ECE 471/571 Cryptanalysis

known-plaintext attack

plaintext : shift key: 3
cipher : vkliw

chosen-plaintext attack. $a \xrightarrow{E} c$

chosen-cipher attack: key: 2

$a \xrightarrow{D} z$ key: 1

Affine cipher.

$$E_K(x) = ax + b \bmod 26$$

Freq. of cipher letters.	English
R — 8	e
D — 7	t
E — 5	a
K — 5	i
H — 5	o
F — 4.	:

if $R \to e$, $D \to t$

$$\begin{cases} 4a + b \equiv 17 \bmod 26 \\ 19a + b \equiv 3 \bmod 26 \end{cases}$$

✗ $a = 6$, $b = 19$.

$\gcd(6, 26) \neq 1.$

if $R \to e$, $E \to b$ $\Rightarrow$ $a = 13$ ✗

if $R \to e$, $K \to t$ $\Rightarrow$ $a = 3$, $b = 5$ ✓

CPA: choose $x_1 = 0$, $x_2 = 1$

$y_1 = 0 \times a + b \equiv b \mod 26$

$y_2 = 1 \times a + b \equiv a + b \mod 26$

$a = y_2 - y_1 \mod 26$

$b = y_1$

CCA $y_1 = 0 = a x_1 + b \mod 26$

$y_2 = 1 = a x_2 + b$

Hill cipher e.g.: $m = 2$

plaintext friday $\underline{x}_1 = (5 \quad 17)^T$

cipher PQCFKU $x_2 = (8, 3)$

$Y_1 = (15 \quad 16)^T$

$Y_2 = (2 \quad 5)^T$ $\quad \vec{Y} = K \cdot \vec{X}$

$$Y = \begin{pmatrix} 15 & 2 \\ 16 & 5 \end{pmatrix} \qquad X = \begin{pmatrix} 5 & 8 \\ 17 & 3 \end{pmatrix}$$

$$Y = K \cdot X$$

$$Y \cdot X^{-1} = K \cdot X \cdot X^{-1}$$

$$= K$$

$$K = \begin{pmatrix} 15 & 2 \\ 16 & 5 \end{pmatrix} \cdot \begin{pmatrix} 9 & 2 \\ 1 & 15 \end{pmatrix}$$

$$= \begin{pmatrix} 7 & 19 \\ 9 & 3 \end{pmatrix} \mod 26$$

\ o