJJSPZXT FXJZXISIKZXDSHJXIZXI
OGYECPOSMMZXZJEXOZDFPZXZHXUOSHISFJXICMYEZBXRZ
XHCMNOZXDZXMCEJXDZXIZXMZJJSPZXIRSFO
```

5. Sachant que le message clair qui se cache derrière ce cryptogramme est rédigé en français, et que dans cette langue la lettre la plus fréquente est le `E` et que l'espace l'est encore davantage, déterminez la clé qui a été utilisée, et déchiffrez le dernier mot du message clair.

Indications : les deux caractères les plus fréquents de ce cryptogramme sont le `X` avec 22 occurrences et le `Z` avec 20 occurrences.
de le déchiffrer entièrement.

3 Autour de Bézout

1. Énoncez le théorème de Bézout.
2. Calculez les coefficients de Bézout pour les nombres $a = 6102$ et $b = 2016$.
3. Résoudre l'équation $ax + by = c$, a et b étant les deux nombres de la question précédente, et c ayant successivement pour valeur 17, 18 et 36.
4. On pose $a' = a/d$ et $b' = b/d$, avec $d = \text{pgcd}(a, b)$. Justifiez le fait que b' est inversible modulo a', et calculez son inverse.

4 Surchiffrement

Comme nous l'avons vu lors du TP, le chiffrement monoalphabétique par substitution consiste à associer chaque lettre de l'alphabet à une autre lettre de l'alphabet sans ordre fixe ou règle générale. La seule condition est que deux lettres différentes ne soient pas associées à la même lettre. Voici un exemple de correspondance :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
C	B	I	Q	Y	A	D	J	R	Z	M	E	K	T	P	F	L	V	U	G	N	W	S	H	O	X

Malgré un très grand nombre de clé possibles, la faiblesse de ce chiffrement est qu'une même lettre est toujours chiffrée de la même façon. Nous avons vu lors du TP que l'on pouvait déchiffrer un texte suffisamment long encodé avec chiffrement monoalphabétique par substitution en procédant avec une analyse fréquentielle.
Pour remédier à cette faiblesse, on envisage différents procédés de «surchiffrement».

1. **Premier procédé :** On choisit une correspondance puis un nombre k compris entre 0 et 25. On chiffre le texte en appliquant la substitution monoalphabétique puis en appliquant un chiffre de César avec un décalage de k. Par exemple, le message `BONJOUR` encodé avec la correspondance ci-dessus et un décalage de 2 devient : `DRVBRPX`. Proposez une attaque pour déchiffrer un texte suffisamment long. Ce procédé de chiffrement est-il plus sûr que le chiffrement mono-alphabétique ? Justifiez.
2. **Second procédé :** On choisit une correspondance et on chiffre le texte de la manière suivante. On applique le chiffrement mono-alphabétique puis on décale la première du message de 1, la deuxième de 2, la $k^{\text{ième}}$ de $k \pmod{26}$,...
   (a) Utilisez la correspondance donnée en exemple pour chiffrer le message suivant avec ce procédé : `BONJOUR`. Que constatez-vous ?
   (b) Quelle est la taille de l'espace des clés ?
   (c) Proposez une attaque pour déchiffrer un texte suffisamment long. Ce procédé de chiffrement est-il plus sûr que le chiffrement mono-alphabétique ? Justifiez.
3. **Troisième procédé :** On choisit une correspondance et on chiffre le texte de la manière suivante. On décale la première lettre de 1 puis on appplique la correspondance, on décale la seconde lettre de 2 puis on applique la correspondance,..., on la décale la $k^{\text{ième}}$ de $k \mod 26$ puis on applique la correspondance,...
   (a) Utilisez la correspondance donnée en exemple pour chiffrer le message suivant avec ce procédé : `BONJOUR` ?
   (b) Quelle doit être la longueur minimale du message pour qu'une lettre puisse être codée deux fois de la même façon ?
   (c) Ce procédé est-il plus sûr que le chiffrement mono-alphabétique standard ?