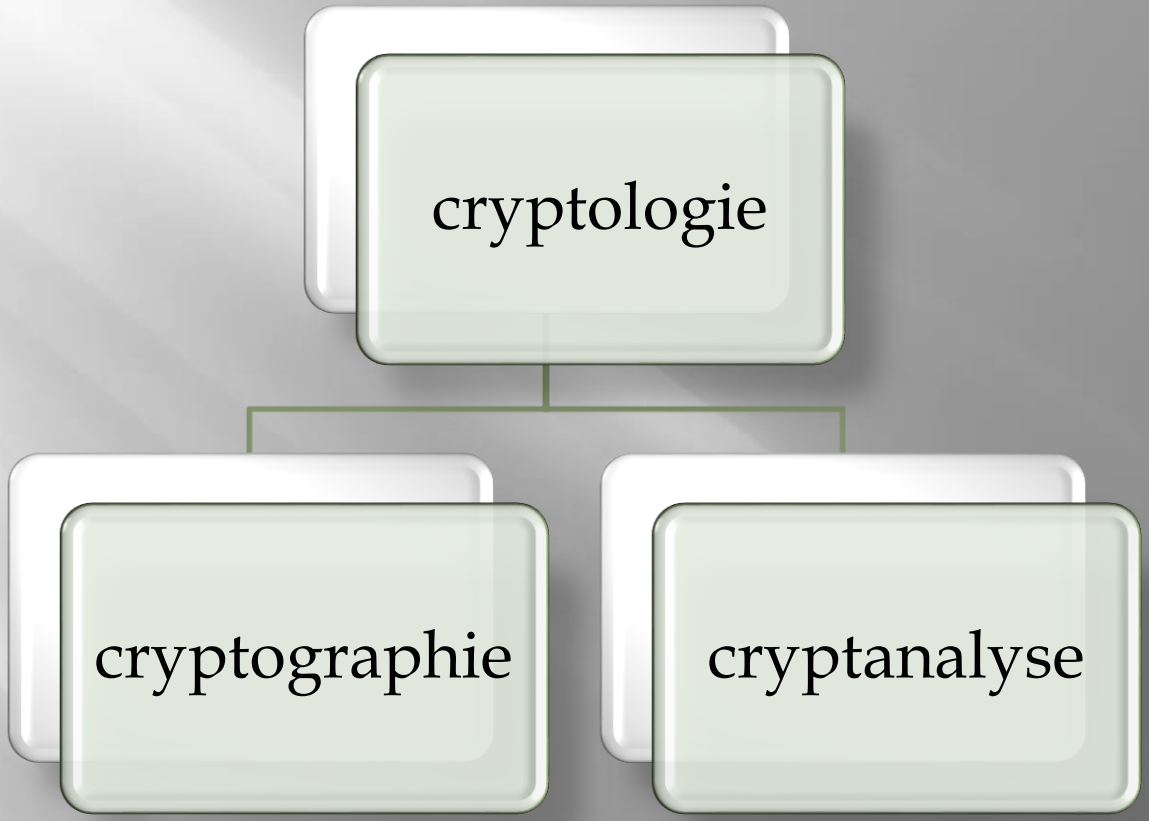
SÉCURITÉ ET CRYPTOGRAPHIE


cryptologie
cryptographie
cryptanalyse

- **Cryptographie :** l'étude des méthodes donnant la possibilité d'envoyer des données de manière confidentielle sur un support donné.

- **Cryptanalyse :** Opposée à la cryptographie, elle a pour but de retrouver le texte clair à partir de textes chiffrés en déterminant les failles des algorithmes utilisés.

En grec :

Cryptographie : (κρυπτο . γραf ην)

écriture cachée / brouillée.

Chiffrement / déchiffrement

- **Chiffrement : transformer à l'aide d'une convention secrète, appelée clé, des informations claires (plaintext) en informations incompréhensibles (ciphertext) pour des tiers n'ayant pas la connaissance du secret.**

- **Déchiffrement : retrouver les informations claires, à partir des informations chiffrées en utilisant la convention secrète de chiffrement.**

- **Décryptage : retrouver l'information intelligible, à partir de l'information chiffrée sans utiliser la convention secrète de chiffrement.**

- **Texte chiffré :** Appelé également cryptogramme (ciphertext), le texte chiffré est le résultat de l'application d'un chiffrement à un texte clair.

  - Il doit être uniquement déchiffré par le destinataire légitime. Un cryptosystème est caractérisé par cinq composants :

– Un espace **M = {M1, M2, …} des messages en clair;**

– Un espace **C = {C1, C2, …} des messages chiffrés;**

– Un espace **K = {K1, K2, …} des clés;**

– Un algorithme de chiffrement paramétré par une clé K

$$E_k : M \longrightarrow C$$
$$m \longrightarrow c = E_k(m)$$

– Un algorithme de déchiffrement paramétré par une clé K'

$$D_{k'} : C \longrightarrow M$$
$$c \longrightarrow m = D_{k'}(c) = D_{k'}(E_k(m))$$

I- Cryptographie classique

➔ Chiffrement par transposition
➔ Chiffrement par substitution

- **Au début, il y eut le texte…**

- l'utilisation **d'alphabet** a permis de **coder** chaque mot du langage à partir des mêmes symboles,

- L'ajout d'un ordre sur ces lettres à permis de définir les premières méthodes «*mathématiques* » de chiffrement ,

- Ces chiffrements partent d'un message contenant des **lettres** vers un cryptogramme contenant également des **lettres**.

Chiffrement par substitution

- substituer un caractère ou un groupe de caractères par un autre dans le texte à chiffrer.

- Plusieurs types de **cryptosystèmes par substitution :**

  - **monoalphabétique**

  - **homophonique**

  - **polyalphabétique**

  - **polygrammes**

Chiffrement de César
(Chiffrement par substitution monoalphabétique)

- ✓ Décaler toutes les lettres d'un message de *k* positions dans l'alphabet (3 pour César);
- ✓ La clé est le décalage *k* (en l'occurrence 3);
- ✓ Ne résiste pas longtemps à une analyse statistique (en repérant la fréquence des lettres), ou même à une recherche exhaustive (26 clés à tester).

- ⊡ **Exemple 1:**

  - k=3
  - La transposition des caractères est la suivante:

    ABCDEFGHIJKLMNOPQRSTUVWXYZ
    DEFGHIJKLMNOPQRSTUVWXYZABC

  Message en clair: BONJOUR
  Message crypté : ERQMRXU

Chiffrement par substitution

- **Exemple 2:**

- construction d'une clé : choix d'un mot particulier

suppression des blancs et des répétitions

JULIUS CESAR ---------- JULISCEAR

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

- Message en clair: BONJOUR
- Message crypté : UZYTZKF

Chiffrement par transposition

- Permuter l'ordre des lettres du message suivant des règles bien définies (par colonne par exemple)

- Le chiffrement par transposition demande de découper le texte clair en blocs, La clé de chiffrement est la permutation elle-même.