Tutorial 4 ENG

06 October 2021 13:56

History of encryption and perfect secrecy

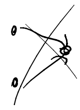
Formal definition of an encryption system

P - set of plaintexts

C - set of ciphertexts

K - set of keys

$e_k: (P \times K) \to C$



$d_k: (C \times K) \to P$

$\forall p, k \quad d_k(e_k(p)) \to P$ → encryption function in injective

CEASAR CRYPTOSYSTEM

0	1	2	3																						25
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	D	E	F	G	H	I	J	K	...															A	B

k=2

$P = \{A, B, \dots, Z\} = \{0, \dots, 25\}$

$C = \{A, B, \dots, Z\} = \{0, \dots, 25\}$

$K = \{A, B, \dots, Z\} = \{0, \dots, 25\}$

$H + C = 7 + 2 = 9 = J$

$e_k(i, k) = i + k \mod 26$

$d_k(j) = j - k \mod 26$

POLYBIOUS CRYPTO SYSTEM

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

$= K, \quad |K| = 25!$ keys

$P = \{A, B, \dots, Z\}$

$C \subseteq \{A, B, \dots Z\}^2$

"CRYPTOLOGY"

C → FC

R → IB

Y → JD

P →

T →

O →

L →

O →

G →

Y → JD

MONOALPHABETIC CRYPTO SYSTEM ↑

EVERY DAY YOU AY A E EVERY TE

WIWGG BYCCXA VYC VYMW LGXUGWOO WIWGC OSWL VYC OW BGAHSBAN

EVERY DAY YOU AY A E EVERY TE

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.

W → E

E → H

S → T

X → O

I → V

G → R

B → F

C → Y

A → U

HILL CRIPTOSYSTEM → NOT MONOALPHABETIC

$P = \{XY \mid x, y \in \{0, \dots, 25\}\}$ (Generally n-tuples)

$C = P$

K = Set of all invertible 2×2 (Generally $n \times n$) matrices invertible mod 26

$$e_{M_2}(ab) = M_2 \begin{pmatrix} a \\ b \end{pmatrix} \bmod 26$$

$$d_{M_2}(ij) = M_2^{-1} \begin{pmatrix} i \\ j \end{pmatrix} \bmod 26$$

$$\boxed{\det(M) = d \qquad \det(M^{-1}) = 1/d}$$

$\det(M)$ needs to be invertible mod 26. $\gcd(d, 26) = 1$

a is invertible mod n iff $\gcd(a, n) = 1$

d is not a divisor of 26

$d \notin \{0, 13, 2\}$

$$M = \begin{pmatrix} 1 & 3 \\ 3 & 4 \end{pmatrix} \qquad \det(M) = 1 \cdot 4 - 3 \cdot 3 \bmod 26$$
$$= 4 - 9 \bmod 26$$
$$= -5 \bmod 26$$

$= 21 \mod 26$

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

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

$$\boxed{\begin{aligned} a \cdot 1 + b \cdot 3 &= 1 \\ a \cdot 3 + b \cdot 4 &= 0 \\ c + 3d &= 0 \\ 3c + 4d &= 1 \end{aligned}} \Rightarrow \begin{aligned} a &= 20 \\ b &= 11 \\ c &= 11 \\ d &= 5 \end{aligned}$$

$AC \leftrightarrow (0\ 2)$

$$M\begin{pmatrix} 0 \\ 2 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 3 & 4 \end{pmatrix}\begin{pmatrix} 0 \\ 2 \end{pmatrix} = (6\ 8) \qquad AC \to GI$$

$CA \leftrightarrow (2\ 0)$

$$M\begin{pmatrix} 2 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 3 & 4 \end{pmatrix}\begin{pmatrix} 2 \\ 0 \end{pmatrix} = (2, 6) \qquad CA \leftrightarrow CG$$

VIGENÉRE CRYPTOSYSTEM

KEY → arbitrary word of length L.

→ CRYPTOLOGY
→ KEYKEYKEYK
MVW . . . . . .

$C+K = 2+10 = 12$
$R+E = 17+4 = 21$

DENCRYPTION
→ CRYPTOLOGY

MVWXYZ . . . .

How to guess the length of the key

KASISKI's METHOD

if a sub word is repeated in the ciphertext in intervals that are a multiple of k, then guess k as the length of the key

XYZ XYZ XYZ XYZ

10 15 5

Guess 5.

FRIEDMAN METHOD

n - number of symbols in the ciphertext (length of ciphertext)
n_i - number of symbols "i" in the ciphertext

$$L = \frac{0{,}027 \cdot n}{(n-1)\cdot \ell - 0{,}038 n + 0{,}065} \qquad \ell = \sum_{i=0}^{25} \frac{n_i(n_i-1)}{n(n-1)}$$

PERFECT SECRECY

Intuitively, secure encryption hides statistical properties of plaintexts (otherwise cryptoanalysis is "easy")

$Pr(P)$ - underlying probability with which plaintexts are sent (frequencies of letters in language)

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

$Pr(C)$ - probability of ciphertexts $\Rightarrow$ influenced by $Pr(P)$, $Pr(K)$

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

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

Perfect secrecy

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

Decide whether cryptosystem is perfectly secure

1/3 1/6 2 1/2

Decide whether cryptosystem is perfectly secure

$P = \{x, y, z\}$

$C = \{a, b, c\}$

$K = \{k_1, k_2, k_3\}$

e_k	x ($1/3$)	y ($1/6$)	z ($1/2$)
k_1	a	b	c
k_2	c	a	b
k_3	b	c	a

$e_{k_1}(z) = c$

$\boxed{\begin{array}{l} P_r(k_1) = 1/3 \\ P_r(k_2) = 1/6 \\ P_r(k_3) = 1/2 \end{array}}$

$P_r(x) = 3/8$

$P_r(y) = 1/8$

$P_r(z) = 1/2$

$$P_r(C=c) = \sum_{i \in P} P_r(P=i) \sum_{k : e_k(i) = c} P_r(k=k)$$

$$\boxed{P_r(C=a)} = P_r(P=x) \cdot P_r(k=k_1) + P_r(P=y) \cdot P_r(k=k_2) + P_r(P=z) \cdot P_r(k=k_3)$$

$$= 3/8 \cdot 1/3 + 1/8 \cdot 1/2 + 1/2 \cdot 1/6 = \boxed{13/48}$$

$P(P=x) \neq P_r(P=x | C=a)$

$$P_r(C=c | P=p) = \sum_{k : e_k(p) = c} P_r(k=k)$$

$\boxed{P_r(C=a | P=x)} = \boxed{1/3}$

not perfectly secure

BAYES' THEOREM

$$\overbrace{P(A|B) \cdot P(B)}^{P(AB)} = \overbrace{P(B|A) \cdot P(A)}^{P(BA)}$$

if $P(A|B) = P(A) \Rightarrow P(B) = P(B|A)$

CRIPTOSYSTEM ABOVE WITH UNIFORM KEY

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

$\Pr(P=x,y,z)$ is arbitrary

$$\forall c \; P(C=c) = \sum_{i \in P} \Pr(P=p_i) \cdot \sum_{k : e_k(i)=c} P(k=k)$$

in our case there is always 1 key that maps i to c for each pair i,c

$$= \sum_{i \in P} \Pr(P=p_i) \, 1/3$$

$$= 1/3 \boxed{\sum_{i \in P} \Pr(P=p_i)} = \boxed{1/3}$$

$$\forall_{p,c} P(C=c \mid P=p) = \sum_{k : e_k(p)=c} P(K=k) = \boxed{1/3}$$