Tutorial IV

30 October 2020 09:43

Historical encryption and perfect secrecy

Formal definition of encryption system

P - set of plaintexts

C - set of ciphertexts

K - set of keys

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

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

$\forall p, k \quad d_k(e_k(p)) = p$

CEASER CRYPTOSYSTEM

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	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	L															A	B

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

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

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

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

$e_k(i) : \quad i + k \mod 26$

$d_k(j) : \quad j - k \mod 26$

POLYBIUS CRYPTOSYSTEM

	A	B	C	D	E
F	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
J	V	W	X	Y	Z

$= |K| = 25!$ keys

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

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

encryption

"CRYPTOLOGY"

C → FC   P →   L →   Y → JD

R → IB   T →   O →

Y → JD   O →   G →

AFFINE CRYPTOSYSTEM

Euclid's algorithm (TUTORIAL V)

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

$K = \{(a,b), \text{ s.t. } a \text{ is invertible mod } 26\}$ $|K| = (12 \times 26)$

a is invertible mod $d \Leftrightarrow \gcd(a,d) = 1$

$a \in \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$

$e_{a,b}(i) = a \cdot i + b \mod 26$

$d_{a,b}(j) = (j - b)\, a^{-1} \mod 26$

MONOALPHABETIC ENCRYPTIONS

EVERY   Y YOU   Y   E R   E   EVERY   E   Y   E

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

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   R → D   N → L

I → V   X → O   E → H

G → R   A → U   H → I

Z → N   S → T   O → N

C → Y   U → G

HILL CRYPTOSYSTEM – NOT MONOALPHABETIC

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

$C = P$

K = Set of all invertible 2x2 (Generally n×n) matrices invertible mod 26

$e_{M_k}(ab) = M_k \begin{pmatrix} a \\ b \end{pmatrix} \mod 26$

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

$\det(M) = d$

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

det(M) must be invertible mod 26 $\gcd(d, 26) = 1$

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

$= 4 - 9 \mod 26$

$M = \begin{pmatrix} x \\ 3\,4 \end{pmatrix}$ $\quad det(\cdot) = 1\cdot 4 - 3\cdot 3 \mod 26$

$= 4 - 9 \mod 26$

$= -5 \mod 26$

$= 21 \mod 26$ ✓

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

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

$21 \cdot 5 = 105 \mod 26$

$= 104 + 1 \mod 26$

$= 26 \cdot 4 + 1 \mod 26$

$= 1 \mod 26$

$a \cdot 1 + b \cdot 3 = 1$

$3a + 4b = 0$

$c + 3d = 0$

$3c + 4d = 1$

$\rightarrow$

$a = 1 - 3b = -32 = \underline{20} \mod 26$

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

$-5b + 3 = 0 \quad | \cdot -1$

$5b - 3 = 0$

$5b = 3 \quad | \cdot 5^{-1} = 21$

~~$b = 3/5$~~

$b = 63$

$= \underline{11} \mod 26$

$c = 11$

$d = 5$

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

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

$M^{-1} \begin{pmatrix} 6 \\ 8 \end{pmatrix} = \begin{pmatrix} 20 & 11 \\ 11 & 5 \end{pmatrix} \begin{pmatrix} 6 \\ 8 \end{pmatrix} = (0\ 2)$

$M \begin{pmatrix} 2 \\ 0 \end{pmatrix} = (2\ 6)$ $\quad$ CA → CG

VIGENÉRE CRYPTOSISTEM

Key = arbitrary word of length L

example key = 'KEY'

KEYKEYKEY K

p, key of CEASAR

C + K = M $\quad$ Y + Y $\quad$ W

2 + 10 = 12 $\quad$ 24 + 24 = 22 mod 26

example key - KEY

KEYKEYKEYK
+ CRYPTOLOGY
MVW I

C+K = M — 2+10 = 12
R+E = V — 17+4 = 21

Y+Y = W — 24+24 = 22 mod 26
P+K = I — 24+10 = 34=8 mod 26

How to guess the length of the key?

KASISKI'S METHOD

if a subword is repeated in the ciphertext in intervals that are a multiple of t, then guess t as the length of the key

i: XYZ — $i+10$: XYZ — $i+25$: XYZ — $i+30$: XYZ

intervals: 10, 15, 5

guess

$K=5$

FRIEDMANN METHOD

n - number of symbols in the ciphertext

n_i - number of symbols 'i' in the siphertext

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

PERFECT SECRECY

Intuitively, secure encryption should hide statistical properties of plaintext. (otherwise cryptoanalysis is "easy")

$Pr(P)$ - underlying probability of plaintexts (frequencies of letters in language)

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

$Pr(C)$ – probability of sending ciphertexts

$\Rightarrow$ Can be calculated from e_k, $Pr(P)$, $Pr(k)$

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

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

Perfect secrecy

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

Decide whether a cryptosystem is perfectly secure?

Example:

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

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

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

e_k	x	y	z
→ k_1	a	b	c
k_2	c	a	b
k_3	b	c	a

$e_{k_1}(z) = c$

$Pr(k_1) = 1/3$ $\quad Pr(x) = 3/8$

$Pr(k_2) = 1/6$ $\quad Pr(y) = 1/8$

$Pr(k_3) = 1/2$ $\quad Pr(z) = 1/2$

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

$$Pr(C=a) = Pr(P=x) \cdot Pr(K=k_1) + P(P=y) \cdot Pr(K=k_2) + Pr(P=z) \cdot Pr(K=k_3)$$

$$+ Pr(P=z) \cdot Pr(K=k_3)$$

$$= 3/8 \cdot 1/3 + 1/18 \cdot 1/2 + 1/2 \cdot 1/6 = \boxed{13/48}$$

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

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

NOT PERFECTLY SECURE

$$\forall_{x,y}\ P(P=x) = P(P=x \mid C=y) \iff \forall_{x,y}\ P(C=x) = P(C=x \mid P=y)$$

Bayes' theorem

$$P(A \mid B) \cdot P(B) = P(B \mid A) \cdot P(A)$$

$$\text{if } P(A \mid B) = P(A) \Rightarrow P(B) = P(B \mid A)$$

CRYPTOSYSTEM ABOVE WITH

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

$Pr(P=x_{1,2,3})$ is arbitrary

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

in our case only single key maps each i to c

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

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

($\sum_{i \in P} Pr(P=i) = 1$)

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

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

$$= Pr(K=k \mid e_k(p) = c)$$

$$= 1/3$$

Perfect cryptosystem