A 3×3 Hill cipher hides not only single-letter but also two-letter frequency information.

Easily broken with a <u>known plaintext attack</u>.

$$c_j = m_j \cdot K, \quad K: \ell \times \ell. \quad j = 1, \dots, \ell.$$

assume (m_j, c_j) are known.

$$\underbrace{\begin{pmatrix} -c_1- \\ -c_2- \\ \vdots \\ -c_\ell- \end{pmatrix}}_{= C} = \underbrace{\begin{pmatrix} -m_1- \\ -m_2- \\ \vdots \\ -m_\ell- \end{pmatrix}}_{= M} \cdot K.$$

If M has an inverse M^{-1}, then

$$K = M^{-1} C.$$

Ex. 2×2 Hill cipher

plaintext = hillcipher

ciphertext = HCRZSSXNSP

$$\begin{array}{ccccc} m_1 & m_2 & m_3 & m_4 & m_5 \\ 7 \ \ 8 & 11 \ \ 11 & 2 \ \ 8 & 15 \ \ 7 & 4 \ \ 17 \\ 7 \ \ 2 & 17 \ \ 25 & 18 \ \ 18 & 23 \ \ 13 & 18 \ \ 15 \\ c_1 & c_2 & c_3 & c_4 & c_5 \end{array}$$

$$\begin{pmatrix} 7 & 2 \\ 17 & 25 \end{pmatrix} = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \cdot K \pmod{26}.$$

check K.

$$K = M^{-1} \cdot \begin{pmatrix} 7 & 2 \\ 17 & 25 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 8 & 5 \end{pmatrix}$$ (verify it).

Polyalphabetic Ciphers

Vigenère cipher

$m \in \mathbb{Z}_{26}^{\ell}$, $k \in \mathbb{Z}_{26}^{n}$, where $n < \ell$.

$c = E(m, k) \in \mathbb{Z}_{26}^{\ell}$, defined by

$c_i = m_i + k_{(i \bmod n)} \mod 26.$

$k = k_0 k_1 k_2 \cdots k_{n-1}$

$m = m_0 m_1 m_2 \cdots m_\ell.$

Ex: $\ell = 15$, $n = 3$.

$$\begin{array}{ccc|ccc|c|c}
m_0 & m_1 & m_2 & m_3 & m_4 & m_5 & \cdots & m_{15}. \\
k_0 & k_1 & k_2 & k_0 & k_1 & k_2 & \cdots &
\end{array}$$

$D(c, k) \triangleq \bar{m}$

$\bar{m}_i = c_i - k_{(i \bmod n)} \mod 26.$

determine the length of the keyword, followed by frequency.

Vernam cipher

$c_i = m_i \oplus k_i$, where $c_i, m_i, k_i \in \mathbb{Z}_2$

$$\begin{cases} m_i \oplus 0 \\ m_i \oplus 1 \end{cases}$$

One-time pad.

$m \in \mathbb{Z}_2^n$. $k \in \mathbb{Z}_2^n$. $c \in \mathbb{Z}_2^n$.

$c = E(m, k) \triangleq m \oplus k$.

$D(c, k) \triangleq c \oplus k$.

Def. (Perfect Secrecy) $\forall m_1, m_2$ plaintext. $\in \mathbb{Z}_2^n$.

c : ciphertext

$$\Pr(M = m_1 \mid C = c) = \Pr(M = m_2 \mid C = c)$$

$$= \frac{1}{2^n}$$

Shannon theory

$\underbrace{m_1}_{n \text{ bits}} \oplus k = c_1$

$\underbrace{m_2}_{n \text{ bits}} \oplus k = c_2$

$\longrightarrow c_1 \oplus c_2 = (m_1 \oplus k) \oplus (m_2 \oplus k) = \underbrace{m_1 \oplus m_2}_{n \text{ bits}}$

fundamental difficulties

1. supplying truely random keys of a large number
2. key distribution & protection.