**Mathematical Explanation for Breaking Ciphers using Cryptanalysis Techniques**

**1. Playfair Cipher**

The Playfair cipher is a **digraph substitution cipher** where pairs of letters are encrypted using a **5×5 key matrix**.

**Breaking Playfair Cipher**

To break the Playfair cipher, we use **frequency analysis and digraph statistics**:

1. **Known Plaintext Attack**: If a plaintext-ciphertext pair is known, we can deduce the key matrix.
2. **Frequency Analysis**:
   * Unlike monoalphabetic ciphers, the Playfair cipher hides single-letter frequencies.
   * However, **digraph frequency analysis** (pairs of letters) can be applied. The most common digraphs in English (e.g., **TH, HE, IN, ER, AN**) can help reconstruct the key.
3. **Mathematical Approach**:
   * Let the **plaintext pair** be (P1,P2)(P\_1, P\_2) and the **ciphertext pair** be (C1,C2)(C\_1, C\_2).
   * Playfair encryption rules (same row, column, or rectangle swapping) are applied to form C1,C2C\_1, C\_2.
   * By collecting a **large number of digraph mappings**, the **structure of the 5×5 key square** can be inferred.

Thus, given enough ciphertext, we can reconstruct the key square and decrypt the text.

**2. Hill Cipher**

The Hill cipher is a **polygraphic substitution cipher** based on **matrix multiplication** in **modulo arithmetic**.

**Breaking Hill Cipher**

1. **Known Plaintext Attack (KPA)**:
   * The **Hill Cipher encrypts an nn-letter block** using an n×nn \times n key matrix KK:

C=K⋅Pmod  26C = K \cdot P \mod 26

where:

* + - CC is the ciphertext vector,
    - PP is the plaintext vector,
    - KK is the encryption matrix.
  + If we obtain **nn plaintext-ciphertext pairs**, we get a system of linear equations:

[C1C2⋮Cn]=K[P1P2⋮Pn]mod  26\begin{bmatrix} C\_1 \\ C\_2 \\ \vdots \\ C\_n \end{bmatrix} = K \begin{bmatrix} P\_1 \\ P\_2 \\ \vdots \\ P\_n \end{bmatrix} \mod 26

* + This system can be solved for KK by computing:

K=C⋅P−1mod  26K = C \cdot P^{-1} \mod 26

where P−1P^{-1} is the modular inverse of the plaintext matrix.

* + If **PP is invertible modulo 26**, we recover KK, allowing full decryption.

1. **Ciphertext-Only Attack (COA)**:
   * If only ciphertext is available, **statistical analysis** can be used:
   * The Hill cipher retains letter frequency properties, making it susceptible to **bigram frequency analysis**.
   * If brute force is feasible (for small nn, like n=2n=2), we can try all invertible matrices.

Thus, solving the system of equations or applying frequency analysis allows breaking the Hill cipher.

**3. Vigenère Cipher**

The Vigenère cipher is a **polyalphabetic substitution cipher** where a keyword determines multiple Caesar shifts.

**Breaking Vigenère Cipher**

1. **Kasiski Examination (Key Length Discovery)**:
   * The **repeating nature** of the key creates **repeated substrings** in the ciphertext.
   * Find **repeated sequences** and measure the **distance** between occurrences.
   * The **greatest common divisor (GCD)** of these distances suggests the key length kk.
2. **Frequency Analysis (Key Recovery)**:
   * Once kk is known, the ciphertext is **split into kk columns**, each encrypted with a single-letter Caesar cipher.
   * **Letter frequency analysis** is applied to each column, comparing frequencies to English letter frequencies to recover each shift.
3. **Mathematical Representation**:
   * Let PiP\_i be the iith plaintext letter and KjK\_j be the jjth key letter (cycling every kk characters).
   * Encryption: Ci=(Pi+Kj)mod  26C\_i = (P\_i + K\_j) \mod 26
   * Decryption: Pi=(Ci−Kj)mod  26P\_i = (C\_i - K\_j) \mod 26
   * If we find each KjK\_j using frequency analysis, we recover the entire key.

Thus, knowing the key length and applying frequency analysis allows us to break the Vigenère cipher efficiently.

**Conclusion**

| **Cipher** | **Primary Breaking Technique** |
| --- | --- |
| Playfair | **Digraph Frequency Analysis, Known Plaintext Attack** |
| Hill | **Matrix Inversion (KPA), Frequency Analysis (COA)** |
| Vigenère | **Kasiski Examination, Frequency Analysis** |

Each cipher relies on **patterns and structure**, making them vulnerable to **mathematical cryptanalysis techniques**.