Enigme : la cryptographie

Comprendre ce qu'est la cryptographie

Extrait du livret :

« La **cryptographie** est une des disciplines de la cryptologie s'attachant à **protéger des messages** (assurant confidentialité, authenticité et intégrité) en s'aidant souvent de *secrets* ou *clés*. Elle se distingue de la stéganographie qui fait passer inaperçu un message dans un autre message alors que la cryptographie rend un **message inintelligible** à autre que qui-de-droit. »

Focus sur le chiffre de Vigenère

Extrait du livret :

« Le **chiffre de Vigenère** est un système de chiffrement par substitution, où une même lettre du message à transmettre (**message clair**) peut, suivant sa position dans celui-ci, être remplacé par des lettres différentes dans le **message chiffré**.

[…]

Le **chiffrement à clé** utilise une chaine de chiffres ou de caractères (**la clé**) pour indiquer par quelle lettre doit être substitué chaque lettre du message en clair. Dans les méthodes modernes, la clé est alphanumérique, unique et aléatoire.

Dans le **chiffre de Vigenère**, la clé est un mot qui est répété plusieurs fois (ce qui est sa faiblesse et a permis d'en produire une méthode de décodage). A chaque lettre du message clair correspond alors une lettre de la clé, qui définit la substitution. Le codage se fait alors à partir d'**une table** indiquant, dans un tableau croisé, la lettre qui servira à coder. »

	Lettre en clair																									
	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**
Lettre de la clé	Lettres chiffrées (au croisement de la colonne *Lettre en clair* et de la ligne *Lettre de la clé*)																									
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

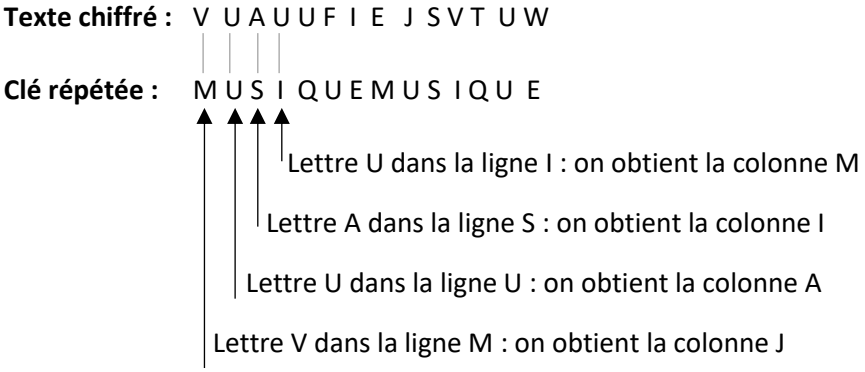
Principe de l'énigme :

Pour cette énigme, nous avons choisi une méthode de cryptographie en particulier, celle évoquée ci-dessus : le chiffre de Vigenère. Il s'agit d'une méthode symétrique, ce qui n'est plus guère utilisé aujourd'hui mais qui a le mérite d'introduire de façon claire le concept de clé en cryptographie et qui se prête bien à la résolution d'une énigme où plusieurs morceaux sont à réunir.

Le participant doit en effet trouver le message à déchiffrer, la clé de déchiffrement, la table de Vigenère et l'exemple ci-dessous qui permet de comprendre le fonctionnement de la table et donc la méthode de déchiffrement :

Le chiffre de Vigenère : exemple de déchiffrement

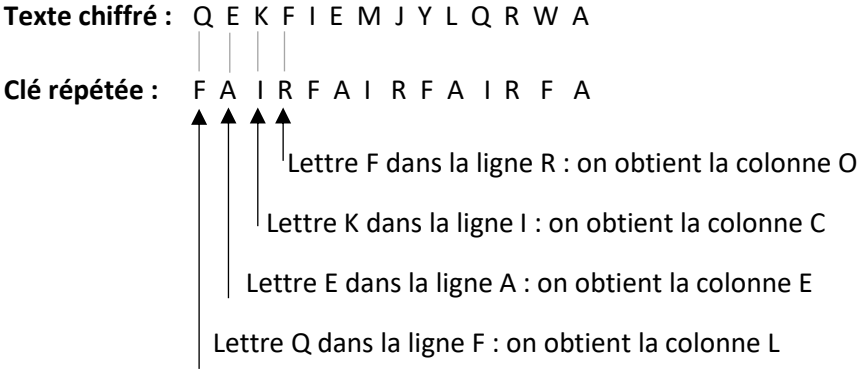
Avec la **clé** « **musique** », on doit **déchiffrer VUAUUFIEJSVTUW** :



Le **message en clair obtenu** par **déchiffrement** est alors : « **j'aime les pandas** »

L'exemple ci-dessus s'appuie sur la table de Vigenère fournie à la page précédente. Pour déchiffrer un message, il faut donc d'abord répéter la clé en-dessous du message autant de fois que nécéssaire pour que chaque lettre du message soit associée à une lettre de la clé. Une fois cela fait, il faut chercher dans la table, la ligne correspondant à la lettre de la clé associée à la lettre à déchiffrer. La première lettre à déchiffrer est la lettre V et elle est associée à la lettre M de la clé. Nous nous plaçons donc dans la ligne M de la table. Dans cette ligne, il faut maintenant chercher la lettre à déchiffrer, c'est-à-dire la lettre V. Une fois cette lettre V trouvée dans la ligne M, il faut remonter dans la table pour lire l'en-tête de la colonne concernée, il s'agit ici de J. La première lettre déchiffrée est donc J. Il faut ensuite répéter ce manège pour toutes les lettres restantes du message avec leurs lettres associées respectives. Le message obtenu est JAIMELESPANDAS soit « j'aime les pandas » si on ajoute de la ponctuation et des espaces.

Pour notre énigme, le message à déchiffrer est QEKFIEMJYLQRWA et la clé est FAIR. En faisant comme dans l'exemple, nous trouvons donc :



Texte chiffré : Q E K F I E M J Y L Q R W A

Clé répétée : F A I R F A I R F A I R F A

Texte déchiffré : L E C O D E E S T L I A R A

En ajoutant ponctuation et espaces, on obtient donc le message : « le code est Liara ». « Liara » est donc le mot à cinq lettres permettant d'ouvrir le Cryptex[1] qui contient le message disant que la porte est déverrouillée. (Il s'agit du deuxième prénom de la chercheuse mais ce n'est mentionné nulle part).

Le participant découvre ici une méthode particulière de cryptographie qui lui permet de comprendre l'utilité de la cryptographie et le concept de clé en cryptographie.

Réaliser l'énigme de la cryptographie :

Matériel :

-papier pour imprimante

-1 stylo

-1 couleur de gommettes à choisir pour cette énigme

3 éléments à préparer :

1 : la table de Vigenère

Imprimez la première page du document cryptographie_impression.pdf, découpez et plastifiez puis redécoupez à 5mm du bord du papier.

(Emplacement : Table centrale, dans pochette sur chaise)

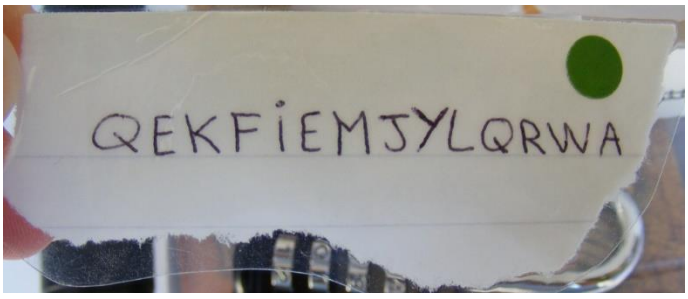
2 : l'exemple de déchiffrement

Imprimez la deuxième page du document cryptographie_impression.pdf, découpez et plastifiez puis redécoupez à 5mm du bord du papier.

(Emplacement : Table centrale, Manteau sur dossier de chaise, poche droite 2)

3 : le message chiffré

Sur un morceau de papier quelconque (feuille blanche, morceau déchiré du carnet de la chercheuse…), écrivez comme ci-contre : Q E K F I E M J Y L Q R W A



[1] Cryptex est un néologisme utilisé par Dan Brown dans son roman *Da Vinci Code* pour désigner une sorte de coffre-fort portable conçu pour cacher des messages secrets. *(Wikipédia)*

Déchirez le papier autour de l'écriture, plastifiez et redécoupez à 5mm du bord du papier.

(Emplacement : Table centrale, collé à la Patafix au fond de la boîte 2)

Gommettes :

Une fois votre couleur (et forme si besoin) choisie pour cette énigme, mettez une gommette sur :

-la table de Vigenère

-l'exemple de déchiffrement

-le message chiffré

-l'espace prévu dans l'écriture à l'encre invisible dans le coin supérieur droit de la fiche Platine (première fiche du paquet de trente fiches pour l'énigme des bases de données), au besoin, voir l'emplacement de la gommette verte sur la dernière page du document base_de_donnees_UV.pdf

-le cryptex que le code (LIARA) permet d'ouvrir (ce cryptex renferme le message « La porte est déverrouillée » (Emplacement : Bureau 2, sur le foulard/écharpe/bonnet))

-l'étiquette qui indique le nombre d'indice pour cette énigme (voir déroulement_nb_indice.pdf)

-l'emplacement réservé à cette énigme sur le schéma de déroulement (pareil)