Université de Lille 1 SCIENCES ET TECHNOLOGIES

L1 - SESI - 2016–2017

Arithmétique et Cryptographie

DS1 – Durée 2h
11 mars 2017

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.

Autour de Vigenère.

On s'interesse dans cet exercice au chiffrement de Vigenère sur l'alphabet à 26 lettres majuscules codées selon le tableau :

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

On suppose définies

- la constante `ALPHABET = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"` ;
- la constante `LEN_ALPHA = len(ALPHABET)`.

1. Quel est l'avantage du chiffrement de Vigenère par rapport au chiffrement par substitution monoalphabétique ?

On considère un chiffrement de Vigenère de clé xyz, x, y et z étant trois lettres de l'alphabet.

2. Quelle est la taille de l'espace des clés ?

3. Chiffrer les six premières lettres de votre nom avec la clé `"QED"`. (si votre nom est trop court, ajoutez les premières lettres de votre prénom).
4. Déchiffrer le message `"TIYEMU"` qui a été chiffré avec la clé `"QED"`.
5. Écrire en PYTHON une fonction prenant en paramètres deux chaînes de caractères : un message `msg` à chiffrer et une clé `cle` et renvoyant le message chiffré.
6. Écrire en PYTHON une fonction `clef_inverse` prenant en entrée une clé sous forme d'une chaine et renvoyant la clé permettant de déchiffrer le message (toujours sous forme de chaine).

Chiffrement affine

Dans cet exercice, on considère la fonction de chiffrement affine f définie par

$$f : \begin{array}{ccc} \mathbb{Z}/26\mathbb{Z} & \longrightarrow & \mathbb{Z}/26\mathbb{Z} \\ x & \longmapsto & ax + b. \end{array}$$

7. Donner une condition sur la clé (a, b) du chiffrement affine pour que ce dernier soit injectif.
8. Chiffrer le mot `"CRYPTO"` avec $(a, b) = (17, 14)$.
9. Lorque la clé (a, b) remplit la condition d'injectivité de f, déterminer la fonction $g : \mathbb{Z}/26\mathbb{Z} \longrightarrow \mathbb{Z}/26\mathbb{Z}$ affine inverse de f, c'est-à-dire telle que :

$$y \equiv f(x) \pmod{26} \Leftrightarrow x \equiv g(y) \pmod{26}.$$

10. Déterminer la fonction g lorsque $(a, b) = (17, 14)$. Puis, déchiffrer le mot `"SQROMOB"`.
11. On suppose que le message `"EZ"` a été chiffré avec une clé (a, b) inconnue et qu'on a obtenu le chiffré `"AB"`. Déterminer la clé utilisée.
12. Est-il possible qu'une clé (a, b) produise comme chiffrement de `"EY"` le résultat `"AB"` ?

Autour de l'algorithme d'Euclide

13. À l'aide de l'algorithme d'Euclide étendu, déterminer le pgcd des nombres a et b ainsi que leur coefficient de Bezout, en détaillant les calculs, lorsque

— $a = 2^{12} - 1$ et $b = 2^8 - 1$;
— $a = 2^{14} - 1$ et $b = 2^{10} - 1$.

Soient m et n deux entiers vérifiant $0 < m \leq n$. On se propose de déterminer le pgcd P de $2^n - 1$ et $2^m - 1$.

Soit r le reste de la division euclidienne de n par m.

14. Démontrer que $2^r - 1$ est le reste de la division euclidienne de $2^n - 1$ par $2^m - 1$.
15. En utilisant l'algorithme d'Euclide, exprimer P en fonction de $d = \text{pgcd}(n, m)$.
16. En déduire que si m et n sont premiers entre eux, alors $2^n - 1$ et $2^m - 1$ sont aussi premiers entre eux.