**La cryptanalyse** est l'étude des méthodes pour déchiffrer des messages chiffrés sans avoir accès à la clé secrète. Voici une analyse des méthodes cryptanalytiques couramment utilisées pour les algorithmes de chiffrement classiques mentionnés **: Affine , Vigenère, Hill et Rail Fence.**

**1. Chiffrement Affine**

Le chiffrement Affine est un chiffrement par substitution mono-alphabétique qui utilise une fonction mathématique linéaire pour chiffrer chaque lettre du texte en clair. La fonction de chiffrement est de la forme ( E(x) = (ax + b) mod m ), où a et b sont des clés, x est la position de la lettre dans l'alphabet, et m est la taille de l'alphabet.

**Méthode cryptanalytique :**

* **Attaque par analyse de fréquence**

- Le chiffrement Affine est vulnérable à l'analyse de fréquence car il conserve la distribution des lettres du texte clair.

- Les lettres les plus fréquentes dans le texte chiffré correspondent probablement aux lettres les plus fréquentes dans la langue du texte clair (par exemple, en français, `E`, `A`, `S`, etc.).

- En identifiant deux lettres fréquentes, on peut résoudre un système d'équations pour retrouver les coefficients de la fonction affine.

* **Attaque par force brut**

- Le chiffrement Affine utilise deux clés (coefficients `a` et `b`), mais il y a seulement `312` paires valides (car `a` doit être premier avec `26`).

- Une attaque par force brute est donc réalisable en testant toutes les combinaisons possibles.

**2. Chiffrement de Vigenère**

Le chiffrement de Vigenère est un chiffrement par substitution poly-alphabétique qui utilise une clé répétée pour décaler les lettres du texte clair.

**Méthode cryptanalytique :**

* Analyse de la longueur de la clé :

La méthode de Kasiski permet d'estimer la longueur de la clé en recherchant des répétitions de séquences dans le texte chiffré.Le test de coïncidence de Friedman peut également être utilisé pour estimer la longueur de la clé.

* **Analyse de Fréquence**:

Une fois la longueur du mot-clé déterminée, chaque sous-texte peut être traité comme un texte chiffré par substitution monoalphabétique, et l'analyse de fréquence peut être utilisée pour casser le chiffrement.

* **Attaque par force brute :**

Si la clé est courte, une attaque par force brute peut être réalisée en testant toutes les combinaisons possibles de la clé.

**3. Chiffrement de Hill**

Le chiffrement de Hill est un chiffrement par substitution polygraphique qui utilise l'algèbre linéaire. Chaque bloc de lettres est traité comme un vecteur et multiplié par une matrice de clés pour obtenir le texte chiffré.

**Méthode cryptanalytique :**

* **Attaque par texte clair connu:**

Si l'attaquant connaît suffisamment de paires de texte en clair et de texte chiffré, il peut utiliser ces paires pour construire un système d'équations linéaires et résoudre pour la matrice de clés..

* **Attaque par analyse de fréquence :**

Bien que le chiffrement de Hill masque les fréquences des lettres individuelles, il peut être vulnérable à des attaques statistiques sur des blocs de lettres.

* **Attaque par force brute:**

Si la taille de la matrice est petite (par exemple, 2x2), une attaque par force brute peut être réalisée en testant toutes les matrices inversibles possibles.

**4. Chiffrement Rail Fence**

Le chiffrement Rail Fence est un chiffrement par transposition qui réorganise les lettres du texte clair en les écrivant en zigzag sur un nombre fixe de rails.

**Méthode cryptanalytique :**

* **Attaque par essai et erreur :**

Le nombre de rails est généralement petit, donc une attaque par essai et erreur peut être utilisée pour tester différentes configurations de rails.

Une fois le nombre de rails trouvé, le texte peut être facilement reconstruit.

* **Analyse des motifs :**

- Le chiffrement Rail Fence conserve certaines propriétés du texte clair, comme la séquence des lettres.

- En analysant les motifs et en essayant de reconstruire le texte, il est possible de retrouver le message original.

* **Attaque par force brute :**

Si le nombre de rails est inconnu, une attaque par force brute peut être utilisée pour tester toutes les configurations possibles.

Les algorithmes de chiffrement classiques sont vulnérables à des attaques cryptanalytiques en raison de leur simplicité et de leur dépendance à des motifs statistiques ou mathématiques prévisibles. Les méthodes modernes de chiffrement (comme AES ou RSA) sont conçues pour résister à ces types d'attaques en utilisant des clés plus longues et des opérations plus complexes,