Codes et cryptographie

L'objectif d'un code est de pouvoir transmettre des informations qu'une tierce personne qui les intercepteraient ne pourra pas comprendre... ou qui aurait tellement de difficulté à les interpréter que lorsqu'il aurait trouvé la clef du code, l'événement en question aura déjà eu lieu.

INTRODUCTION

Nous allons étudier 4 sortes de codage différents : le code morse, le code braille, le code César et le code Vigenere.

LE CODE MORSE

Le code morse est un code permettant de transmettre un texte à l'aide de séries d'impulsions courtes et longues, qu'elles soient produites par des signes, une lumière ou un geste.

Inventé en 1832 pour la télégraphie, ce codage de caractères assigne à chaque lettre, chiffre et signe de ponctuation une combinaison unique de signaux intermittents. On marque un temps de pause entre chaque lettre (à l'écrit on place un caractère slash « / ») et un double temps de pause entre chaque mot (à l'écrit, un double slash « // »). Le code morse est considéré comme le précurseur des communications numériques.

Aujourd'hui, le morse est principalement utilisé par les militaires comme moyen de transmission ou dans le civil pour certaines émissions. Le morse est également pratiqué par des radioamateurs, scouts (morse sonore et lumineux), plongeurs ou alpinistes (morse lumineux) ainsi que comme sonnerie par défaut de réception de message pour les gsm de marque Nokia ("SMS SMS" en morse)

Lettre	Code	Mnémotechnique	Lettre	Code	Mnémotechnique
A	. _	Allo	**N**	_ .	Noël
B	_ . . .	Bonaparte	**O**	_ _ _	Oporto
C	_ . _ .	Coca-cola	**P**	. _ _ .	Philosophe
D	_ . .	Docile	**Q**	_ _ . _	Quocorico
E	.	Et	**R**	. _ .	Ramoneur
F	. . _ .	Farandole	**S**	. . .	Sardine
G	_ _ .	Gondole	**T**	_	Thon
H	. . . .	Hilarité	**U**	. . _	Union
I	. .	Ici	**V**	. . . _	Valparaiso
J	. _ _ _	Jablonovo (Jupon nouvo)	**W**	. _ _	Wagon-post
K	_ . _	Kohinor	**X**	_ . . _	Xocadéro ([e]xonération)
L	. _ . .	Limonade	**Y**	_ . _ _	Yoshimoto
M	_ _	Moto	**Z**	_ _ . .	Zoroastre

Chiffre	Code	Chiffre	Code
0	_ _ _ _ _	**5**	. . . . .
1	. _ _ _ _	**6**	_ . . . .
2	. . _ _ _	**7**	_ _ . . .
3	. . . _ _	**8**	_ _ _ . .
4	. . . . _	**9**	_ _ _ _ .

1. Questions

Traduisez en morse les textes suivants :

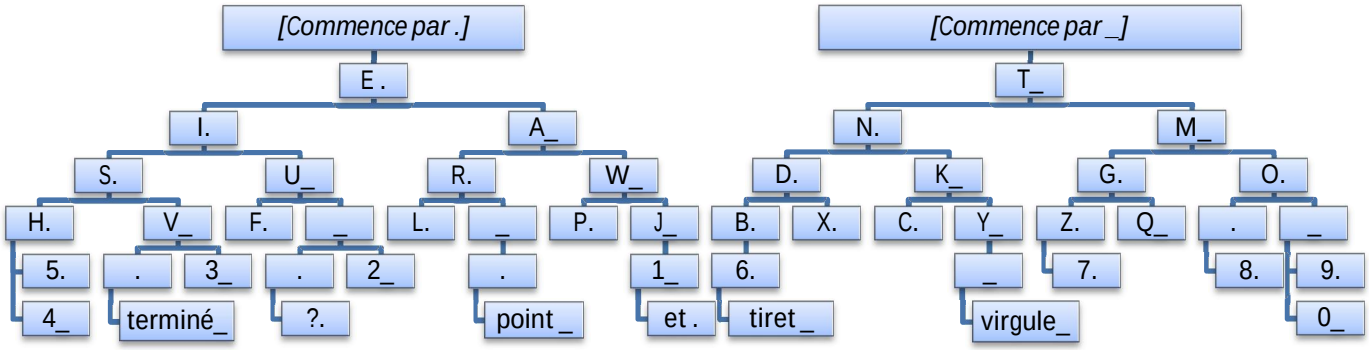
- SOS :
- ATTAQUER DEMAIN :
- LES SANGLOTS LONGS DES VIOLONS DE L'AUTOMNE :

Décodez le texte suivant :

. - . . / . / / . - - . / . / . - . / . - . / - - - / - - . - / . . - / . / - /
/ . / . . . / - / / . . - / - . / / . - . . / . / . . - / . - . / . - . / . /

Astuces : Autres façons d'écrire le morse

1. Au lieu d'écrire des points et des tirets, on peut dessiner une ligne avec des pics : soit que les petits pics sont les points et les grands pics les tirets, ou encore, les pics vers le haut sont les points, et les pics vers le bas sont les tirets (ou vice-versa).
2. Les points sont représentés par des traits horizontaux et les tirets par des traits verticaux ou obliques. On peut donner une forme cunéiforme aux traits pour imiter un texte assyrien.
3. On peut aussi utiliser une corde. Un nœud simple représente un point, et un nœud en huit représente un tiret. On laisse un plus grand espace entre les mots.
4. Représenter les points par une lettre et les tirets par une autre (par exemple, respectivement P et Z). Le mot "allez" deviendrait ainsi : PZ PZPP PZPP P ZZPP
5. Représenter les points par une voyelle quelconque et les tirets par une consonne quelconque. Le mot "allez" pourrait devenir ainsi : EL IKOA UZAI O BLEI
6. On peut s'aider du graphique suivant pour apprendre et utiliser le code morse :



LE CODE CESAR

Il s'agit de l'un des codes les plus anciens, il est très facile à mettre en œuvre et à programmer (Sur calculatrice programmable par exemple). Dans ce code, on ne considère que les lettres, sans accents. L'alphabet est simplement décalé d'un certain nombre appelé "décalage" et noté D_{code} dans les programmes. Originellement, Jules César aurait utilisé une valeur de décalage de 4. On revient au début quand on arrive à Z. Pour le décodage, on applique l'opération inverse, on l'on recode le message codé avec un décalage $D_{décode} = 26 - D_{code}$.

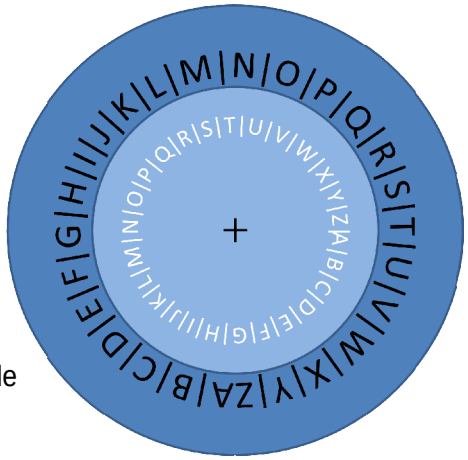
2. Questions

Complétez le tableau suivant avec un décalage de 4.

Original	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
Codé																										

Décodez les phrases suivantes, le décalage étant de 4 :

- `GIXXI STXMSR QTW IWX TEWWMSRRERXI`



Astuce : des disques de codage / décodage rapide

Il est possible de coder/décoder de tels messages rapidement. Il suffit de réaliser deux disques représentant chacun l'alphabet, dont l'un a un diamètre légèrement plus petit. Ces deux disques vont vous aider à chercher des codes de décalages inconnus : pour déchiffrer un code César, il suffit de tester les 25 décalages possibles.

VARIANTE DU CODE CESAR : PERMUTATION

Pour déchiffrer un code César, il suffit de tester les 25 décalages possibles, ce qui est très rapide à la main et instantané à l'aide d'un programme informatique. Nous allons voir un code plus compliqué que celui de César. Là aussi on ne code que les lettres majuscules, sans accent, mais chaque lettre de l'alphabet est remplacée par une autre. On ne se contente donc pas de faire un décalage de l'alphabet, mais on mélange les lettres de l'alphabet et on applique cette « clef » pour coder le message.

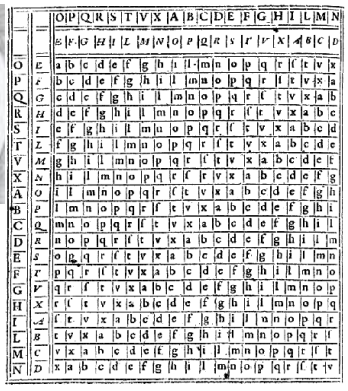
Il y a donc un très grand nombre de codes possibles (26x25x24x....x2x1=26!=403291461126605635584000000). Si le message est très court (Par exemple: "ON VIENT DEMAIN"), le décodage est quasi impossible. Par contre, dans le cas contraire, on peut avoir une idée de la clef de codage en analysant les fréquences des lettres du message codé.

Exemple :

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

L'observation du message à déchiffrer est importante; il faut savoir reconnaître les petits signes qui donnent des indices sur le genre de code à trouver. Par exemple, dans un code ne comportant que des lettres (pas de chiffre), étudiez les fréquences en notant la lettre qui se répète le plus souvent : dans la langue française, les lettres les plus utilisées sont, dans l'ordre décroissant: E S A N I T R U. Il est également possible de rechercher des petits mots courants tels que de, la, le, les, et, à, l', un, ...

CHIFFRE DE VIGENERE



Dans ce système de codage, on choisi un mot « clef » qui va servir à coder le message. On calcule le décalage à partir de cette clé et on le reporte à la lettre non-codé correspondante. Il est nommé ainsi au XIXe siècle en référence au diplomate du XVIe siècle Blaise de Vigenère, qui le décrit (intégré à un chiffrement plus complexe) dans son traité des chiffres paru en 1586.

Exemple :

On désire coder la séquence « ATTAQUER DEMAIN », avec la clef convenu d'avance « GOLF ».

Lettre	A	T	T	A	Q	U	E	R		D	E	M	A	I	N
Clef	G	O	L	F	G	O	L	F	G	O	L	F	G	O	L
Décalage	6	14	11	5	6	14	11	5	6	14	11	5	6	14	11
Codage	G	H	E	F	W	I	P	W		R	P	R	G	W	Y

- La clef est répétée autant de foi que nécessaire sous le message. On applique ensuite un simple décalage « de César » en fonction de la lettre de la clef.
- La première lettre "A" doit être codée avec "G". On lui applique un décalage de 6, ce qui donne "G". La deuxième lettre "T" doit être codée avec "O". On lui applique un décalage de 14, ce qui donne "H". La troisième lettre "T" doit être codée avec "L". On lui applique un décalage de 11, ce qui donne "E".
- Le message codé est donc : « GHEFWIPW RPRGWY »
- On constate qu'une même lettre peut être codée de plusieurs façons, ce qui rend inefficace l'analyse des fréquences pour décrypter!

Pour coder-décoder, on peut utiliser un carré de Vigenère :

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

Utilisation : La lettre « T » (colonne) est codée par « E » lorsque la lettre de la clef est « L » (ligne).

3. Questions

Codez le message **:** « NOUS MANQUONS DE MUNITIONS », avec la clef « CLEF »
Pour cela, remplissez le tableau suivant :

Lettre	N	O	U	S		M	A	N	Q	U	O	N	S		D	E		M	U	N	I	T	I	O	N	S
Clef	C	L	E	F	C	L	E	F	C	L	E	F	C	L	E	F	C	L	E	F	C	L	E	F	C	L
Décalage	2	11	4	5	2	11	4	5	2	11	4	5	2	11	4	5	2	11	4	5	2	11	4	5	2	11
Codage																										

4. Décoder le message "DTFPTR HDME P EUCMUI SG ESDR"

Pour cela, remplissez le tableau suivant. La clef de codage est "MPS"

Lettre																													
Clef																													
Décalage																													
Codage	D	T	F	P	T	R		H	D	M	E		P		E	U	C	M	U	I		S	G		E	S	D	R	D

Le chiffre de Vigenère a été cassé par le major prussien Friedrich Kasiski qui a publié sa méthode en 1863. Il n'offre plus depuis cette époque aucune sécurité.

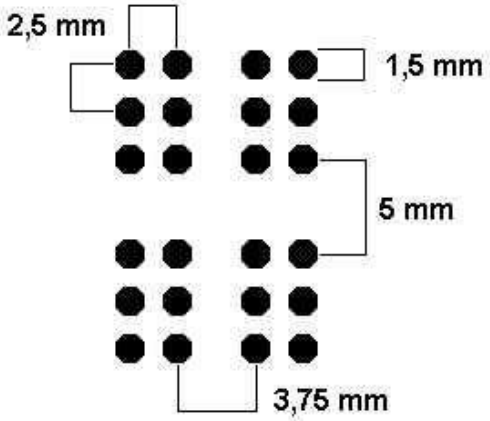
LE CODE BRAILLE

Le braille est un système d'écriture tactile à points saillants, à l'usage des personnes aveugles ou fortement malvoyantes. Le système porte le nom de son inventeur, le Français Louis Braille (1809-1852) qui avait perdu la vue à la suite d'un accident. Élève à l'Institution royale des jeunes aveugles, il modifie et perfectionne le code Barbier. En 1829 paraît le premier exposé de sa méthode.

1	4
2	5
3	6

En braille standard, un caractère est représenté dans une matrice de six points sur deux colonnes, chaque caractère étant formé par un à six points en relief. Ces points sont conventionnellement numérotés de haut en bas et de gauche à droite, voici un extrait de quelques signes d'usage courant :

Code	Lettre	Code	Lettre	Code	Lettre
⠁	A 1	⠝	N	⠠	Capitale
⠃	B 2	⠕	O	⠼	Chiffre
⠉	C 3	⠏	P	⠲	Point
⠙	D 4	⠟	Q	⠂	Virgule
⠑	E 5	⠗	R	⠦	Point d'interrogation
⠋	F 6	⠎	S	⠱	deux-points
⠛	G 7	⠞	T	⠖	Point d'exclamation
⠓	H 8	⠥	U	⠶	Guillemet ouvrante
⠊	I 9	⠧	V	⠷	Guillemet fermante
⠚	J 0	⠺	W	⠐	Crochet
⠅	K	⠭	X	⠤	Tiret
⠇	L	⠽	Y		
⠍	M	⠵	Z		



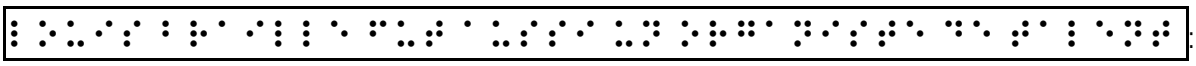
5. Questions

Convertir en braille :

- Mettre les petits plats dans les grands.

M	e	t	t	r	e		l	e	s		p	e	t	i	t	s		p	l	a
t	s		d	a	n	s		l	e	s		g	r	a	n	d	s	.		

- Traduire le code Braille suivant :



.....

.....

.....

Question bonus :

Comment s'appelle cet appareil, et quel est son utilité ?

Comment contourner la protection très facilement par une méthode que n'avait pas prévue son inventeur ?