Département d'informatique **25/02/2020**

Module : Cryptographie

Série 3 (Cryptographie classique)

Exercice 1 : (décalage)

On rappelle qu'on a la numérotation des lettres de l'alphabet suivante :

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. Coder le message « la rencontre est prévue à la cafétéria » à l'aide du chiffrement par décalage et de la clé K = 5.

2. Décoder le message « RGNEIDVGPEWXTRAPHHXFJT » sachant qu'il a été créé par un chiffrement par décalage.

Exercice 2 : (analyse fréquentielle)

L'analyse des fréquences d'apparition des lettres dans un message codé montre que ceux sont les lettres K et O les plus fréquentes dans ce message. Dans un texte en français les lettres les plus fréquentes sont le A (8.4%) et le E (17.26%). Sachant que le message est en français, codé en utilisant le chiffrement par décalage sur les 26 lettres de l'alphabet, déterminer la clef et déchiffrer le début du message :

SVOXFYIKNKXCVKVSQEBSOKMRODOBNOCCYVNKDC

Exercice 3 : (substitution)

1- Coder le message « la rencontre est prévue à la cafétéria » à l'aide du chiffrement parsubstitution et de la clé suivante :

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

2- Est-il possible de décoder le message « YHVMQUVMH » codé par un chiffrement par substitution sans connaître la clé. Décoder ce message sachant qu'il a été créé avec la clé précédente.

Exercice 4 : (Vigenère)

1. Coder le message « la rencontre est prévue à la cafétéria » à l'aide de la méthode deVigenère et du mot clé POULE.
2. Est-il possible de décoder le message « DSJWPHYRSSUHPAJXVQV » codé par un chiffrement de Vigenère sans connaître la clé. Décoder ce message sachant qu'il a été créé à l'aide du mot clé BORDEAUX.

Exercice 5. (affine)

1. On représente l'alphabet latin par les entiers entre 0 et 25 avec la convention A = 0;B =1;C = 2; … ; Z=25

Un chiffrement affine x ➔ ax+b mod 26 transforme le message CRYPTO en le cryptogramme ROXEYZ. Trouver la clé (a; b) correspondante.
2. Le message clair CRYPTO a cette fois été chiffré deux fois de suite par un chiffre affine de clé (a'; b') (c'est-à-dire qu'on a chiffré le chiffré) pour donner en sortie NGBAMX.
(a) Montrer que NGBAMX est le chiffré de CRYPTO par un chiffre affine de clé (a''0; b''):
Trouver (a''; b''):

Exercice 6.(permutation)

1. Définir le chiffrement par permutation.
2. Coder le message "la rencontre est prévue à la cafétéria" à l'aide de cette méthode et de la clé suivante :

$$K = \begin{matrix} 1\ 2\ 3\ 4 \\ 2\ 4\ 1\ 3 \end{matrix}$$

.
3. Décoder le message « MELSEGESEADESCTPTREY » sachant qu'il a été créé avec la clé suivante :

$$K = \begin{matrix} 1\ 2\ 3\ 4\ 5 \\ 3\ 4\ 1\ 5\ 2 \end{matrix}$$

Exercice 7 (Chiffrement de Polybe)

On considère l'alphabet privé de W, soit 25 lettre Polybe (200-125 av J.C). Il a proposé le mécanisme suivant : On range les lettres dans un tableau 5*5, en commençant par le mot clé et on supprimant les doublons, puis on continue avec les lettres restantes de l'alphabet, dans l'ordre. Par exemple avec le mot clé MYSTERE, on construit le tableau suivant :

	1	2	3	4	5
1	M	Y	S	T	E
2	R	A	B	C	D
3	F	G	H	I	J
4	K	L	N	O	P
5	Q	U	V	X	Z

Le chiffrement s'effectue alors en remplaçant la lettre par les deux chiffres :ligne + colonne qui indique sa position dans la grille. Par exemple F est chiffré par 31

1- Expliquez comment on peut cryptanalyser un tel système
2- Raoul a envoyé un message à Anna pour fixer un rendez-vous. Le cryptogramme est le suivant :

123222 512215 424215 512242 242255 534352 111524 225254 322252

512211 525222 532251 142251 154352 21

Décrypter ce message

Exercice 8 : (Chiffrement affine)

Le chiffrement affine consiste à chiffrer toute lettre claire m en une lettre c égale à $c = (am + b) \pmod{26}$;
où a et b sont deux entiers compris entre 0 et 25 fixés. Le couple $(a; b)$ est la clé de chiffrement.
Pour le choix de la clé tous les couples $(a; b)$ ne conviennent pas. Il est nécessaire que a soit inversible modulo 26, ce qui est le cas si a et 26 sont premiers entre eux.
Pour déchiffrer, on calcule la lettre claire m par l'équation $m = a^{-1}(c - b) \pmod{26}$;
où a^{-1} est l'inverse de a modulo 26, c'est à dire l'unique entier x compris entre 0 et 25 tel que $ax \pmod{26} = 1$:

Question 1. Combien y a-t-il de clés ?

Question 2. Le cryptogramme qui suit a été chiffré avec la clé $(a; b) = (11; 17)$.
Déchiffrez-le.
YREHI HRDEJ QJDWJ YRUUI DJENJ
DESVA JYREH IJHOB EFSHB KREHN
QRAJR DTPDR OJNNP WYPEW JTAIR
NRESI JWDCR ENPDS WPAIP EFNPT
TJHBP EIDBR ORBSS BWJYJ HHDHI
JHFJE HYJHN JEYJE SIJSV AJJEL
DJHSB PEHBW WBSJN PESWJ DEOPB
HBEBI IDBWJ AWPNQ JYJIJ CPDHN
DIJWN QRLDJ UPBHL DBIAR HHJLD
JILDD ESPEA IJDWE BNQRW YLDBH
JOJDS TJNQR ES

Question 3. Retrouvez la clé utilisée pour obtenir le cryptogramme ci-dessous.
UJWXN WMJCJ GGPGP MVMPU PCPZS
JWFGP XPUPM GJZJW SGPGR WFUNW
PGVFW PUCRV SPNWA RBRVU PJMCP
XPWSJ WSNWP ZJGRS SPXMA PCVHN
PPWSR NCPPU PUPNY XVWNX RVUPX
JNUPX XNXUN WPMJC SVPZT GVWUC
VHNPU PGRWF NPNCX NMPCV PNCPJ
WMCPX PWSPN WMRVW SUPZR WSJZS
JIPZN WARBR VUPSC VIVJG EUPBR
WSCPC HNPZP MRVWS UPZRW SJZSP
XSNWM RVWSU PCPEC RNXXP BPWS