Historical encryption and $\boxed{\text{Perfect secrecy}}$

Formal definition of encryption system.

P - set of plaintexts

C - set of ciphertexts

K - set of keys

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

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

$$\forall_{p,k} \quad d_k(e_k(p)) = p$$

EXAMPLE:

CEASAR 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	.	.																			A	B

$\leftarrow k=2$

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

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

$$K = \{0, \dots, 25\} = \{\overset{0}{A}, \overset{1}{B}, \dots, Z\}$$

$$e_k(i): i \to i+k \pmod{26}$$

$$d_k(j): j \to j-k \pmod{26}$$

POLYBIOUS

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

$= K = 25!$ keys

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

"CRYPTOLOGY"

C → EC   P →   L →   Y → JD

R → 1B ...   T →   O →

Y → JD   U →   G →

AFFINE CIPHER

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

$K = \{(a,b),\ \text{s.t. } a \text{ is invertible mod } 26\} \setminus \{(1,0)\}$ ✓ ⇑ because of Euclid algorithm (Tutorial V)

When is a invertible mod d? $\iff \gcd(a,d) = 1$

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

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

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

MONOALPHABETIC ENCRYPTIONS ↑

they map letters to letters, in whole ciphertext same plaintexts are represented by the same ciphertexts.

EVERYDAY YOU Y EVERY Y
WIWGC RYC CXA VYC VYMW LGXUGWOO. WIWGC OSWL VYC QW BGAHSBAN.
YOU AN
CWS SEWGW DHNN OSGWSPE XAS QWBXGW CXA YZ WIWG–NWZUSEWZHZU,
EVER EVER YOU YOU NEVER
WIWG–YOPWZRHZU, WIWG–HVLGXIHZU LYSE. CXA MZXD CXA DHNN ZWIWG
O
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   X → O   Y → A

I → V   A → U

G → R   R → D

C → Y

Z → N

HILL CRYPTOSYSTEM (NOT MONOALPHABETIC)

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

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

$C = P$

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

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

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

$$\boxed{\begin{aligned} \det(M) &= d \\ \det(M^{-1}) &= \frac{1}{d} \end{aligned}}$$

$\gcd(d, 26) = 1$

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

$= 4 - 9 \mod 26$

$= -5 = 21 \mod 26$

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

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

$a + 3b = 1$

$3a + 4b = 0$

$c + 3d = 0$

$3c + 4d = 1$

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

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

$-5b = -3 \quad | :-1$

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

$b = 63$

$= 11 \mod 26$

$\rightarrow c = 11$

$d = 5$

$5^{-1} \mod 26$

$5 \cdot 21 = 105 = 1 \mod 26$

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

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

A C $\rightarrow$ G I

C A $\rightarrow$ C G

CA → CG

VIGENÈRE CRYPTOSYSTEM

key is an arbitrary word (of length L)

example key = "KEY"

Plaintext, key of CAEASAR

KEYKEYKEYK
CRYPTOLOGY
MVW I

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

$2 + 10 = 12$ $\qquad$ $24 + 24 = -2 + -2 = -4 = 22 \pmod{26}$

$R + E = V$ $\qquad$ $Y + K = I$

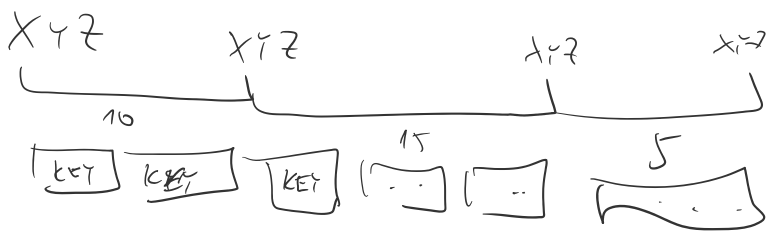
$17 + 4 = 21$ $\qquad$ $24 + 10 = 34 = 8$

M V W

How to guess the length of the key?

KASISKI'S METHOD

if a sub word is repeated in the cyphertext in intervals that are a multiple of ℓ guess ℓ as the key length



FRIEDMANN METHOD

n – number of symbols in the ciphertext

n_i – number of symbols i in the cyphertext

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

PERFECT SECRECY

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

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

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

$Pr(C)$ ~ probability of sending ciphertexts c

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

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

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

PERFECT

$$\boxed{\forall p, c} \quad \boxed{Pr(P=p) = Pr(P=p \mid C=c)} \; \not\forall$$

Decide whether cryptosystem with e_k given by a table, is Perfectly Secure

	X	Y	Z
k_1	a	b	c
k_2	b	c	a
k_3	c	a	b

← P

↑ K

$$e_{k_2}(Y) = c$$

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

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

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

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

$$Pr(C=a) = Pr(P=X) \cdot Pr(K=k_1) + Pr(P=Y) \cdot Pr(K=k_3) + Pr(P=Z) \cdot Pr(K=k_2)$$

$$\frac{3}{8} \cdot \frac{1}{3} + \frac{1}{8} \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{6}$$

$$= 13/48$$

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

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

$$\boxed{\Pr(C=a) \neq \Pr(C=a \mid P=x)}$$

BAYES' THEOREM

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

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

CRYPTOSYSTEM $\mathcal{P}$ with

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

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

in our case sum over 1 element

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

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

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

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

$$= 1/3$$

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

$\forall c, p$

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

$$= 1/3$$

PERFECT CRYPTOSYSTEM!