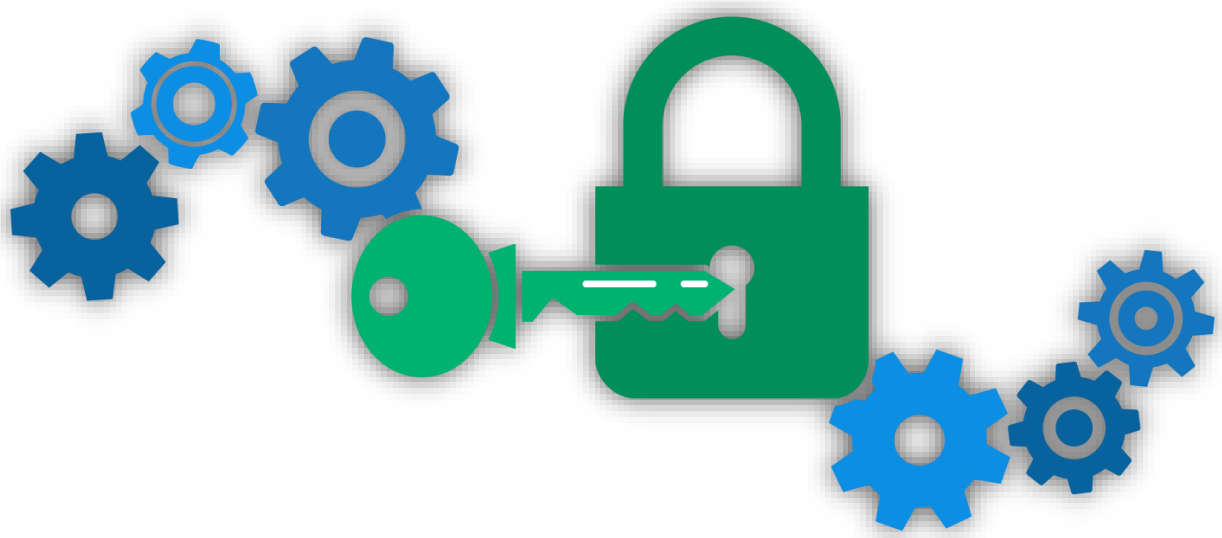
COMPTE RENDU

CRYPTAGE



Réalisé par :

- **OTHMANE TAYBI**

Encadré par :

- **Mr. A.OMOR**

Cryptage :

☑Quelques notions :

Avant de me lancer dans le vif de cette partie de travaux pratiques qui s'appelle 'Cryptage' On va traiter des notions :

- **Chiffrement :**

Transformation, à l'aide d'une clé, d'un message en clair en message chiffré.

- **Chiffre :**

Utilisation de la substitution au niveau des lettres.

- **Code :**

Utilisation de la substitution au niveau des mots ou phrases pour coder.

- **Coder :**

Utilisation d'un code sur un texte.

- **Cryptogramme :**

Message chiffré.

- **Cryptosystème:**

Algorithme de chiffrement.

- **Décrypter :**

Retrouver le message clair à partir du message chiffré sans connaître la clé.

- **Cryptanalyse :**

Science de l'analyse des cryptogrammes pour les décrypter.

- **Cryptographie :**

Étude de l'art du chiffrement.

- **Cryptologie :**

Science regroupant la cryptanalyse ET la cryptographie.

- **Cryptolecte :**

Vocable utilisé par un groupe d'individus utilisant la cryptographie.

- **Cypher :**

Vient de zéro "sifr" (صفر).

Chiffrements faibles

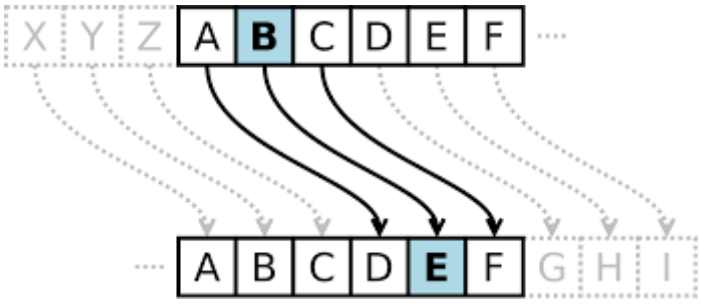
- **Le chiffre de César :**

✦ Procédé de chiffrement par substitution monoalphabétique.

✦ On remplace les lettres par d'autres (décalage de l'alphabet).

✦ Présent encore de nos jours sous le nom ROT13.

✦ Faiblesse à l'analyse de fréquence.



- ***La scytale lacédémonienne :***

✦ Première trace de procédé de dissimulation intentionné.

✦ Bâton que se transmettent les coureurs de courses de relais.

✦ Principe :

- **Destinataire et émetteur ont deux bâtons strictement identiques.**
- **L'émetteur enroule une courroie autour du bâton.**
- **L'émetteur écrit le message puis déroule la courroie.**
- **Le destinataire n'a qu'à enrouler la courroie autour de son bâton pour lire le message !**

✦ Message chiffré :

KTMIOILMDLONKRIIRGNOHGWT

.

- ***Stéganographie :***

✦ Pas à proprement parler un procédé cryptologique → cacher et non chiffrer.

✦ Utiliser une image ou un texte pour cacher de l'information.

✦ Message transmis par un espion allemand pendant le premier conflit → mondial.

Mili tu m infin
i tus eſt exerc itus
ac prope diem ini
bunt be llum, ex plo rato
res omnes deprehen ſi ſu nt,
capite pœn as de dere.

Gratæ Miliſie tuæ fuere literæ, preſertim cum infin i ſcr ip tus eſt ludus, quo ſe exerceт T itus noſter fami-liaris, ac prope modum in diem inimicus, propterea ama bunt bene illum, ſi is exemplo eorum, rato que modo res omnes deprehendet, at ſi ſumunt, alij rem à ſummo capite, eum pœnitebit illas amplius deri dere. vale.

Honor Militiæ tuus fuit Carolus pater, nam cum infini to vic tus eſt, cum minima exercitu inuitus parte hoſtis fugit, ac prope vltimum diem iniurius peribit, ne-cabunt Bere illum atque extem plo puer Arato pe-ribit, res omnes deprehenſæ bonæ ſi ſunt, ante Syllam, & optimo capite non pœnitentias amplius deci dere ſperabit. vale.

☑Pourquoi le cryptage :

- **Confidentialité :**

Mécanisme pour transmettre des données de telle sorte que seul le destinataire autorisé puisse les lire.

- **Intégrité :**

Mécanisme pour s'assurer que les données reçues n'ont pas été modifiées durant la transmission.

- **Authentification :**

Mécanisme pour permettre d'identifier des personnes ou des entités et de certifier cette identité.

- **Non-répudiation :**

Mécanisme pour enregistrer un acte ou un engagement d'une personne ou d'une entité de telle sorte que celle-ci ne puisse pas nier avoir accompli cet acte ou pris cet engagement.