**Exposé sur le Chiffrement de César**

**Introduction**

Le chiffrement de César est l'un des systèmes de cryptographie les plus anciens et les plus simples. Il doit son nom à Jules César, qui l'utilisait pour communiquer secrètement avec ses généraux. Ce système repose sur le principe du décalage des lettres de l'alphabet pour rendre un message illisible sans la clé de déchiffrement. Dans cet exposé, nous allons découvrir le fonctionnement du chiffrement de César, ses avantages, ses limites et ses applications actuelles.

**I. Principe de Fonctionnement**

Le chiffrement de César consiste à remplacer chaque lettre d'un message par une autre lettre située à un certain nombre de positions plus loin dans l'alphabet.

**Exemple :** Avec un décalage de 3 :

* A devient D
* B devient E
* C devient F

La formule mathématique utilisée pour chiffrer est :

Où :

* représente la position de la lettre dans l'alphabet (A = 0, B = 1, ..., Z = 25)
* est la clé de décalage
* signifie que l'on revient au début de l'alphabet après la lettre Z

**II. Déchiffrement**

Pour décoder un message chiffré,

**Exemple :** FKDW → CHAT avec un décalage de 3.

**III. Avantages et Limites**

**Avantages :**

* Simplicité d'utilisation
* Facile à comprendre
* Adapté pour l'apprentissage de la cryptographie

**IV. Applications Modernes**

Bien que ce système soit obsolète pour la sécurité, il est encore utilisé pour :

* Des jeux de cryptographie (escape games, chasses aux trésors)
* L'apprentissage de la cryptographie
* Des messages cachés simples

**Conclusion**

Le chiffrement de César est un système de cryptographie simple mais fondamental pour comprendre les bases de la sécurité des informations. Bien qu'il soit aujourd'hui dépassé, il reste une première étape dans l'étude des méthodes de chiffrement modernes. La cryptographie a évolué vers des systèmes beaucoup plus complexes, mais l'histoire du chiffrement de César montre l'importance de protéger les informations sensibles.