Tutorial IV

10 October 2019 09:18

Historical Cryptosystems and Perfect secrecy.

Definition of encryption system:

P - set of plaintexts

K - set of keys

C - set of cipher texts

e_k - encryption function : $(P \times K) \to C$ (input: $P \times K$, output: C)

d_k - decryption function : $(C \times K) \to P$

$$\forall p \in P, k \in K \qquad d_k(e_k(p)) = p$$

EXAMPLE:

CEASAR CRYPTOSYSTEM

$P = \{A, B, C, \ldots, Z\} \quad |P| = 26$

$C = \{A, B, C, \ldots, Z\} \quad |C| = 26$

$K = \{0, \ldots, 25\}$

0	1	2	3	4	5	...	24	25
A	B	C	D	E	F	...	X	Y	Z

$e_k : p \to p + k \pmod{26}$

$p = C$

$k = 3$

$e_3(C) \to F$

$d_k : c \to c - k \pmod{26}$

	25
$k = 1$	A B C D E F ... Z
	B C D E F G ... A

$k=1$

A	B	C	D	E	F	...	Z
B	C	D	E	F	G	...	A

EXAMPLE OF A MONOALPHABETIC ENCRYPTION

(it maps letters to letters, it maps the same letter to the same letter for each k)

4.2

[redacted]

Encrypt "CRYPTOLOGY"

$P: \{A \to Z\} \setminus \{J\}$

different 25! keys

$K=$	A	B	C	D	E
→ F	A	B	C	D	E
G	F	G	H	I/J	K
H	L	M	N	O	P
→ I	Q	R	S	T	U
→ K	V	W	X	Y	Z

$C \to FC$ $R \to IB$ $Y \to KD$ P T

O L O G Y → KD

$$C = \{ x_0 \mid x \in \{A,B,C,D,E\}, Y \in \{F,G,H,I,K\} \}$$

Affine Cryptosystem

$P = C = \{0, \dots, 25\}$

$K = \{(a,b)$ s.t. a is invertible mod 26 $\}$ $= a \in \{1,3,5,7,9,11,15,17,19,21,23,25\}$

$\Leftrightarrow$ $\gcd(a,26) = 1$

$e_k(p) = p \cdot a + b \mod 26$

$d_k(c) = (c-b) \cdot a^{-1} \mod 26$

$p \cdot a + b = p$

How to break monoalphabetic cryptosystems?

EVERYDAY E R R EVERY E

WIWGC RYC CXA VYC VYMW LGXUGWOO. WIWGC OSWL VYC QW BGAHSBAN.

CWS SEWGW DHNN OSGWSPE XAS QWBXGW CXA YZ WIWG–NWZUSEWZHZU,

WIWG–YOPWZRHZU, WIWG–HVLGXIHZU LYSE. CXA MZXD CXA DHNN ZWIWG

UWS SX SEW WZR XB SEW FXAGZWC. QAS SEHO, OX BYG BGXV

RHOPXAGYUHZU, XZNC YRRO SX SEW FXC YZR UNXGC XB SEW PNHVQ.

C P

W → E C → Y R → D

I → V K → O

G → R A → V

Z → W Y → A

WIWG . . . WIGC

5, 10, 15, 25

HILL CRYPTOSYSTEM

$P = \{xy \mid x \in \{A-Z\}, y \in \{A-Z\}\}$ (0-25, 0-25)

$C = P$

$K =$ set of all invertible matrices over $\mathbb{Z}_{26}$

$e_k : M_k \begin{pmatrix} x \\ y \end{pmatrix}$

$d_k : M_k^{-1} \begin{pmatrix} a \\ b \end{pmatrix}$

$\det(M) = d$

$\det(M^{-1}) = d^{-1}$ ✓ when does this exist

$\gcd(d, 26) = 1$

$M = \begin{pmatrix} 1 & 3 \\ 3 & 4 \end{pmatrix}$ $\det(A) = 1 \cdot 4 - 3 \cdot 3 \mod 26$

$= 4 - 9 = -5 = 21$

$M^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$a + 3b = 1$

$3a + 4b = 0$

$\Rightarrow a = 1 - 3b \Rightarrow a = 1 - 33 = -32 = 20$ ✓

$\Rightarrow 3(1 - 3b) + 4b = 0 \Rightarrow -9b + 4b + 3 = 0$

$-5b = -3$

$5b = 3 \quad / \cdot 5^{-1}$

$3c + 4b = 0$

$c + 3d = b$

$3c + 4d = 1$

$\Rightarrow c = -3d$

$\Rightarrow -9d + 4d = 1$

$-5d = 1 \quad / \cdot -1$

$5d = -1 \quad / \cdot 5^{-1}$

$d = -1 \cdot 21$

$= -21$

$= 5$

$-5b = -3$

$5b = 3 \quad / \cdot 5^{-1}$

$b = 3 \cdot 21$

$b = 63 = 11$ ✓

$M^{-1} = \begin{pmatrix} 20 & 11 \\ 11 & 5 \end{pmatrix}$

$C = -15 = 11$

$\begin{pmatrix} 13 \\ 34 \end{pmatrix} \begin{pmatrix} 0 \\ 2 \end{pmatrix} = \begin{pmatrix} 6 \\ 8 \end{pmatrix}$ $\quad \begin{pmatrix} 13 \\ 34 \end{pmatrix} \begin{pmatrix} 2 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ 6 \end{pmatrix}$

b b

(AC) -> (G I)

(CA) -> (C G)

P P

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

P	Q	R	S	T	U	V	W	X	Y	Z
15	16	17	18	19	20	21	22	23	24	25

P P

VIGENÉRE CRYPTOSYSTEM

KEY | KEY | KEY K ← shift of alphabet in this position

CRYPTO LOGY

MVW . . .

$K + C = 10 + 2 = 12$

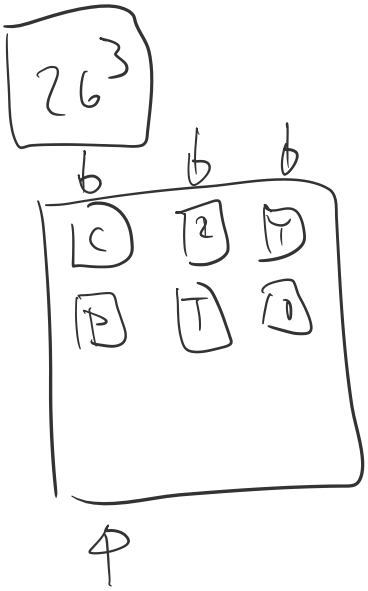
$E + R = 4 + 17 = 21$

$Y + Y = 24 + 24 = -2 + -2 = -4 = 22$

$K + Y = 24 + 10 = 34 = P$

KEYHOLE

CRYPTOG



KASISKI'S METHOD

-> if a subword is repeated in the cryptotext in intervals that are a multiple of ℓ, that ℓ is probable key length

FRIEDMANN

For english:

$$L = \frac{0{,}027\, n}{(n-1)\ell - 0{,}038 n + 0{,}065}$$

n - length of cryptotext
n_i - is number of letter 'i' in cryptotext

PERFECT SECRECY

Intuitively secure encryption should hide statistical properties of the plaintext. (Otherwise easy cryptoanalysis is possible).

$Pr(P)$ ~ underlying probability of plaintext messages.

$Pr(K)$ ~ distribution of the keys (typically uniform)

$Pr(C)$ ~ probability of seeing a cyphertext c.
=> Can be calculated from $P(P)$ and $Pr(K)$

$Pr(C=c \mid P=p)$ probability that p gets encrypted as c

$Pr(P=p \mid C=c)$ probability that c gets decrypted as p

Perfect secrecy ✓ ✓

Perfect secrecy

$\forall p, c \quad Pr(P=p) = Pr(P=p \mid C=c)$

$P(C=c) = \sum_{p \in P} Pr(P=p) \cdot Pr(K=k : e_k(p)=c)$

$P(C=c \mid P=p) = \sum_{k : e_k(p)=c} P(K=k)$

BAYES' THEOREM

$P(A|B) \cdot P(B) = P(B|A) \cdot P(A) \Rightarrow P(A|B) = \frac{P(B|A) \cdot P(A)}{P(B)}$

$P(P=p \mid C=c) = \frac{P(C=c \mid P=p) \cdot Pr(P=p)}{Pr(C=c)}$

If $P(P=p \mid C=c) = Pr(P=p)$ (perfect secrecy)

$\forall c, p$ $P(C=c \mid P=p) = Pr(C=c)$ ⇔ Perfect secrecy

[redacted]

4.15

messages

keys	x	y	z
k_1	a	b	c
k_2	b	c	a
k_3	c	a	b

$e_{k_1}(x) = a$

$e_{k_3}(z) = b$

$Pr(P=x) = 3/8$ | $Pr(K=k_1) = 1/3$

$Pr(P=x) = 3/8$
$Pr(P=y) = 1/8$
$Pr(P=z) = 1/2$

$Pr(K=k_1) = 1/3$
$Pr(K=k_2) = 1/6$
$Pr(K=k_3) = 1/2$

[redacted] $= Pr(P=x) \cdot Pr(K=k_1) + Pr(P=z) Pr(K=k_2)$
$+ Pr(P=y) \cdot Pr(K=k_3)$

$= 3/8 \cdot 1/3 + 1/2 \cdot 1/6 + 1/8 \cdot 1/2 = \frac{1}{8} + \frac{1}{12} + \frac{1}{16} = \frac{13}{48}$

$Pr(C=b) =$

[redacted] $= P(K=k_1) = 1/3$

MEANS THAT CRYPTOSYSTEM ↑ IS NOT PERFECTLY SECURE.

$\forall\ Pr(K=k_1) = P(K=k_2) = P(K=k_3) = 1/3$

$P(C=a) = 3/8 \cdot 1/3 + 1/2 \cdot 1/3 + 1/8 \cdot 1/3 = 1/3$

$= 1/3 \left(\sum_{a \in P} Pr(P=a) \right) = 1/3$

$Pr(C=a \mid P=x) = Pr(K=k_1) = 1/3$

$\forall c, a \quad \exists$ single key mapping $a \to c$

$$Pr(C=c \mid P=a) = 1/3$$

$$Pr(C=c) = \sum_{a \in P} Pr(P=a) \cdot \sum_{k : e_k(a) \to c} P(K=k)$$

$$= \sum_{a \in P} Pr(P=a) \cdot P(K=k \mid e_k(a) \to c)$$

$$= \sum_{a \in P} Pr(P=a) \cdot 1/3$$

$$= 1/3 \sum_{a \in P} Pr(P=a)$$

$$= 1/3$$