



Codes Secrets

La cryptographie est la science des messages secrets. En voici quelques exemples.

1) Le code César

Jules César utilisait le système le plus simple, celui des alphabets décalés d'un ou plusieurs crans (où l'on remplace, par exemple A par B, B par C, etc.). En vous servant des “disques César” fournis saurez-vous décoder le message suivant ?

ZPYTM RS CQ SL CQNGML

2) On peut employer des méthodes plus sophistiquées. Par exemple permuter les lettres selon une règle simple. Un espion envoie le message

À L'AIDE

sous la forme

Z M'ZRWV

Saurez-vous trouvez la règle qu'il a utilisée ?

A vous de lui répondre

J'ARRIVE



Codes Secrets

La cryptographie est la science des messages secrets. En voici quelques exemples.

1) Le code César

Jules César utilisait le système le plus simple, celui des alphabets décalés d'un ou plusieurs crans (où l'on remplace, par exemple A par B, B par C, etc.). En vous servant des “disques César” fournis saurez-vous décoder le message suivant ?

ZPYTM RS CQ SL CQNGML

2) On peut employer des méthodes plus sophistiquées. Par exemple permuter les lettres selon une règle simple. Un espion envoie le message

À L'AIDE

sous la forme

Z M'ZRWW

Saurez-vous trouvez la règle qu'il a utilisée ?

A vous de lui répondre

J'ARRIVE



Codes Secrets

3) Ces méthodes ont un défaut : il suffit d'identifier les lettres qui apparaissent le plus. Par cette méthode, pouvez-vous traduire le message suivant ?

**SALCF CFVH LCNE ANVHHP L GNZIPUANA KN RNHHLBN
CFVH NYOANE GLYH KN ZKVS OANH UNARN GNH ZLHHNVAH
GN ZFGNH HNZANOH UALYZLPH KNH NHMPFYH Y'FYO MKVH
TV'L SPNY HN ONYPA UNKPZPOLOPFYH**

en sachant qu'en français, les lettres les plus fréquentes sont, dans l'ordre, E, puis S et A, puis R, I, N et T, puis U, puis O et L, etc et que dans le message ci-dessus les lettres qui apparaissent le plus souvent sont A (11 fois), F (7 fois), H (22 fois), L (10 fois), N (25 fois), O (7 fois), P (9 fois), V (7 fois) et Y (8 fois).

Indication : commencer par identifier les mots

ANVHHP

KNH

NHMPFYH

SPNY

ONYPA.

C'est après que l'un de ses messages a été décodé de cette manière que Marie Stuart fut condamnée à mort.



Codes Secrets

La cryptographie est la science des messages secrets. En voici quelques exemples.

1) Le code César

Jules César utilisait le système le plus simple, celui des alphabets décalés d'un ou plusieurs crans (où l'on remplace, par exemple A par B, B par C, etc.). En vous servant des “disques César” fournis saurez-vous décoder le message suivant ?

ZPYTM RS CQ SL CQNGML

2) On peut employer des méthodes plus sophistiquées. Par exemple permuter les lettres selon une règle simple. Un espion envoie le message

À L'AIDE

sous la forme

Z M'ZRWW

Saurez-vous trouvez la règle qu'il a utilisée ?

A vous de lui répondre

J'ARRIVE



Codes Secrets

3) Ces méthodes ont un défaut : il suffit d'identifier les lettres qui apparaissent le plus. Par cette méthode, pouvez-vous traduire le message suivant ?

**SALCF CFVH LCNE ANVHHP L GNZIPUANA KN RNHHLBN
CFVH NYOANE GLYH KN ZKVS OANH UNARN GNH ZLHHNVAH
GN ZFGNH HNZANOH UALYZLPH KNH NHMPFYH Y'FYO MKVH
TV'L SPNY HN ONYPA UNKPZPOLOPFYH**

en sachant qu'en français, les lettres les plus fréquentes sont, dans l'ordre, E, puis S et A, puis R, I, N et T, puis U, puis O et L, etc et que dans le message ci-dessus les lettres qui apparaissent le plus souvent sont A (11 fois), F (7 fois), H (22 fois), L (10 fois), N (25 fois), O (7 fois), P (9 fois), V (7 fois) et Y (8 fois).

Indication : commencer par identifier les mots

ANVHHP

KNH

NHMPFYH

SPNY

ONYPA.

C'est après que l'un de ses messages a été décodé de cette manière que Marie Stuart fut condamnée à mort.



Codes Secrets

4) Pouvez-vous deviner la méthode de codage utilisée pour le message précédent ?

5) Le code Gödel

De nos jours les codes secrets sont partout sur internet et les méthodes plus sophistiquées utilisent des propriétés fines des nombres premiers. Voici un exemple, peu utile en pratique mais amusant, de code utilisant les nombres premiers ; il a été inventé par le grand logicien Kurt Gödel.

À chaque lettre on associe son rang dans l'ordre alphabétique : ainsi, on associe 1 à A, 2 à B, 3 à C, etc.

La n-ième lettre du texte à coder est ensuite remplacée par le n-ième nombre premier élevé à la puissance qui correspond à la lettre.

Par exemple, si la première lettre du message est B, ce B sera codé $2^2 = 4$.

Si la deuxième lettre est A, cette lettre sera codée par $3^1 = 3$, etc.

Le message lui-même sera codé par le produit des codages de ses lettres. Ainsi le mot BA est codé par le nombre 12 ($= 2^2 \cdot 3^1$).

À vous de décoder le message suivant (constitué d'un seul nombre) :

5 804 752 896