# Auto-key cipher.

pass key: $\bar{k}$ length $l$  $\bar{x}_1\ \bar{x}_2\ \cdots\cdots$

except the last one each of $\bar{x}_i \in \mathbb{Z}_n^l$ for $n \in \mathbb{N}$

$\left[\cdot\ \bar{y}_i = \bar{x}_i + \bar{k}\right.$ where $\bar{x}_i = (x_{i1}\ x_{i2} \cdots\ x_{il})$ $\left.\bar{k} = (k_1, k_2, \cdots, k_l)\right]$

$\bar{y}_1 = \bar{x}_1 + \bar{k}$ ✓

$\bar{y}_2 = \bar{x}_2 + \bar{x}_1$

$\bar{y}_{i+1} = \bar{x}_{i+1} + \bar{x}_i$  for $1 \leq i$

Example: $\bar{k}$ = ANT $\rightarrow$ pass key.

plain text $\bar{x}$ = WE_DISAGREE

ANTWE-DISAG

cipher text $\bar{y}$ = WRSZMRD

$A = \{A, B, \cdots, Z, \_\}$ (A $\to$ 0, _ $\to$ 26)

Decryption: $\bar{x}_i = \bar{y}_i - \bar{k}$ (Vigenere)

For Auto key cipher: $\bar{x}_1 = \bar{y}_1 - \bar{k}$

$\bar{x}_2 = \bar{y}_2 - \bar{x}_1$

$\vdots$

$x_{i+1} = \bar{y}_{i+1} - \bar{x}_i$

---

Suppose the cipher text obtained by Vigenere Encryption

is $C_1 = y_{11}\ y_{12} \cdots\ y_{1l}$

$C_2 = y_{21}\ y_{22} \cdots\ y_{2l} \longrightarrow (x_{21}, x_{22} \cdots x_{2l}) + (k_1, \quad k_2 \cdots \quad k_l)$

$\vdots$

$C_m = y_{m1}\ y_{m2} \cdots y_{ml}$

We want to decrypt it without knowing the pass key $\bar{k}$

Suppose we know the length of $\bar{k}$, say $l$.

Consider the columns

$$\begin{array}{c|c|c|c}
y_{11} & y_{12} & \cdots & y_{1\ell} \\
y_{21} & y_{22} & & y_{2\ell} \\
\vdots & \vdots & & \vdots \\
y_{m1} & y_{m2} & & y_{m\ell}
\end{array}$$

Apply frequency analysis in each of the columns & find $x_{ij}$ s.t. $\mathcal{E}(x_{ij}) = y_{ij}$ where $y_{ij}$ has the highest frequency in the $j$th column

For each $j$ we decrypt $y_{sj}$ $\underline{1 \le j \le \ell}$, $1 \le s \le m$.

---

Cipher text $\bar{x}_1 \, \bar{x}_2 \cdots \bar{x}_m$ where $\bar{x}_i \in A^\ell$

$\bar{x}_i = x_{i1} \, x_{i2} \cdots x_{i\ell}$

$\bar{x}_i \longmapsto A\bar{x}_i$

for $A \in M_{\ell \times \ell}(\mathbb{Z}_n)$ where $n = |A|$

---

Example: CRYPTOGRAPHY IS THE PRACTICE OF SECURING INFORMATION BY USING CODES AND ALGORITHMS TO ENCRYPT AND DECRYP DATA.

$n=27$, $A = \{A, B, \ldots, -\}$

$\underline{\ell = 2}$

$A = \begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix}$, $\det(A) = 4-6 = 25 \in U(\mathbb{Z}_{27})$ (coprime to 27).

$\mathbb{Z}_n^\ell \longrightarrow \mathbb{Z}_n^\ell$

$X \longmapsto AX$

for $A \in M_\ell(\mathbb{Z}_n)$ is an isomorphism if $A$ is invertible & the inverse map is

$Y \longmapsto A^{-1}Y$

A is invertible if & only $\det(A) \in U(\mathbb{Z}_n)$

$A^{-1} = 25^{-1}\begin{pmatrix} 4 & -3 \\ -2 & 1 \end{pmatrix}$

$= 13\begin{pmatrix} 4 & -3 \\ -2 & 1 \end{pmatrix}$

$= \begin{pmatrix} -2 & -12 \\ 1 & 13 \end{pmatrix}$

$2 \times 14 = 28 = 1 \pmod{27}$

$2^{-1} = 14$

$-2^{-1} = -14 = 13 \pmod{27}$

$N$ (plaintext) $= \underline{2-17} - \underline{24-15} - 19 - 14 - 6 - \cdots$

$$\mathcal{E}\begin{pmatrix}2\\17\end{pmatrix} = \begin{pmatrix}1 & 3\\2 & 4\end{pmatrix}\begin{pmatrix}2\\17\end{pmatrix} = \begin{pmatrix}2+51\\4+68\end{pmatrix} = \begin{pmatrix}-1\\-9\end{pmatrix} = \begin{pmatrix}26\\18\end{pmatrix}$$

$\underline{\mathcal{E}(CR) = -S}$

$$\mathcal{E}\begin{pmatrix}24\\15\end{pmatrix} = \begin{pmatrix}1 & 3\\2 & 4\end{pmatrix}\begin{pmatrix}24\\15\end{pmatrix} =$$

More generally, we have matrix analogue of affine cipher ~~R~~ namely, $X \longmapsto AX+B$ where $A \in GL_\ell(\mathbb{Z}_n)$ & $B \in M_{\ell \times 1}(\mathbb{Z}_n)$

& Decryption is given by $Y \longmapsto A^{-1}Y - A^{-1}B$.

$$\left[\ \mathcal{D}\,\mathcal{E}(X) = \mathcal{D}(AX+B) = A^{-1}(AX+B) - A^{-1}B = (A^{-1}A)X + A^{-1}B - A^{-1}B = X.\ \right]$$

$\underline{\text{Sly}}$ $\underline{\mathcal{E}\circ\mathcal{D}(\cancel{X}) = Y}$