principles of cryptography
Algorithms and Formulas

Find GCD(a, b)

Q	A	B	R
Q1	A1	B1	R1
	B1	R1	

Euclids Algorithm
method-2 for GCD

a > b

Euclid_GCD (a, b):
if b = 0
return a
else
return Euclid-GCD(b, amodb)

Find GCD(a, b)
if a > b

$GCD(a,b) = GCD(b, a \bmod b)$

Relatively prime numbers:
They should have no prime factors in common.
only common factor is 1

$GCD(a,b) = 1$

a and b are relatively prime numbers

Fermat's Little Theorem

'p' is prime number and a is +ve number integer not divisible by 'p'

$a^{p-1} = 1 \pmod p$

Euler's theorem

$a^{\phi(n)} = 1 \bmod n$

a, n are relatively prime

primitive Root

'α' is a primitive root of prime numbers p if $\alpha \bmod p, \alpha^2 \bmod p, \alpha^3 \bmod p \ldots \alpha^{p-1}$ are distinct

$n \neq a = \{1 \ldots a\}$

$\alpha \bmod p, \alpha^2 \bmod p$

∴ α is P.R.

Multiplicative Inverse using Euclids Algo

Q	A	B	R	T_1	T_2	T
				0	1	
1						1
①	X	X	6	T_1	X	X

$T = T_1 - T_2 \times Q$

T_1 is multiplicative inverse

At initial $T_1 = 0$ $T_2 = 1$

Euler Totient Function

	criteria of 'n'	formula
$\phi(n)$	'n' is prime	$\phi(n) = (n-1)$
	$n = p \times q$ 'p' and 'q' are primes	$\phi(n) = (p-1)(q-1)$
	$n = a \times b$ either 'a' or 'b' is composite Both 'a's 'b' are composite	$\phi(n) = n \times (1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots$

The chinese Remainder Theorem

$x = a_1 \pmod{m_1}$
$x = a_2 \pmod{m_2}$
$x = a_3 \pmod{m_3}$

$$x = \sum_{i=0}^{n} (a_i M_i M_i^{-1})$$

Given			To Find		
$a_1 =$	a_2	a_3	M_1	M_1^{-1}	M
m_1	m_2	m_3	M_2	M_2^{-1}	
			M_3	M_3^{-1}	

$M = m_1 \times m_2 \times m_3$

$M_1 = \frac{M}{m_1}$ $M_2 = \frac{M}{m_2}$

$M_3 = \frac{M}{m_3}$

finding inverse
$M \times M^{-1} = 1 \bmod m$,
Trial & error.

Ceaser cipher

$C = E(P, K) \bmod 26$
$= (P + K) \bmod 26$
$P = D(C, K) \bmod 26$
$= (C - K) \bmod 26$

here K = 3

$C = (P+3) \bmod 26$
$D = (C-3) \bmod 26$

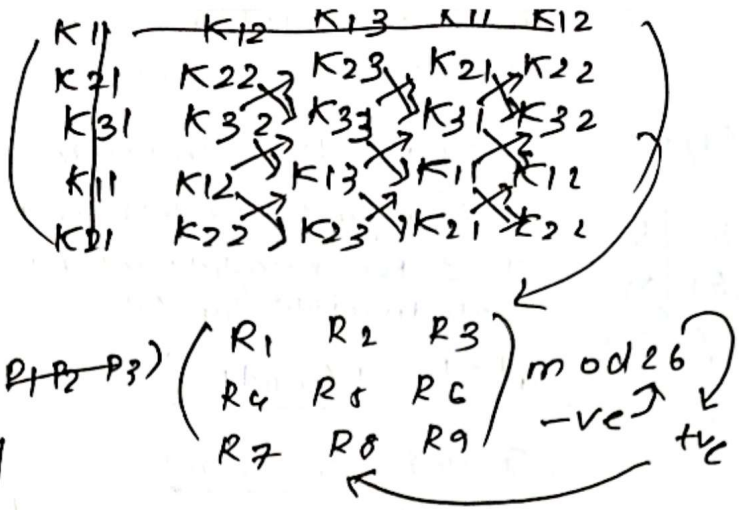
shift cipher

A ceaser cipher is a special case of ~~ceas~~ shift cipher

Play-Fair cipher

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

5×5 matrix



Keyword is keywood

same column ↓ wrap

same row → wrap

Rectangle ⇄ swap

polyalphabetic cipher

Encryption

$C_i = (P_i + K_i \bmod m) \bmod 26$

$P_i = (C_i - K_i \bmod m) \bmod 26$

Transposition Techniques

Hill cipher * imp

$C = E(K, P) = PXK \bmod 26$

where K is a key matrix

$$K = \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \bmod 26$$

For Decryption

$P = D(K, C) = CK^{-1} \bmod 26$

$= PXKK^{-1} \bmod 26$

~~Key : P1 P2~~

plaintext $(P_1\ P_2\ P_3)$

ciphertext $(C_1\ C_2\ C_3)$

$$K^{-1} = \frac{1}{\det K} \times \text{adj} K$$

$$\therefore (C_1\ C_2\ C_3) = (P_1\ P_2\ P_3) \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \bmod 26$$

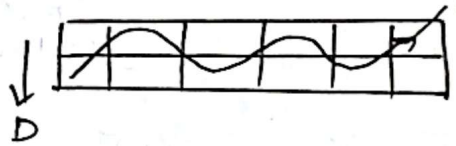
~~polyalphabetic cipher~~

$$\begin{pmatrix} K_{11} & K_{12} & K_{13} & K_{11} & K_{12} \\ K_{21} & K_{22} & K_{23} & K_{21} & K_{22} \\ K_{31} & K_{32} & K_{33} & K_{31} & K_{32} \end{pmatrix}$$

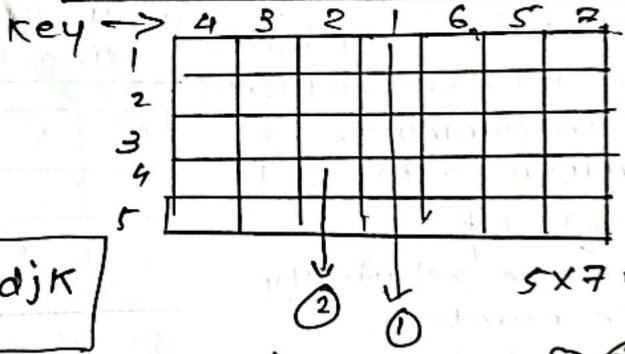
↓

Rail Fence Technique

Depth : D



Row-column Transposition



Ciphertext ①, ②, ③ ... ⑥ this manner