**Cryptographie : TD2\_1&2 Chiffrement de Vigenère 22/02/2019**

1. **Expliquer le principe de la substitution poly-alphabétique.**
2. **Expliquer rigoureusement le principe du chiffrement de Vigenère**
3. **Utiliser le chiffrement de Vigenère avec la clé « IVRY », pour chiffrer le message suivant : « CRYPTOGRAPHIE SYMETRIQUE »**
4. **Le chiffrement de Vigenère a été utilisé pour chiffrer un message avec la clé « ESIEA ». Le chiffré obtenu est la suivant : « XZMSRMWLISRGUFRIK ». Déchiffrer ce message et retrouver le message initialement caché.**
5. **Voici un message clair et chiffré correspondant. Retrouver la clé utilisée lors du chiffrement.**

**Texte clair : ROLEDESALGORITHMESENINFORMATIQUE**

**Texte chiffré : CGRTVKHSRVGXXLNBWYTFOCXUGEGIAWJW**

1. Dans un procédé de substitution poly-alphabétique, une même lettre du texte original, peut suivant son emplacement dans celui-ci, être remplacé par des lettres différentes dans le texte chiffré correspondant
2. L’idée de Vigenère est d’utiliser un chiffre de César mais avec un décalage variable. Vigenère utilise une clé k, composée de L lettres, représentant chacune la valeur du décalage. A=0, B=1... Un message clair de longueur n est tout simplement découpé en bloc de L caractères ou chaque bloc est ainsi chiffrée avec la même clé k.

Le chiffrement d’un bloc est le suivant :

* La première lettre du bloc est chiffrée avec la première lettre de la clé
* La deuxième lettre du même bloc est chiffrée avec la deuxième lettre de la clé etc. Jusqu’à épuisement du bloc.
* Cette manœuvre est ainsi réitéré pour chaque bloc jusqu’à la fin du message.

1. Chiffrement de Vigenère avec ka clé « IVRY » : CRYPTOGRAPHIE SYMETRIQUE

L12 R18 Q17 O15 M13 K11 Y25 Q17 J10 L12 Z26 L12N14 O15 Q17 L12 N14 P16 J10 H8 Z26 Q17 W23

LRQOMNKYQJLZLN OQLNPJHZQW erreur

KMPNBJXPIKYGMNPKMOIGYPV

Correspondance des nombres :

**A0**

B1

C2

D3

**E4**

F5

G6

H7

**I8**

J9

K10

L11

M12

N13

O14

P15

Q16

R17

**S18**

T19

U20

V21

W22

X23

Y24

Z25

1. Déchiffrer le message : X Z M S R M W L I S R G U F R I K avec la clé « ESIEA »

THEORIEDESNOMBRES

1. Retrouver la clé :

PSG

1. La force du chiffre de Vigenère, est que la même lettre dans le texte clair sera chiffrée différemment selon sa position. Ce qui permet de brouiller la cryptanalyse par analyse de fréquence
2. Supposons que la clé est de longueur L, on peut alors découper le message chiffré en L morceaux. Chacun des messages est un chiffré par décalage et le décalage peut être retrouvé par analyse de fréquence. Ainsi, en appliquant le décalage dans le sens inverse, on peut retrouver les caractères du texte clair pour chaque morceau.