Travail Expérimental – 2nde	Sciences et investigation policière
MPS	
Séance de Cryptographie numéro 01	

Cryptographie : séance 1

Groupe 4/5/6 : **Mardi 4 octobre**

Quelques sites internet : http://www.bibmath.net/crypto/ & http://matoumatheux.ac-rennes.fr/tous/crypto/accueil.htm

I) Un premier codage

Alice et Bob s'envoient régulièrement des messages qu'ils codent afin de ne pas en révéler la teneur à n'importe qui. Alice utilise le procédé suivant : à chaque lettre de l'alphabet, elle associe son rang dans l'alphabet (ainsi 1 est associé à A, 2 est associé à B, etc…).

1) Compléter le tableau suivant :

Lettres	A	B	C	D	E	F	G	H	I	J	K	L	M
Rang x dans l'alphabet	1	2	3	4	5								

Lettres	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Rang x dans l'alphabet													

2) Coder le mot suivant : CRYPTOGRAPHIE. A quel problème est-on confronté ? Peut-on y remédier ? Est-ce judicieux d'essayer d'y remédier ?

3) Décrypter le message suivant :

10 ' 19131919 520 10 ' 19135 514315185 12519 131208513120917215 19 16152118 51212519 13513519 3151313 14 ' 14135202011420 16119 12 ' 825161531891995 520 125 2217215 , 13519 452124 2520519 4 ' 1225181991514. *192051448112*

4) Des multiples variantes

- On peut aussi permuter deux voyelles, par exemple coder un A comme si c'était un E, etc…
- On peut faire aussi ce qu'on appelle une permutation circulaire par rapport au 1) ; c'est-à-dire 1 est associé à B, 2 est associé à C, …, 26 est associé à A.

J'ai choisi un codage (pas trop compliqué) mais c'est un secret ! Si vous êtes capable de décoder le message suivant, c'est promis je tiendrai ma parole !!!

2215519 15182126 514 161591420 421 1612519 2114 131619 411419 221520186 13152521141421

II) Avec le reste de la division euclidienne par 26

Après avoir fait le codage de l'alphabet du 1), Alice associe ensuite à x un nouveau nombre entier y qui est le reste de la division euclidienne de $3x + 5$ par 26. On a donc $0 \leq y \leq 25$.

1) Compléter le tableau suivant :

Lettres	A	B	C	D	E	F	G	H	I	J	K	L	M
Rang x dans l'alphabet	1	2	3	4	5								
Nombre y associé					20								

Lettres	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Rang x dans l'alphabet													
Nombre y associé													

2) Coder le mot suivant : CRYPTOGRAPHIE.

On constate toujours le même problème que précédemment auquel nous ne remédierons pas afin que le message soit un peu plus dur à décoder.

3) Décrypter le message suivant :

15 ' 2013161720 172010 188133201881364162010 201013 1424181820 1520 21615 , 4166 1424181820211420 2021 182417201013620 2013 23621613 2021 188021623614202114 20

14387152010 148152011 142415132421

III) Et un codage de plus…

Il est préférable de coder des lettres par des lettres, donc aux deux codages ci-dessus, Alice va en rajouter un dernier qui associe de nouveau au nombre *y* la lettre qui lui correspond dans l'alphabet (à zéro elle associera la lettre Z, à 1 la lettre A, à 2 la lettre B … et à 25 la lettre Y).

1) Compléter le tableau suivant :

Lettres	A	B	C	D	E	F	G	H	I	J	K	L	M
Rang x dans l'alphabet	1	2	3	4	5								
Nombre y associé					20								
Lettre de l'alphabet					T								

Lettres	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Rang x dans l'alphabet													
Nombre y associé													
Lettre de l'alphabet													

2) Coder le mot suivant : CRYPTOGRAPHIE.

3) Décrypter le message suivant :

OTJ NCHPJJPGTJ JXUM PU FUJMGPRTUM AXPG RHGNCTG . OTJ RHMCTRHMFDPT JXUM PU FUJMGPRTUM AXPG ATUJTG. XU ATPM RHGNCTG JHUJ NCHPJJPGTJ RHFJ XU SH RXFUJ OXFU .

ITHU-RHGFT JXPGFHU

IV) Pour la prochaine séance : lundi 7 novembre

- Finir cette feuille si cela n'a pas été le cas aujourd'hui.
- Chercher par trinôme (et proposer) une méthode de codage que vous présenterez le lundi 7 novembre. Je souhaite que vous m'adressiez par mail votre document (un seul par trinôme) ou que vous me le posiez dans mon casier au plus tard le vendredi 4 novembre à 12 h. (vincent.obaton@ac-grenoblefr) Attention le codage doit être sérieux. Aidez vous des adresse du début du document.

Et bonnes vacances les experts ..... !!!