ECG 471/571 Early ciphers (cont'd)

- Vigenere cipher
- Hill cipher $P = C = (\mathbb{Z}_{26})^m$

$\underline{K}$ is $m \times m$ matrix.

$\vec{x}$. $\vec{y} = \underline{K \cdot \vec{x}} \mod 26$

$\vec{y}^T = \vec{x}^T \cdot K^T$

plaintext "$\underline{\underline{te}}\,\underline{st}$" $K = \begin{pmatrix} 2 & 5 \\ 3 & 7 \end{pmatrix}$

$t \to 19$

$e \to 4$

$\vec{y}_1 = \begin{pmatrix} 2 & 5 \\ 3 & 7 \end{pmatrix} \begin{pmatrix} 19 \\ 4 \end{pmatrix} \mod 26$

$m=2$

$= \begin{pmatrix} 38+20 \\ 57+28 \end{pmatrix} \mod 26$

$= \begin{pmatrix} 6 \\ 7 \end{pmatrix} \to \begin{pmatrix} G \\ H \end{pmatrix}$

$s \to 18$

$\begin{pmatrix} 2 & 5 \end{pmatrix} \begin{pmatrix} 18 \end{pmatrix}$

$t \to 19$ $\vec{y}_2 = \begin{pmatrix} - & - \\ 3 & 7 \end{pmatrix} \begin{pmatrix} \cdot \\ 19 \end{pmatrix}$

$= \begin{pmatrix} 20 \\ 21 \end{pmatrix} \to \begin{pmatrix} U \\ V \end{pmatrix}$

cipher: $\begin{pmatrix} G \\ H \\ U \\ V \end{pmatrix}$

$\underline{D_K}(\vec{y}) = K^{-1} \cdot \vec{y} \mod 26$

$= \underline{K^{-1}} \cdot (\underline{K} \cdot \vec{x}) \mod 26$

$= \vec{x}$

K^{-1} exists iff $(\det K)$ has multplicative inverse.

$K = \begin{pmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{pmatrix}$

$\det K = K_{11} \cdot K_{22} - K_{21} \cdot K_{12} \mod 26$

$-1 \begin{pmatrix} K_{22} & -K_{12} \end{pmatrix}$

$$K^{-1} = (\det K)^{-1} \begin{pmatrix} k_{22} & -k_{12} \\ -k_{21} & k_{11} \end{pmatrix} \bmod 26$$

e.g.

$$K = \begin{pmatrix} 5 & 8 \\ 17 & 3 \end{pmatrix}$$

$$\det K = 9 \bmod 26$$

$$\gcd(9, 26) = 1$$

$$9^{-1} \bmod 26 = \underline{3}$$

$$\underline{K^{-1}} = 3 \cdot \begin{pmatrix} 3 & -8 \\ -17 & 5 \end{pmatrix} = \begin{pmatrix} 9 & 2 \\ 1 & 15 \end{pmatrix} \bmod 26$$

$$K \cdot K^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod 26.$$

- Block cipher
- stream cipher

Vernam cipher.

$x = 1\,0\,1\,0\,1\,0\,0\,1\,0\,0 \cdots$

$k = 0\,1\,0\,1\,0 \cdots 1\,0\,0 \cdots$

random

$y_i = x_i \oplus k_i$

$x_i = y_i \oplus k_i$

XOR

$\oplus$	0	1
0	0	1
1	1	0

$\oplus$: $x_i + k_i \bmod 2$ $\qquad \mathbb{Z}_2$ $\{0, 1\}$.

a.k.a. One-time pad

$$
\begin{array}{rl}
x: & 1101100101 \\
\oplus\ k: & 0110100011 \\
\hline
y: & 1011000110
\end{array}
$$

permutation cipher $\quad 6!$

j	1	2	3	4	5	6
$\pi(j)$	3	5	1	6	4	2

1 2 3 4 5 6

follow | ashore |

LWFOOL HEARSO

1 2 3 4 5 6

decryption

j	1	2	3	4	5	6
$\pi^{-1}(j)$	3	6	1	5	2	4