Université de Lille — FACULTÉ DES SCIENCES ET TECHNOLOGIES

L1 - SESI - 2017–2018

Mathématiques Informatique
Arithmétique et Cryptographie

DS1 – 24 mars 2018
Durée 2h

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

Les documents et appareils électroniques (calculatrices, téléphones, ordinateurs portables, etc. . .).

Notez le numéro de votre groupe sur la copie.

Exercice 1 (7 points)

On modifie le chiffrement de César selon le principe suivant.

— On considère l'alphabet "AbCdEfGhIjKlMnOpQrStUvWxYz". Chaque lettre est numérotée par son rang k avec $0 \leq k < n = 26$. On va distinguer les lettres qui ont un rang pair dans l'alphabet (qui seront notées en majuscules) et les lettres de rang impair dans l'alphabet (qui seront notées en minuscules).

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

— On fixe une clé (α, β) formée de deux entiers **pairs** avec $0 \leq \alpha, \beta < n = 26$.
— Si une lettre a un rang pair dans l'alphabet alors elle est chiffrée par un décalage de César de valeur α.
— Si une lettre a un rang impair dans l'alphabet alors elle est chiffrée par un décalage de César de valeur β.

1. Chiffrer le mot `pAnOrAMIx` avec la clé $(\alpha, \beta) = (4, 6)$.
2. Déchiffrer le mot `hEhESxYQ` qui a été chiffré avec cette même clé.
3. Écrire la fonction mathématique $f_{\alpha,\beta}$ qui a un entier k (qui correspond au rang de la lettre du message) associe le rang $f_{\alpha,\beta}(k)$ (qui correspond au rang de la lettre chiffrée). Bien préciser les ensembles de départ et d'arrivée.
4. (a). Montrer que α et β doivent être tous deux pairs ou tous deux impairs. (*Indication.* Que se passerait–il si α et β étaient de parités différentes ?)
   (b). Combien y a –t–il de clés possibles ?
   (c). Quelle est la fonction de déchiffrement ?
   (d). Détailler les attaques possibles pour un espion qui intercepterait un message chiffré sans connaître la clé ?
5. **Bonus.** Décrypter les trois premiers mots de la citation suivante d'Obélix :

```
Cp vIrQA rMtAIp xWnM MAv UQMCz YC Cp vIrQA xWnIpv rMtKM !
```

Exercice 2 (8 points)

On fixe un entier c positif. Pour (a, b) donné (a et b sont des entiers strictement positifs), on souhaite associer un couple d'entiers (x, y) tel que

$$ax - by = c.$$

1. **Question de cours.** Énoncer une condition nécessaire et suffisante afin qu'il existe des solutions $(x, y) \in \mathbb{Z}^2$ à une équation du type $ax - by = c$.
2. **Exemples.**
   (a). Pour $c = 2$ et $(a, b) = (8, 5)$ trouver une solution (x, y).
   (b). Pour $c = 1$ et $(a, b) = (1100, 1029)$ trouver une solution. Détailler les étapes de la résolution.
   (c). Pour $c = 6$ et $(a, b) = (875, 700)$ que se passe-t-il ?
3. **Choix d'une solution.**
   1. Pour la clé $c = 3$ et $(a, b) = (309, 303)$. On admet que $(x_0, y_0) = (152, 155)$ est une solution de $ax - by = c$. En déduire toutes les solutions possibles. Trouver la solution (x_1, y_1) où $x_1 \geq 0$ est le plus petit possible.
   2. Soit $c = 1$ et (a, b) un couple d'entiers strictement positifs. Supposons connue une solution (x_0, y_0) de $ax - by = 1$.
      (a). Écrire la forme générale de toutes les solutions (x, y) en fonction a, b, x_0, y_0.
      (b). Montrer qu'il existe une solution (x_1, y_1) avec $0 < x_1 \leq b$.
      (c). Montrer que cette solution vérifie en plus $0 \leq y_1 \leq a$.
      (d). Cette solution est-elle unique ?

Exercice 3 (5 points)

On considère le principe de chiffrement suivant basé sur le chiffre de Vigenère. La clé secrète est un entier $n \geq 2$. On décompose n en produits de facteurs premiers :

$$n = 2^{\alpha} \cdot 3^{\beta} \cdot 5^{\gamma} \cdots$$

Les exposants $\alpha \geq 0$, $\beta \geq 0$, $\gamma \geq 0$ associés aux nombres premiers 2, 3, 5 peuvent être nuls (par exemple si n est impair, $\alpha = 0$). On ne tient pas compte des autres nombres premiers (représentés par les pointillés $\cdots$).

Un message est chiffré par le chiffre de Vigenère de décalage $[\alpha, \beta, \gamma]$ (pour des blocs de longueur 3, donc).

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

1. (a). Décomposer $n = 19\,400$ en produit de facteurs premiers. *Indication :* diviser par 2 tant que possible, puis par 3, etc...
   (b). Décomposer $n = 40\,950$ en produit de facteurs premiers.
2. Pour la clé $n = 19\,400$ et le mot `MARMITE`, calculer le mot chiffré.
3. Quel mot a été chiffré en `QATBOKEG` par la clé $n = 40\,950$?
4. (a). On se limite ici à la situation $2 \leq n \leq 1000$. Quelle est la valeur maximale de α parmi tous ces n ? Même question pour β, puis pour γ.
   (b). Justifier que les clés n et $7n$ définissent le même décalage.
   (c). Justifier que n et $n + 1$ ne définissent jamais le même décalage.