20 August 2020 08:00

Cryptanalysis

Assumptions 1. The adversary, Oscar, knows the cryptosystem being used.

2. We will consider ciphertext only attack.

3. Plaintext is in ordinary English without punctuation and spaces.

1. Cryptanalysis of Affine Cipher :

FMXVEDKAPHFERBNDKRXRSREFMORUDSDKDVSHVUFEDK
APRKDLYEVLRHHRH

Affine Cipher :

Encryption : $C = (Pk_1 + k_2) \bmod 26$

letter	frequency	letter	frequency
A	2	*N*	1
B	1	*O*	1
C	0	*P*	2
D	7	*Q*	0
E	5	*R*	8
F	4	*S*	3
G	0	*T*	0
H	5	*U*	2
I	0	*V*	4
J	0	*W*	0
K	5	*X*	2
L	2	*Y*	1
M	2	*Z*	0

The most frequent ciphertext characters are

R — 8 times
D — 7 "
E, H, K — 5 "
F, S, V — 4 "

Guess : $E_K(e) = R$ & $E_K(t) = D$

$E_K(4) = 17$, & $E_K(19) = 3$

$4k_1 + k_2 = 17 \pmod{26}$ —— 1

$19k_1 + k_2 = 3 \bmod 26$ —— 2

20 August 2020 08:18

Solving 1 & 2 we get $k_1 = 6$, $k_2 = 19$ ✓ ✗

Q. Is it a valid key? Ans No

We know that $k_1 \in \mathbb{Z}_{26}^{*} = \{x \in \mathbb{Z}_{26} \mid \gcd(x, 26) = 1\}$

$k_2 \in \mathbb{Z}_{26}$

(6, 19) can not be a key.

Guess: $E_K(e) = R$, $E_K(t) = K$

i.e. $E_K(4) = 17$, $E_K(19) = 10$

$4k_1 + k_2 = 17 \mod 26$ — 3

$19k_1 + k_2 = 10 \mod 26$ — 4

Solving 3 & 4 we get $k_1 = 3$ & $k_2 = 5$

Q. Is it a valid key?

A. Yes

$D_K(c) = [(c - k_2) \times k_1^{-1}] \mod 26$

$D_K(c_1) = (5 - 5) \times 9 \mod 26$

$= 0$

$\equiv a$

```
algorithmsarequitegeneraldefinitionsofarit
hmeticprocesses
```

20 August 2020 08:27

Cryptanalysis of Hill Cipher

Hill Cipher : $P \equiv (P_1 P_2 \cdots P_m)(P_{m+1} P_{m+2} \cdots, P_{2m}) \cdots$

$C \equiv (C_1 C_2 \cdots C_m) \; (C_{m+1}, \cdots, C_{2m}) \cdots$

$K \text{ (key)} = \begin{bmatrix} k_{11} & \cdots & k_{1m} \\ \vdots & & \\ k_{m1} & \cdots & k_{mm} \end{bmatrix}$ (K is the key and it is such that K^{-1} exists)

$$[C_1, C_2, \cdots, C_m] = [P_1, P_2, \cdots, P_m] \begin{bmatrix} & & \\ & K & \\ & & \end{bmatrix}$$

Ciphertext only attack is very difficult to implement.

Let's assume that m is known to the adversary Oscar.

Suppose Oscar has at least m- distinct plaintext-Ciphertext pairs.

$x_j = x_{1,j}, x_{2,j}, \cdots, x_{m,j} \quad , \quad 1 \le j \le m$

& $y_j = y_{1,j}, y_{2,j} \cdots, y_{m,j} \quad , \quad 1 \le j \le m$

such that $y_j = E_K(x_j) \qquad 1 \le j \le m$

Let $X = [x_{i,j}]$ & $Y = [y_{i,j}]$

Then $Y = XK$ – K is the key i.e. it is an $m \times m$ matrix which is unknown.

If X^{-1} exists then $K = X^{-1} Y$

20 August 2020 08:36

Ex: Plaintext : friday
Ciphertext : PQCFKU
$m = 2$
Hill Cipher is being used

known to Oscar

$E_K(5, 17) = (15, 16)$ — 1

$E_K(8, 3) = (2, 5)$ — 2

$E_K(0, 24) = (10, 20)$ — 3

from 1 & 2

$$\begin{bmatrix} 15 & 16 \\ 2 & 5 \end{bmatrix} = \begin{bmatrix} 5 & 17 \\ 8 & 3 \end{bmatrix} K$$

$$K = \begin{bmatrix} 5 & 17 \\ 8 & 3 \end{bmatrix}^{-1} \begin{bmatrix} 15 & 16 \\ 2 & 5 \end{bmatrix}$$

$$K = \begin{bmatrix} 9 & 1 \\ 2 & 15 \end{bmatrix} \begin{bmatrix} 15 & 16 \\ 2 & 5 \end{bmatrix} = \begin{bmatrix} 7 & 19 \\ 8 & 3 \end{bmatrix}$$

Book : Cryptography : Theory & Practices by Douglas R. Stinson

20 August 2020 08:44

Steganography : This is technique in which we hide a message inside another message.

1. Invisible ink
2. tiny pin punctures ✓
3. minute variations b/w handwritten characters
4. pencil marks on handwritten char. etc.

Take an image file and replace the last two least significant digits of each pixel of that image with two bits of our message.

Resulting image would not look too different