

Exercice 01 : Le Chiffrement de Jules César

Le système le plus ancien est attribué à Jules César. Il consiste en un décalage de l'alphabet (dans le système original A était remplacé par C, B par D, C par E,).

Le texte ci-dessous a été chiffré avec la clé **R** :

TV KVOKV R VKV TYZWWIV RMVT AR TAV H

- Retrouvez le texte clair.

Exercice 02 : Le Chiffrement de Vigenère

Ce cryptogramme a été obtenu par chiffrement de vigenère avec le mot-clé « **RAYMOND** »

RILEW FRETJ QGZRV UPERR VDAJQ GRWUE QRSZH CLCER NQJLC DSTQV ALUAN OUEDM
QBQGR MHWQH ETGQZ YH.

Retrouvez le texte clair.

Exercice 03 : Le Chiffrement par transposition (1)

Rappel : Le chiffrement par transposition est une technique où les caractères d'un message sont simplement réordonnés dans un ordre différent de l'original.

Utiliser la permutation **24531** (le caractère 2 prend la position 1, 4 la position 2) pour chiffrer le message suivant :

MANOS ARRIBA ESTO ES UN ATRACO

Exercice 04 : Le Chiffrement par transposition (2)

Voici un autre procédé de chiffrement par transposition ou permutation :

- La clé est une suite de lettres, mot ou phrase, comme par exemple « **PHRASE** ». Chacune des lettres de la clé est numérotée, à partir de A, et suivant l'ordre alphabétique. Si la clé était « **PHRASE** », cela donne :

Colonne littérale : P H R A S E

Ordre numérique : 6 3 4 1 5 2

- Lors de chiffrement, le texte clair est écrit sur des lignes de même longueur que la clé, ces lignes étant disposées l'une au-dessus de l'autre pour former un rectangle.
- On relève ensuite les colonnes dans l'ordre déterminé par les nombres associés aux lettres de la clé.

1. Le cryptogramme suivant :

USTS INEUU TTHSE RSNTE NSEECEN EEIUEGTI ESEH NIUTO SMPRU DE UVEETDI
NRDERC ITN INEEE SDER.

A été construit suivant ce procédé avec le mot-clé « **NGDCKW** ». Retrouver le texte clair.

2. Que pourrait-on faire si on ne disposait pas de la clé, mais seulement de sa longueur ? et si on ne savait rien de la clé ?