ation)

① Security Management / Risk Management

② Access Control System & Methodology

③ Access levels

↳ ① Verification ② Authentication ③ Access Control List

③ Telecommunication & Network Security

④ Cryptography

① Symmetric (shared secret key)

② Asymmetric
public key — encryption
private key — decryption

① Ceasar Cipher

Plain Text :- meet me after toga party

Cipher Text:-

② Using Modular Math

$C = E(3,P)$	C → Cipher Text
$= (P+3) \bmod 26$	E → Encryption
$P = D(k,C)$	key = 3, k ⟶ key
$= (C-k) \bmod 26$	P → Plain, Text
	D → Decryption

③ ~~CT~~ S Ceasar Cipher (ROT-13)

A	B	C	D	. . .	M
↕	↕	↕	↕		↕
N	O	P	Q	. . .	Z

P.T = hello

C.T = URYYB

Brute Force Attack: Try all possible combination to decrypt the encrypted text (C.T)

④ Substitution (Monoalphabetic)

A = B ⟶ k = +1

B = V ⟶ k = +20

C = G ⟶ k = +4

D = Q ⟶ k = +13

r ⟶ remainder.

The Division Algo: $a = qn + r$ $\quad r = a - qn$

⑤ With keyword

Keyword : KEYWORD → It can be any word which include non-repeatable alphabet

P.T →	A	B	C	D	E	F	G	H	I	J	K	L	M...
	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
C.T →	K	E	Y	W	O	R	D	A	B	C	D	E	F...

P.T : alkindi CT : KGFBIWB

⑥ Homophone Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	
D 9	X	S	F	Z 2 I	E	H	C	V	I	T	P	G	A 5	Q 0	L	K	J	R 4	U 6	

U	V	W	X	Y	Z
↕	↕	↕	↕	↕	↕
O	W	M	Y	B	N

C.T → F7E25F UC2 IDR6 MQPD ØF SD4UP1

P.T → Defend the east wall of castle

⑦ Playfair Cipher (Digraph substitution Cipher)

keyword = MONARCHY

→ Matrix 5x5

→ I/J => Replacement

→ Repeating letter (x) Filler letter

→ ~~if 2 pairs use "x"~~

or "2"

→ if 2 alphabet comes repeating then use 'x' b/w them

eg Hello → He l(x) lo

PT : instruments(x) ← use x to complete pair

GA TL MZ CL RQ XA

⑧ Hill Cipher

msg → act Order of Matrix => n = 3

key → gybnqkurp => 9 alphabet
3×3

Encryption:

$C = kP \bmod 26$

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} = \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} \bmod 26 = \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix}$$

C.T = PoH

Decryption:

$P = k^{-1} C \bmod 26$

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}^{-1} = \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} = \begin{bmatrix} 260 \\ 574 \\ 539 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$$

P.T → act

$\begin{bmatrix} S \\ H \end{bmatrix} = \begin{bmatrix} 18 \\ 7 \end{bmatrix}$, ...

$\begin{bmatrix} 7 & 8 \\ 4 & 11 \end{bmatrix} \begin{bmatrix} 18 \\ 7 \end{bmatrix} = \begin{bmatrix} 182 \\ 275 \end{bmatrix} \bmod 26$

$\begin{bmatrix} 0 \\ 15 \end{bmatrix} = \begin{bmatrix} A \\ P \end{bmatrix}$

P.T → Short exampk

key → Hill

n = 2 => 2×2 = 4

$\begin{bmatrix} H & I \\ L & L \end{bmatrix} = \begin{bmatrix} 7 & 8 \\ 11 & 4 \end{bmatrix}$

Key matrix

~~Encrypted~~

C.T = APADJIFIWLFJ

Decryption : $k^{-1} c \bmod 26$

$$\begin{bmatrix} 7 & 8 \\ 10 & 11 \end{bmatrix}^{-1} = \frac{\text{Adj. A}}{|A|} \qquad |A| = \begin{vmatrix} 7 & 8 \\ 11 & 11 \end{vmatrix}$$

$$\text{Adj. A} = \begin{bmatrix} 11 & -8 \\ -11 & 7 \end{bmatrix} \qquad |A| = 77 - 88 = -11$$

$$|k| = -4$$

$$k^{-1} = \begin{bmatrix} 11 & -8 \\ -11 & 7 \end{bmatrix} \Rightarrow |k| = -11 \bmod 26$$

$$|k| = 15$$

$$k^{-1} = \frac{1}{15}\begin{bmatrix} 11 & -8 \\ -11 & 7 \end{bmatrix} = 15^{-1}\begin{bmatrix} 11 & -8 \\ -11 & 7 \end{bmatrix} \Rightarrow (15 \times x) \bmod 26$$

$$= x = 7 \Rightarrow 15 \times 7 \bmod 26$$

$$= 15x \bmod 26 = 105 \bmod 26 = 1$$

$$k^{-1} = 7\begin{bmatrix} 11 & 18 \\ 15 & 7 \end{bmatrix} \bmod 26 = \begin{bmatrix} 77 & 126 \\ 105 & 49 \end{bmatrix} \bmod 26$$

$$k^{-1} = \begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix}$$

Decryption

$$\begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix}\begin{bmatrix} 0 \\ 15 \end{bmatrix} = \begin{bmatrix} 330 \\ 345 \end{bmatrix} \bmod 26 = \begin{bmatrix} 18 \\ 7 \end{bmatrix} = \begin{bmatrix} S \\ H \end{bmatrix}$$

$$\begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix}\begin{bmatrix} 0 \\ 3 \end{bmatrix} = \begin{bmatrix} 66 \\ 69 \end{bmatrix} \bmod 26 = \begin{bmatrix} 14 \\ 17 \end{bmatrix} = \begin{bmatrix} O \\ R \end{bmatrix}$$

$$\begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix}\begin{bmatrix} 9 \\ 19 \end{bmatrix} = \begin{bmatrix} 643 \\ 446 \end{bmatrix} \bmod 26 = \begin{bmatrix} 19 \\ 4 \end{bmatrix} = \begin{bmatrix} T \\ E \end{bmatrix}$$

$$\begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix}\begin{bmatrix} 5 \\ 19 \end{bmatrix} = \begin{bmatrix} 543 \\ 442 \end{bmatrix} \bmod 26 = \begin{bmatrix} 19\,23 \\ 0 \end{bmatrix} = \begin{bmatrix} X \\ A \end{bmatrix}$$

$$\begin{bmatrix}25 & 22\\ 1 & 23\end{bmatrix}\begin{bmatrix}22\\ 11\end{bmatrix} = \begin{bmatrix}792\\ 275\end{bmatrix} \bmod 26 = \begin{bmatrix}12\\ 15\end{bmatrix} = \begin{bmatrix}m\\ p\end{bmatrix}$$

$$\begin{bmatrix}25 & 22\\ 1 & 23\end{bmatrix}\begin{bmatrix}5\\ 9\end{bmatrix} = \begin{bmatrix}323\\ 212\end{bmatrix} \bmod 26 = \begin{bmatrix}11\\ 4\end{bmatrix} = \begin{bmatrix}l\\ e\end{bmatrix}$$

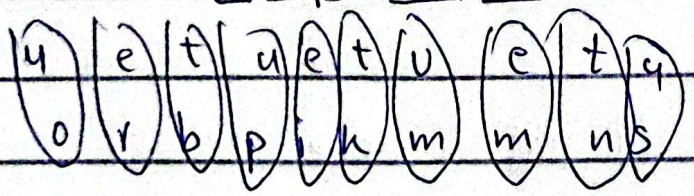
P.T = short example

Wednesday IS 31-1

⑨ Vigenere Cipher

keyword → uet

C.T → orbpikmmns P.T = ?



→ Now look this in vigenere cipher table

Decryption:

UNIVERSITY

⑩ Verman Cipher

P.T →	r	a	m	S	w	a	m	i
P.No →	17	0	12	18	22	0	12	8
key →	r	a	n	g	e	e	l	a
key No. →	17	0	13	6	4	4	11	0
J = PN + kN	34	0	25	24	26	4	23	8
if (J > 26)	-26				-26			
then mod26	8	6	25	24	0	4	23	8
C.T →	I	A	Z	Y	A	E	X	I

⑪ VIC Cipher

- Straddling checkboard → Top Row → [0 – 9]
- Second Row → Popular letters in any order

E S T O N I A R

VIC Cipher: Straddling Checkboard

	0	1	2	3	4	5	6	7	8	9
	E	T	*	A	O	N	*	R	I	S
2	B	C	D	F	G	H	I	K	L	M
6	P	Q	J	U	V	W	X	Y	Z	_

Encryption

P.T → marry queen of scots

m a r r y q u e e n o f s c o t s

29 3 7 67 61 0 0 5 4 23 9 21 4 19

S.T #① Assign alphabet number from straddling table

② Break 2 digit into single digit

2 9 3 7 6 7 6 1 6 3 00

5 4 2 3 9 2 1 4 1 9

③ Add key 1542

2 9 3 7 6 7 6 1 6 3 0 0 5 4 2 3 9 2 1 4 1 9

1 5 4 2 1 5 4 2 1 5 4 2 1 5 4 2 1 5 4 2 1 5 4 2 1 5 4 2

If Result > 10 then (Result mod 10)

3 14 7 9 7 12 10 3 7 8 4 2 6 9 6 5

10 7 5 6 2 14

3 4 7 9 7 2 0 3 7 8 4 2 6 9 6 5 0 7 5

6 2 4

④ Pairing the Result digit

3	4	7	9	7	20	3
A	O	R	S	R	B	A

Decryption:

① Assign numbers to C.T from S.T

② Split double number into single

③ Substract the key

④ Pairing the result digit.

A	O	R	S
3	4	7	9

if value > 10 or value < 10

then mod 10 → -1 mod 10 = 9

-1 5 4 2 2 9 37 => MAR

2 -1 3 7

Transposition (Permutation)

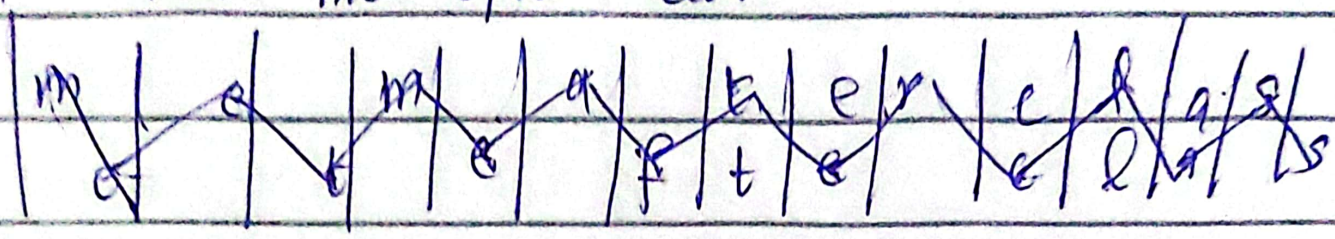
① Scytale Cipher

• write the P.T on a ribbon and then wrap it on a fixed diameter rod. The horizontal straight alphabet well be C.T

② Rail Fence Cipher

depth = 2

P.T → meet me after class



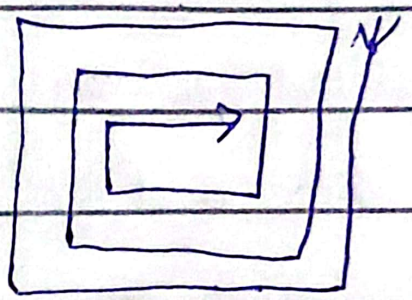
C.T → ME MA TR LS E TE FE CAS

③ Route cipher : → # of colums

key = 6, P.T → i am going to school

i	a	m	g	d	i
n	g	t	o	s	c
h	o	o	l	x	y

filler ~~val~~var



C.T scheme

C.T = l c y x l o o h n i a m g

s o t g

IS

VIC Cipher

Decryption

key = 1542

① Assign numbers to C.T ~~to~~ from S.T

② Split double number into single integer

③ Substract the key

④ Pairing the result digit.

Straddling Checkboard

	0	1	2	3	4	5	6	7	8	9
	E	T	*	A	O	N	*	R	I	S
2	B	C	D	F	G	H	J	K	L	M
6	P	Q		U	V	W	X	Y	Z	_

C.T = AORSRBA

	A		O		R	S	R	B	A	F	A	R	J
①	3	4	~~7~~	9	8	20	3	0	3	17	8		
②	3	4	7	9	7	2	0	3	7	8			
③	1	5	4	2	1	5	4	2	1	5			
	2	-1	3	7	6	-3	-4	1	6	3			

2 9	3 7	6 7	6 1	6 3
* M	A R	* y	* Q	* U

Tuesday IS 13-1

Number Theory

→ **Division algo:**

if 'a' & 'b' → integers $b \geq 1$

then $a = qb + r$

modular form

$$a \equiv r \bmod b$$

$$r = a \bmod b$$

Divisor & GCD

integers a, b, c

$c \mid a$, $c \mid b$ → c is common divisor

GCD (a, b) → greatest largest common divisor

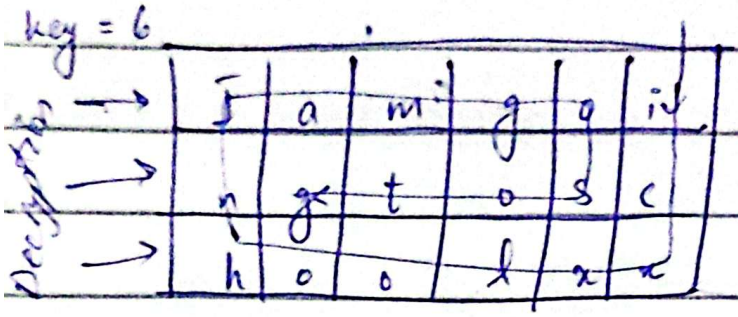
→ Co Prime / Relatively Prime (must)

IS (Homework)

Route cipher

P.T -> I am going to school

key = 6



C.T -> ICXXLOOHNIAMGTOSOTGT

Decryption:

- Make the table with no. of colums equal to key then fill the cipher text according to pattern, then read the text row wise for plain text.

→	I	A	M	G	O	I
→	N	G	T	O	S	C
→	H	O	O	L	X	X

Filler Text

IAMGOING TOSCHOOL

Rail Fence

P.T -> geeks for geeks

- make a table with rows = depth and col = length
- Place the char row wise
- leaving empty spaces for char in rows

Continue...

Congurence

If 'a' & 'b' are integers then 'a' is said to be congurent to 'b' mod m' . if $m | a-b$

m → modulus of congurence

Ex $24 \equiv 9 \bmod 5$ as $5 | 24-9$

$-8 \equiv 5 \bmod 13$ as $13 | -8-5$

Properties

① $a \equiv b \bmod n$ if $n | a-b$

② $a \equiv b \bmod n$ implies $b \equiv a \bmod n$

③ if $a \equiv b \bmod n$ & $b \equiv c \bmod n$ then $a \equiv c \bmod n$

④ $(a+b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$

⑤ $(a-b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$

⑥ $(a*b) \bmod n = [(a \bmod n) * (b \bmod n)] \bmod n$

Repeatire Square Method

→ $11^7 \bmod 13 \Rightarrow 11^{4+2+1} \bmod 13 = 11^4 . 11^2 . 11 \bmod 13$

$11^2 \bmod 13 = 121 \bmod 13 = 4 \bmod 13$

$11^4 \bmod 13 = (11^2)^2 \bmod 13 = 4^2 \bmod 13 = 16 \bmod 13 = 3 \bmod 13$

Now put in $11^4 . 11^2 . 11 \bmod 13$

$= (3 \times 4 \times 11) \bmod 13 = 132 \bmod 13$

$= 2 \bmod 13$

GCD → Greatest Common Divisor

Multiplicative Inverse

- Let $a \in Z_n$ then $a^{-1} \bmod n$ is an integer $x \in n$

i.e: $a.x \bmod n = 1 \bmod n$

→ $a \in Z_n$ is invertable iff $\gcd(a,n) = 1$

Calculating Multiplicative Inverse

Euclidean Algorithm

If 'a' & 'b' are positive integers $a > b$ then

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

Calculate GCD of 4864 & 3458

$4864 = 1.3458 + 1406$

$3458 = 2.1406 + 646$

$1406 = 2.646 + 114$

$646 = 5.114 + 76$

$114 = 1.76 + 38$

$76 = 2.38 + 0$

Extended Euclidean Algorithm (To find inverse)

$ax + by = d$

$4864x + 3458y = 38$

$38 = 114.1 - 76.1$

$38 = 114.1 - [646.1 - 114.5].1$

$38 = 114.1 - 646.1 - 114.5$

$38 = 114.6 - 646.1$

$38 = (1406.6 - 646.2).6 - 646.1$

$38 = 1406.6 - 646.12 - 646.1$

$38 = 1406 - (3458 - 1406.2).13$

$38 = 1406.6 - 3458.13 + 1406.26$

$38 = [4864 - 3458.1]32 - 3458.13$

Tuesday SQE 13-2

Worst case BVT

① (min+, min+) = (1, 2)

② (nominal, min) = (15, 1)

Normal: Nominal + wiwthin

Worst: Corner + within rang

Robust: nominal + out

Robust worst: all

Wednesday IS 14-2

GCD(1025, 35)

Using eclidean algo:

$1025 = 29 \cdot 35 + 10$

$35 = 3 \cdot 10 + 5$

$10 = 2 \cdot 5 + 0$

GCD = 5

① $45(x) + 130(y) = 5$

② $513(x) + 144(y) = 9$

$13^{-1} \bmod 15 = ?$

① → $45x + 130y = 5$

Affine Cipher

- monoalphabetic Substitution Cipher
- each letter encryptes to one letter and back again
- working in mod 'm' (length of alphabets)
- letters are mapped to ~~integrate~~ integers in the range (0 − m−1) → $\{0, \ldots, n-1\} \Rightarrow 0 \ldots 25$
- key consists of two numbers 'a' and 'b'

GCD(1025, 35)

Using eclidean algo:

$1025 = 29 \cdot 35 + 10$

$35 = 3 \cdot 10 + 5$

$10 = 2 \cdot 5 + 0$

GCD = 5

① $45(x) + 130(y) = 5$ | $13^{-1} \bmod 15 = ?$

② $513(x) + 144(y) = 9$ |

① → $45x + 130y = 5$

Affine Cipher

- monoalphabetic Substitution Cipher
- each letter encryptes to one letter and back again
- working in mod 'm' (length of alphabets)
- letters are mapped to ~~integrate~~ integers in the range $(0 - m-1) \longrightarrow \{0, \ldots, n-1\} \Rightarrow 0 \ldots 25$
- key consists of two numbers 'a' and 'b'

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21

W	X	Y	Z
22	23	24	25

- for 26 alphabets 'a' must be reletively prime to 'm'

Encryption

$$C = (ap + b) \bmod m$$

$b \rightarrow 1 \le b \le m$ and $a \rightarrow 1 \le a \le m$, $\gcd(a, m) = 1$

Decryption

$$P = a^{-1}(c - b) \bmod m$$

Example 1

msg → i am a secret

9 0 12 0 18 4 2 17 4 19

$\begin{cases} m = 26 \\ a = 15 \\ b = 7 \end{cases}$

$\Rightarrow$

i → $C = (15 \times 8 + 7) \bmod 26 = 23 \rightarrow X$

~~a → $C = (15 \times 0 + 7) \bmod 26 = 22 \rightarrow W$~~

a → $C = (15 \times 0 + 7) \bmod 26 = 7 \bmod 26 = 7 \rightarrow H$

m → $C = (15 \times 12 + 7) \bmod 26 = 187 \bmod 26 = 5 \rightarrow F$

a → H

s → $C = (15 \times 18 + 7) \bmod 26 = 277 \bmod 26 = 17 \rightarrow R$

e → $C = (15 \times 2 + 7) \bmod 26 = 30 \bmod 26 = 4 \rightarrow E$

e → $C = (15 \times 4 + 7) \bmod 26 = 67 \bmod 26 = 15 \rightarrow P$

r → $C = (15 \times 17 + 7) \bmod 26 = 262 \bmod 26 = 2 \rightarrow C$

e → P

T → $C = (15 \times 19 + 7) \bmod 26 = 292 \bmod 26 = 6 \rightarrow G$

~~GT = XHFHRPECPG~~

$P = a^{-1}(c-b) \bmod m$

Decryption:

$15^{-1} \bmod 26 = ?$

$15 \cdot x = 1 \bmod 26$

$26 = 15 \times 1 + 11$

$15 = 11 \times 1 + 4$

$11 = 4 \times 2 + 3$

$4 = 3 \times 1 + 1$

$3 = 1 \times 3 + 0$

$1 = 4 - 3$

$\therefore 3 = 11 - 4 \times 2$

$1 = 4 - (11 - 4 \times 2)$

$1 = 4 \times 3 - 11$

$\therefore 4 = 15 - 11 \times 1$

$1 = (15 - 11)3 - 11$

$= 15 \times 3 - 11 \times 4$

$\therefore 11 = 26 - 15 \times 1$

$P = a^{-1}(c-b) \bmod m$

$X \rightarrow$

$P =$

$1 = 15 \times 3 - (26 - 15)4$

$1 = 15 \times 7 - 26 \times 4$

$1 = 15 \times 7$

$15^{-1} \bmod 26 = 7$

$15x = 1 \bmod 26$

$x = 7$

9	0	12	0	18	4	2	17	4
J	a	m	a	s	c	r	e	t

Example #1 [Encryption]

① $J \rightarrow (9 \times 15 + 7) \bmod 26 \rightarrow X$

② $a \rightarrow (0 \times 15 + 7) \bmod 26 \rightarrow H$

③ $m \rightarrow (12 \times 15 + 7) \bmod 26 \rightarrow F$

④ $s \rightarrow (18 \times 15 + 7) \bmod 26 \rightarrow R$

⑤ $e \rightarrow (9 \times 15 + 7) \bmod 26 \rightarrow P$

⑥ $c \rightarrow (2 \times 15 + 7) \bmod 26 \rightarrow L$

⑦ $r \rightarrow (17 \times 15 + 7) \bmod 26 \rightarrow C$

⑧ $t \rightarrow (19 \times 15 + 7) \bmod 26 \rightarrow G$

$\therefore$ JAMASCRET = XHFHRPLCPG

Decryption:

$X \rightarrow 7(23-7) \bmod 26 = 8 = I$

$H \rightarrow 7(7-7) \bmod 26 = 0 = a$

$F \rightarrow 7(5-7) \bmod 26 = 12 = m$

$R \rightarrow 7(17-7) \bmod 26 = 18 = s$

$P \rightarrow 7(15-7) \bmod 26 = 4 = e$

$L \rightarrow 7(11-7) \bmod 26 = 2 = c$

$C \rightarrow 7(2-7) \bmod 26 = 17 = r$

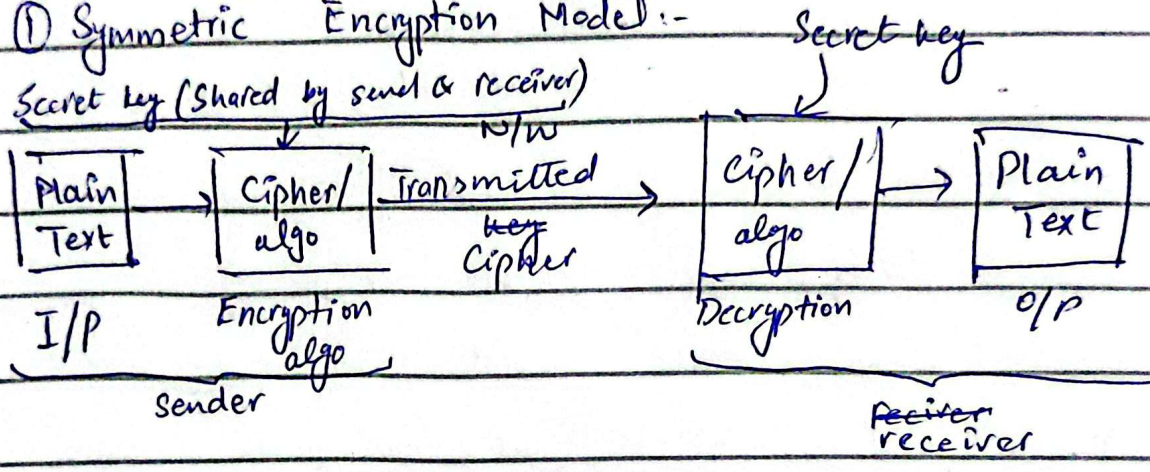
$G \rightarrow 7(6-7) \bmod 26 = 19 = t$

Crypto Dimensions

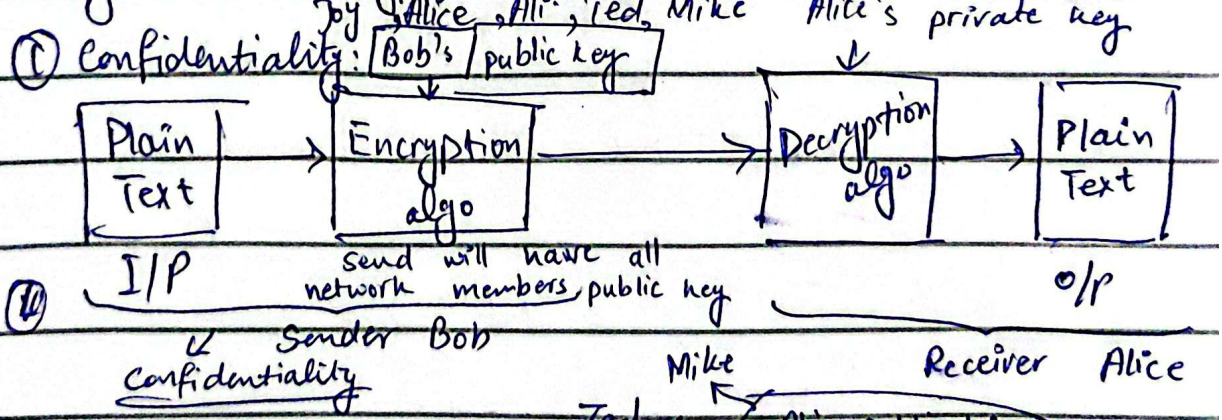
- → Types of Operation ← Substitution, Transposition
- → Number of keys ← Symmetric key, Asymmetric key (Public key)
- → Processing ways ← Block cipher, Stream cipher

Basic Encryption Models:

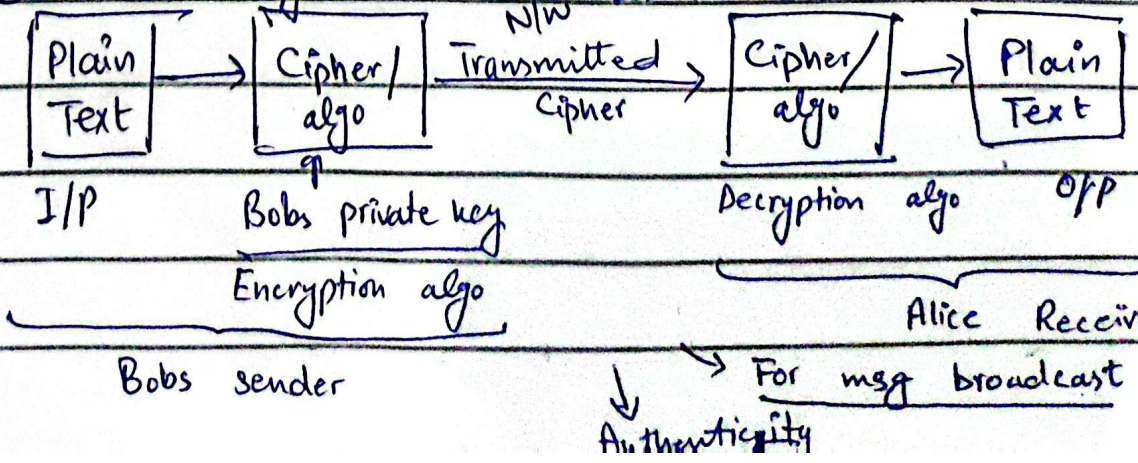
① Symmetric Encryption Model :-



② Asymmetric Encryption Model



② Authenticity:



Secure Symmetric Encryption

1- Strong Encryption algo

2- Saret key

Cryptanalytic Attacks

1. Ciphertext only
2. Known Plain Text
3. Select plain text
4. Choosen cipher text
5. Choosen text

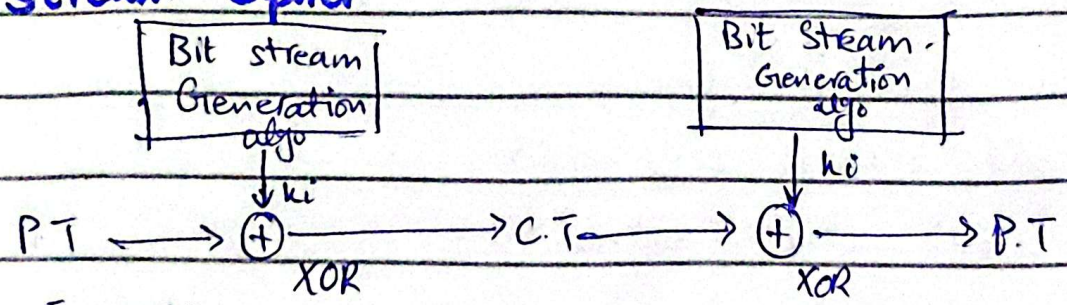
No matter how much resource you have you can't recover plain text from C.T

Unconditional Security

Computational Security

any shortcut which allow recovery of plain text from C.T

Stream Cipher

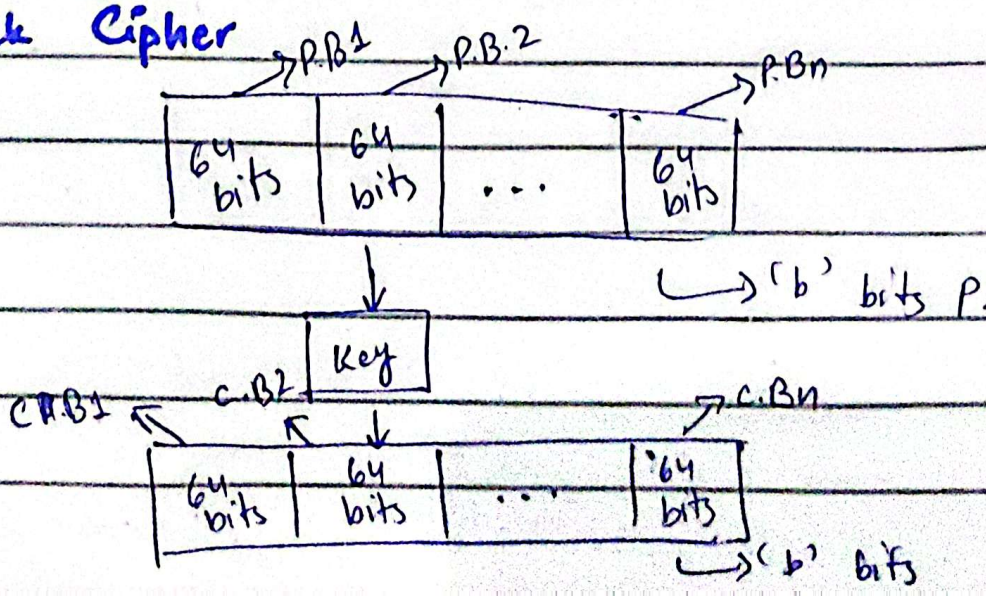


Encryption:-

msg → 1011 0110 XOR → 11100011 XOR → 10110110

key → 0101 0101 01 01 0101

Block Cipher



Block cipher	Stream cipher
→ P.T is grouped in block & then converted to C.T	→ 1 bit / 1 byte of P.T is converted into C.T.
→ uses 64 or more bits	→ 8 bits are used
→ complexity is simple	→ more complex
→ uses confusion & diffusion	→ uses cofusion only
→ algorithmic modes used: ↳ ECB ↳ CBC	→ algorithmic modes used: ↳ CFB ↳ OFB
→ uses transposition	→ uses substitution
→ slower than stream cipher	→ faster
→ ~~Increase~~ Increases the redundency of P.T	→ No redundency
→ requires more code	→ requires less code

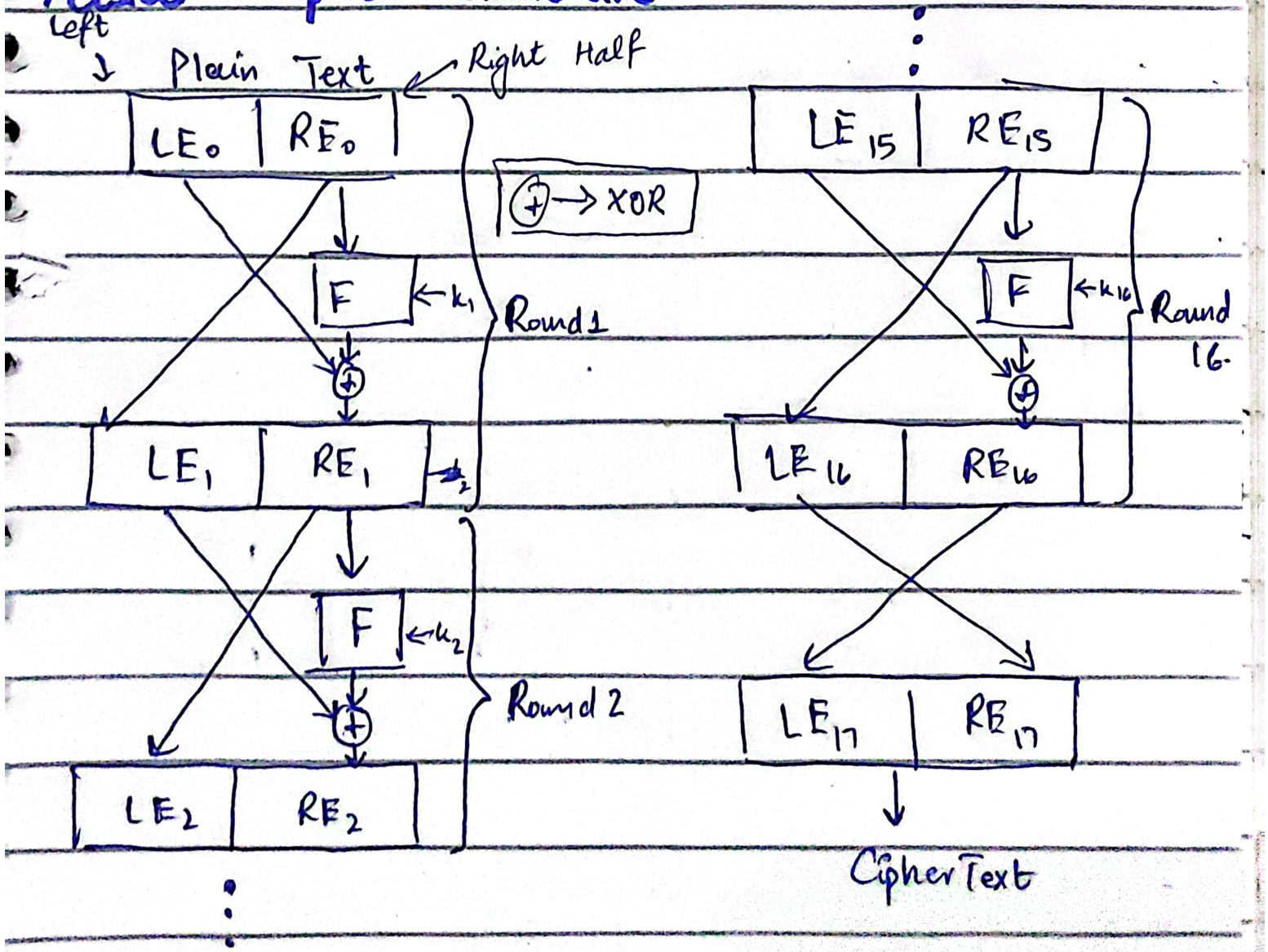
Shannon's Theory of Confusion & Difusion

→ Diffusion → Hide the relationship b/w C.T & P.T

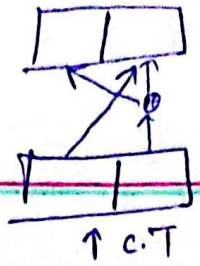
→ Confusion → Hides the relationship B/W C.T & key

21-2 IS Wednesday

Feistal Cipher Structure



Modern cryptography Technique



Block Cipher Design Principles

→ Block Size — 64 bits

→ key size — equal to P.T size → $(k_1, k_2 \ldots k_n)$ key (all keys are all generated from)

→ No. of Rounds — 16 rounds (optimal)

→ Subkey count

→ Round Function

→ Plain Text divided into 2 half.

Data Encryption Standard (DES)

→ Block Cipher

→ Symmetric

→ 64-bit Plain Text Block

→ 16 rounds → ~~each~~

→ each round is a Fiestal round

4-Steps

① Initial Permutation

② 16-Fiestal rounds

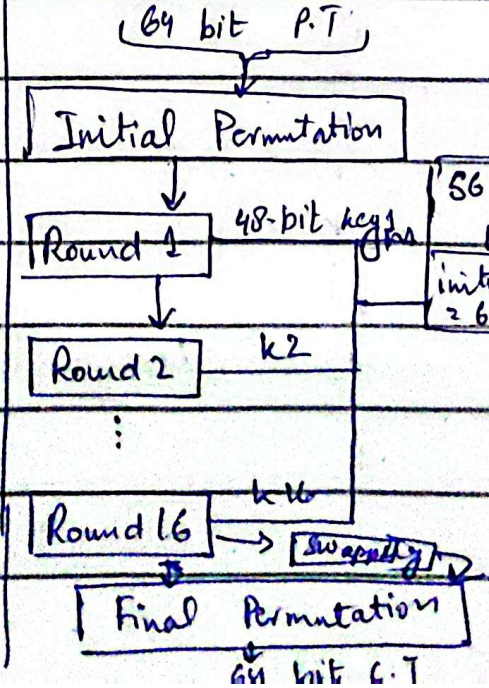
③ Swapping

④ Final Permutation

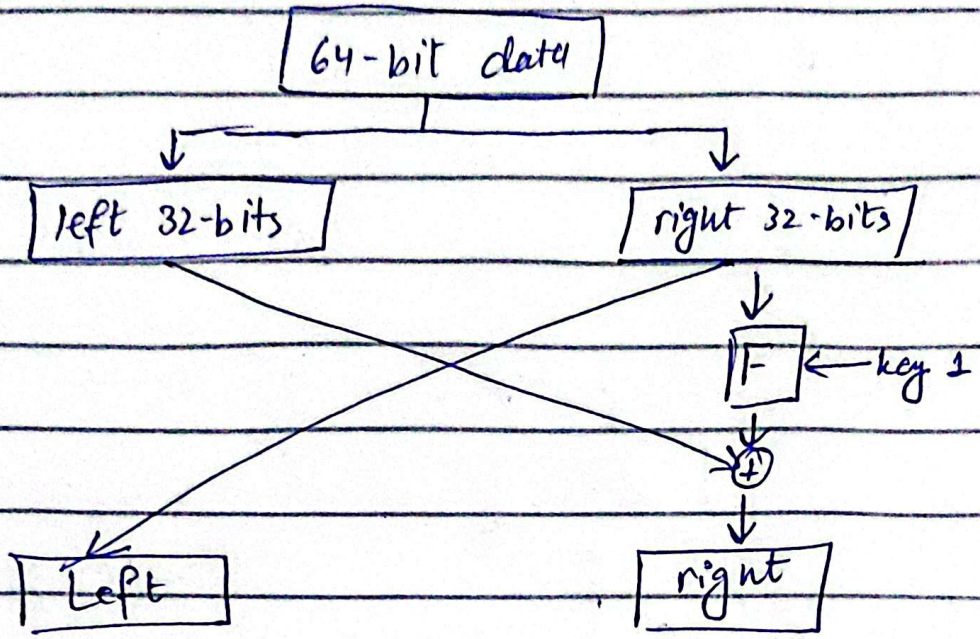
Inverse of initial permutation

56-bit ~~56 bit~~ key is used to extract 48 bit key

Basic Structure

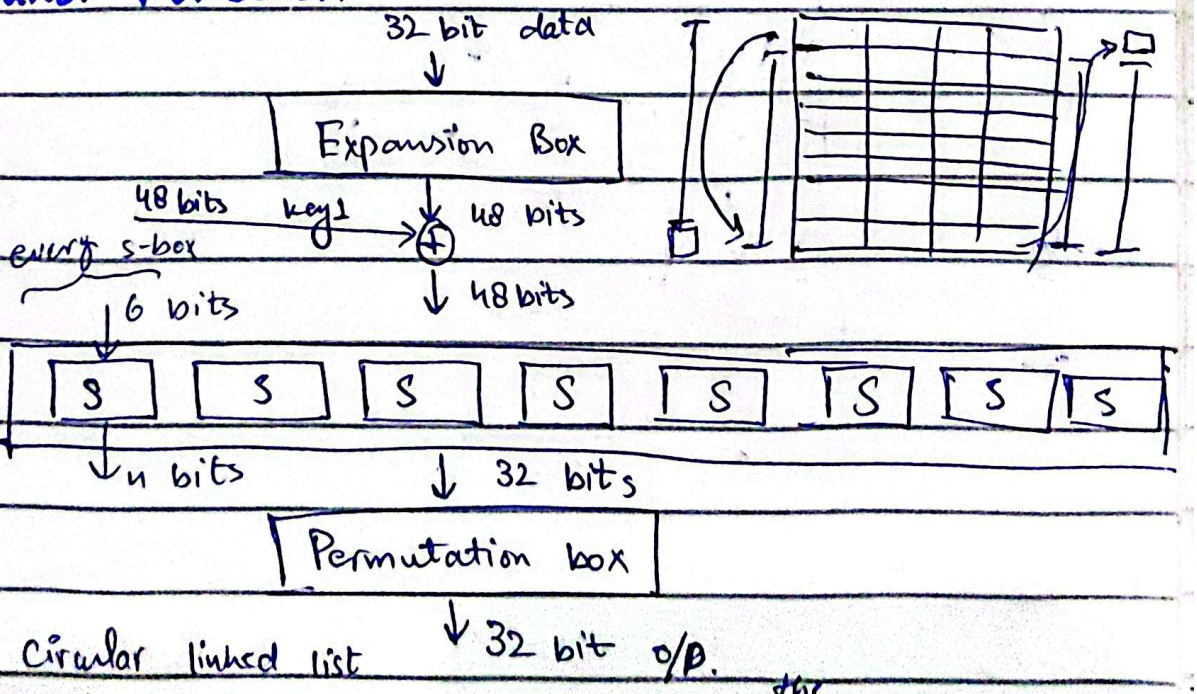


Fiestal Round



1

Round Function



Circular linked list

Expansion box data → dont give the money to that person ever.

R | DONT | GIVE | THEM | ONEY | TO TH | ATPE | RSON

R | DONT G | T | GIVE T | E | THEM O | M | ONEY T | EVER

32 → size

Convert → 48

8 × 6 = 48

S-Box

S-Box → 64 bit → S → 4 bits

S-Table = unique

0 1 2 3 0 .. 15

1 5 7 . .

Random no.

row = 01

00 1011 → 0101

00 0000

01

10

11

row → 01 → 1

col → 0101 → 5

→ bits

1 2 3 4 5 6 7 8

1 0 1 1 0 1 0 1

Discard

64 key → 8×8 blocks

PC-1

7 bits × 8

i = 1, 2, 9, 16

56

shift key 1

else

shift key 2

rotate left

C_0 | D_0

28 28

Shift | Shift

28 28

C_1 | D_1

56 → PC-2 → 48 bits key 1

28 28

Shift | Shift

C_{16} | D_{16}

PC-2 56 → 48

C1 → 28 bits → (1-28)

D1 → 28 bits → (29-56)

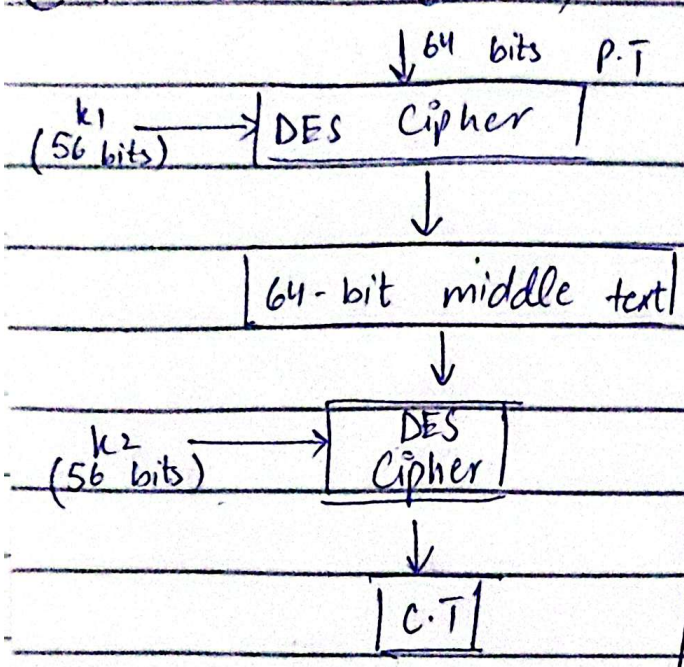
left half C1 → 9, 8, 22, 25 → 24

Right half C2 → 35, 38, 43, 54 → 24

} 48 bits

Multiple DES

① Double DES (2 DES)



Encryption: $C.T = E(k_2, E(k_1, P))$ (key2, key1)

Decryption: $P.T = D(k_1, D(k_2, C\bar{T}))$ (key1, key2)

single DES

Problems:

DES | Brut force attack

key = 64 bits

effective 64-8 = 56 bits

2^{56} keys

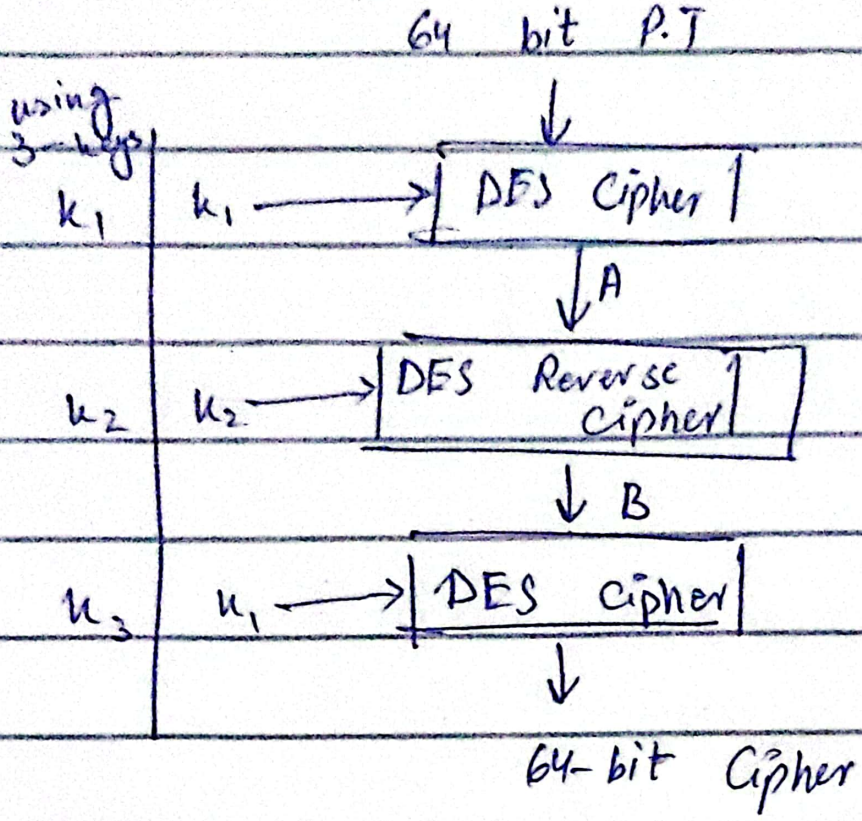
Meet-in-the-middle Attack

key	P.T	Middle Cipher	key	C.T	Middle Cipher
1	XX X →	—	1	Y Y Y →	—
2	→	—	2	→	—
⋮	⋮	⋮	⋮	⋮	⋮
56		—	56		—

- There will be one pair where both Middle Cipher will match, from there we can identify key 1 and key 2

$$X = E(k_1, P) = D(k_2, C)$$

② Tripple DES (3 DES) — using 2 key method



3DES - using 3 key method

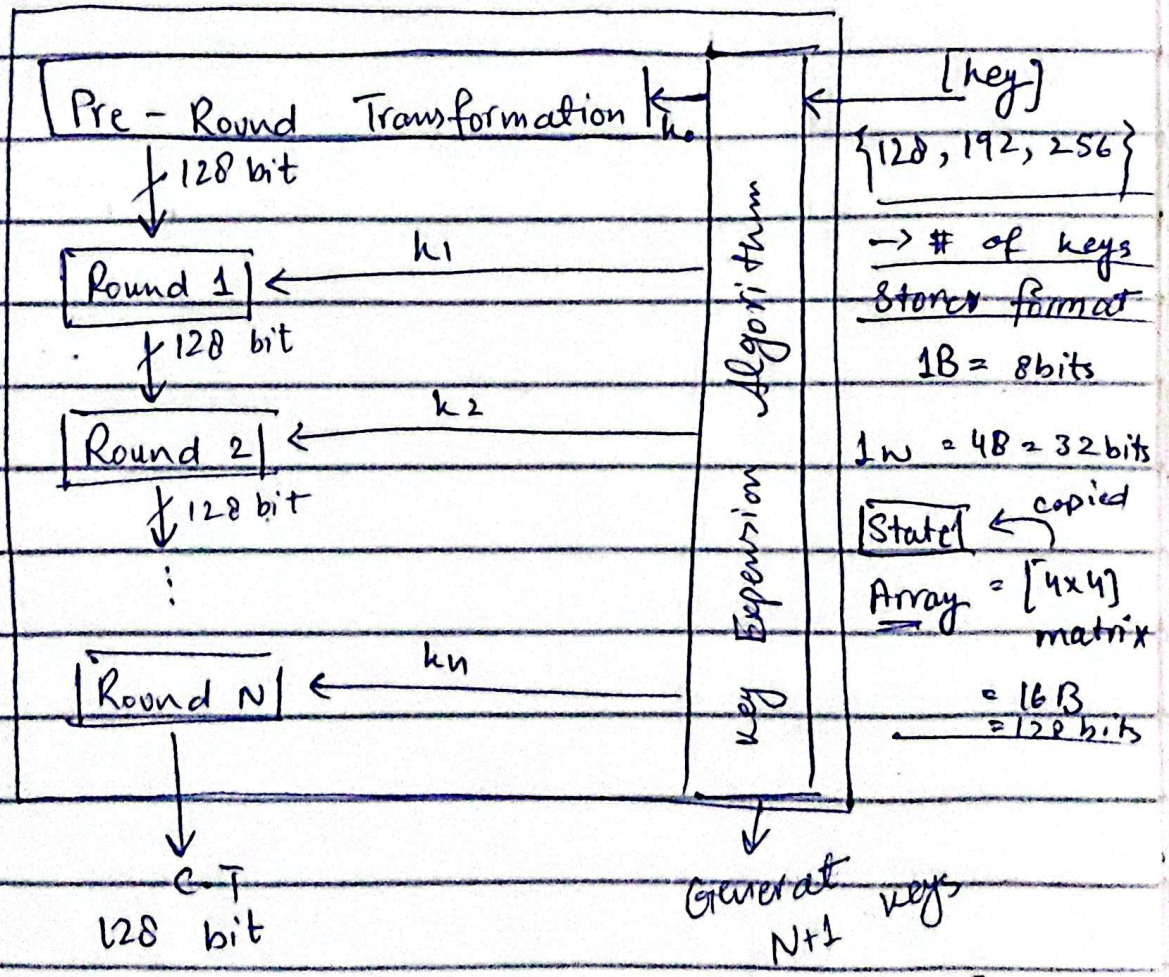
$$C = E(k_3, D(k_2, E(k_1, P)))$$

$$P = D(k_1, E(k_2, D(k_3, C)))$$

Advanced Encryption Standard (AES)

	Rounds	# of bits in key
Version 128	10	128
Version 192	12	192
Version 256	14	256

General Structure



⇒ 128 bit block input is depicted as a 4x4 square matrix of bytes. This block is copied into the State array which is modified at each stage.

Input → State Array → Output

Input Array

in_0	in_4	in_8	in_{12}
in_1	in_5	in_9	in_{13}
in_2	in_6	in_{10}	in_{14}
in_3	in_7	in_{11}	in_{15}

4 × 4 = 16B = 128 bits

State Array

w_0	w_1	w_2	w_3
$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$

→ 3rd Byte of 1st word

→ $[w_0, w_1, w_2, w_3]$

Key

128 bits - 4 words [1 key]

k_0	k_4	k_8	k_{12}
k_1	k_5	k_9	k_{13}
k_2	k_6	k_{10}	k_{14}
k_3	k_7	k_{11}	k_{15}

key expansion algo → w_4 w_5 ... 44 words

Generate: 44 words [11 keys]

Round Structure

PT (128 bits)

Pre-Round Transformation ← $k_0 [w_0 - w_3]$

key (128) → key expansion algo

4×4 matrix ↓ PT (128 bits)

1 → Substitution bytes

2 → Shift rows

3 → mix column

4 → add round key ← $k_1 [w_4 - w_7]$

Round 1

4 Transformation

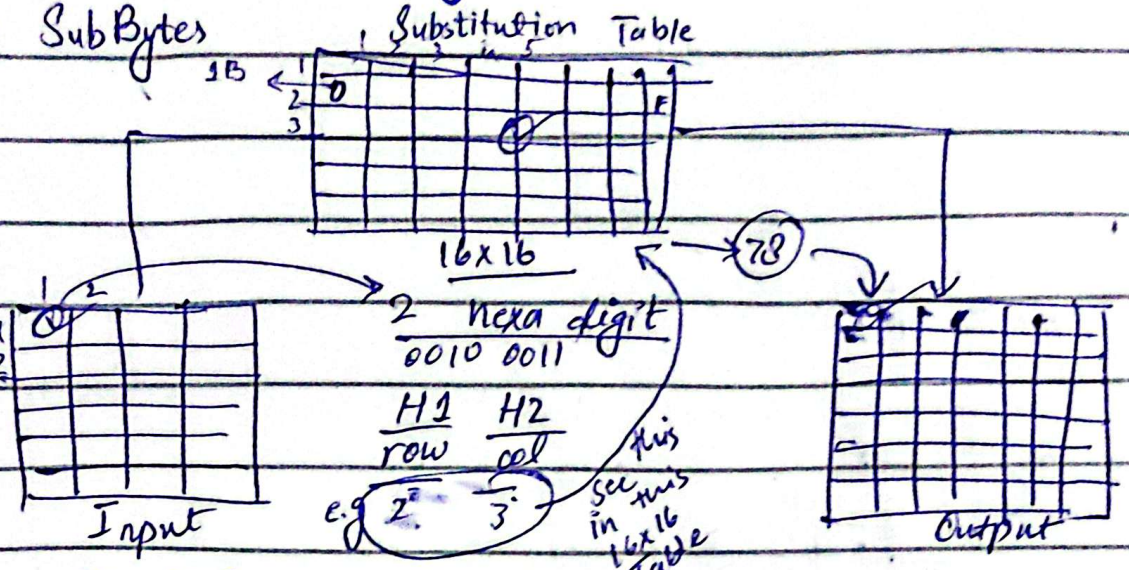
N - 1 Rounds

For [R1 - R9] => 4 Transformation

For [R10] => 3 Transformation [3rd is not part]

1- Substitution Bytes Transformation

- SubBytes



2- ShiftRows Transformation

R_0	63	C9	FE	30	→ Not altered
R_1	F2	F2	63	26	→ 1-byte circular shift
R_2	C9	C3	7D	D4	→ 2-byte circular shift
R_3	BA	63	82	D4	→ 3-byte circular shift

↓ Shit to left by Row #

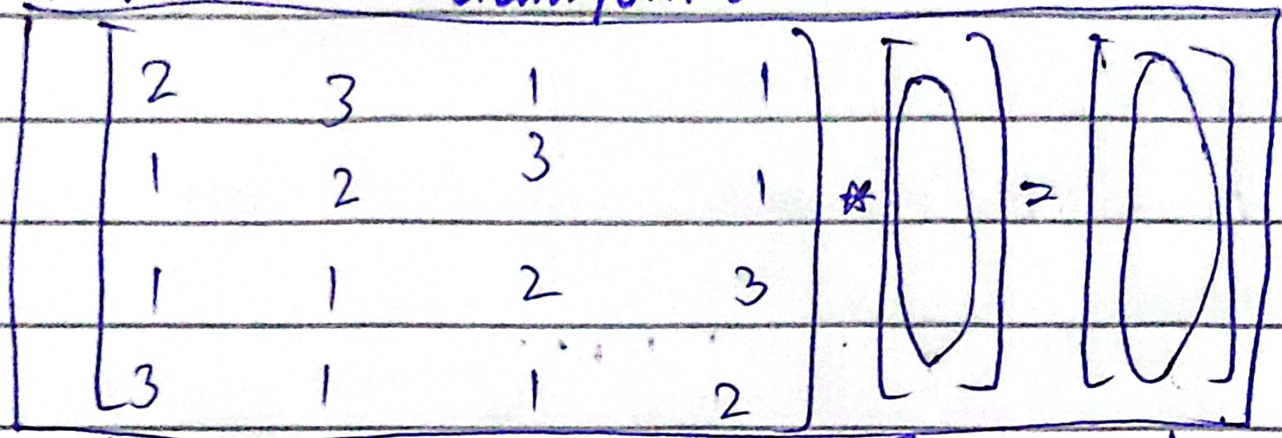
63	C9	FE	30
F2	63	26	F2
7D	D4	C9	C3
D4	BA	63	82

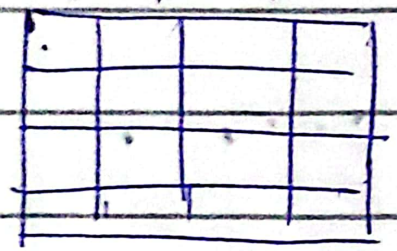
87	F2	4D	97
EC	6E	4C	90
4A	C3	46	E7
8C	D8	95	A6

→

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

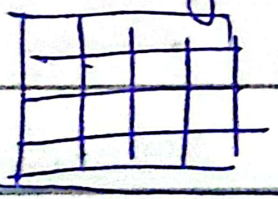
3/1.3- Mix column transformation

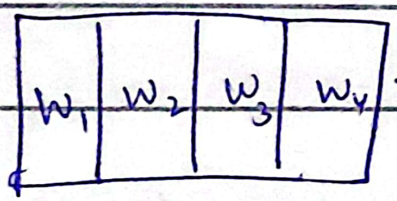


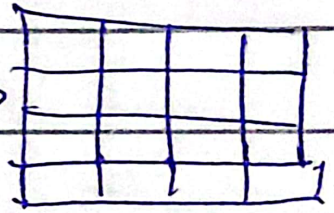


4/1 key adding

Round key







Block Cipher Mode of Operation

- Every block is encrypted independently.

① Electronic Code Block Mode (ECB)

② Cipher block chaining mode (CBC)

IV → Initialization vector

↳ sender/receiver agree upon one single

③ Cipher Feedback Mode (CFM)

④ Output Feedback Mode (OFM)

⑤ Counter Mode

↳ Counters (1 ... N) - Counter blocks have values

RC4 Algorithm

- ~~RP6A~~ - Stream cipher

① key scheduling ② key stream generation

③ Encryption & Decryption

S[i] → State Vector (256 bits)

T[i] → key vector / Temporary array

S = [0 1 2 3 4 5 6 7] for → size 256 bits

key array = [1 2 3 6]

P.T → [1 2 2 2]

T = [1 2 3 6 1 2 3 6]

key

↳ created from key array and same size

① KS - key scheduling

No. of iterations = size of S-array

j = 0

for i = 0 to 255

do

j = [j + S(i) + T(i)] mod 256

swap (S[i], S[j])

② SG - key stream generation

No. of iterations = size of key

i, j = 0

while (True)

i = (i+1) mod256

j = (j + S[i]) mod256

Swap [S(i), S(j)]

t = (S[i] + S[j]) mod256

ki = S[t]

③

Encryption → P.T ⊕ New key

Eular's Tailent Function (Eular's Phi function)

→ $\boxed{\phi(n) = n-1}$

→ no. of +ve integers less than "n" that are co-prime to "n", where $(n > 1)$

Ex

$\boxed{\phi(1) = 1}$
$\boxed{\phi(5) = ?}$

No. < 5 are → 1, 2, 3, 4

GCD (1,5) = 1

GCD (2,5) = 1 ⇒ $\phi(5) = 4$

GCD (3,5) = 1 $\phi(6) = ?$

GCD (4,5) = 1

P1 if 'n' in prime then $\boxed{\phi(n) = n-1}$

P2 $\phi(a*b) = \phi(a) * \phi(b)$

P3 $\phi(p^n) = p^n - p^{n-1}$

Eular's Toient Theorem:

if 'x' & 'n' and positive co-prime integers then $\boxed{x^{\phi(n)} \equiv 1 \bmod n}$

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

Ex $x = 11$, $n = 10$

$11^{\phi(10)} = 1 \bmod 10$

$\therefore \phi(10) = \phi(2) * \phi(5)$

$= 1 * 4 = 4$

$\Rightarrow 11^4 = 1 \bmod 10$

$1461 = 1 \bmod 10$

$1461 \% 10 = 1$

P: $x^{\phi(n).Q} \equiv 1 \bmod n$

Ex: $11^{4*2} \equiv 1 \bmod 10$

$2143588881 \equiv 1 \bmod 10$

Ex:

$11^{40} \equiv 1 \bmod 10$

GCD (1,6) = 1

(2,6) = x

(3,6) = x

(4,6) = x

(5,6) = 1

Ex: $4^{99} \bmod 35 = 29 \bmod 35$

$x = 4$, $n = 35 \rightarrow$ co-prime

By Eular's Theorem:

$4^{\phi(35)} = 1 \bmod 35$

$\therefore \phi(35) = \phi(7) * \phi(5)$

$= 6 * 4 = 24$

$\Rightarrow 4^{24} = 1 \bmod 35$

$4^{99} \rightarrow 4^{(24)4+3}$

$= (4^{24})^4 \bmod 35.$

$.4^3 \bmod 35$

$= 1.4^3 \bmod 35$

$= 64 \bmod 35$

$= 29$

gcd(302, 3)

$302 = 3 \times 100 + 2$

$3 = 2 \times 1 + 1$ →

$2 = 1 \times 2 + 0$ ←

Ex: $3^{302} \bmod 13 \rightarrow 3$

$x = 3$, $n = 302 \rightarrow$ co-prime

$3^{\phi(302)} = 1 \bmod 302$

$\phi(302) = \phi(151) * \phi(2)$

$= 150 * 1 = 150$

$= 3^{150} \bmod 302$

~~$= (3^{10})^{15} \bmod 302$~~

~~$= (3^5 \times 3^2)^{10} \bmod 302$~~

2

Fermat's Theorem

→ Specific case of eular's theorem, where 'n' is prime no.

→ If 'n' is prime and 'x' is +ve integer not divisible by 'n', then

$$x^{n-1} \equiv 1 \bmod n$$

$$x^n = x \bmod n$$

Ex

$x = 3, n = 5$

$3^{5-1} = 1 \bmod n$

$3^4 = 81 = 1 \bmod n$

$x^n = x \bmod n$

$3^5 = 3 \bmod 5$

$243 = 3 \bmod 5$

$243 \,\%\, 5 = 3$

Ex

$4^{332} \bmod 11$

$x^{n-1} \equiv 1 \bmod n$

$x = 4, n = 11$

$4^{n-1} = 1 \bmod 11$

$4^{10} = 1 \bmod 11$

$4^{332} = 4^{10(33)+2}$

$\Rightarrow 4^{(10)33} \cdot 4^2 \bmod 11$

$= (1 \bmod 11)(4^2 \bmod 11)$

$= 16 \bmod 11 = 5$

RSA

→ Rivest - Shamir - Adelman → 1978

→ Asymmetric (2 keys)

1- Key Generation

① Select 2 large prime #'s 'p' & 'q'

② $n = p * q$

③ $\phi(n) = (p-1)(q-1)$

④ Choose value of 'e'

$1 < e < \phi(n)$

$\gcd(\phi(n), e) = 1$

⑤ Calculate

$d \equiv e^{-1} \bmod \phi(n)$

i.e $ed = 1 \bmod \phi(n)$

$ed \bmod \phi(n) = 1 \bmod \phi(n)$

⑥ Public key $\{e, n\}$

⑦ Private key $\{d, n\}$

e → public key

d → private key

M → P.T

C → C.T

$n = p \times q$

2- Encryption

$C = M^e \bmod n \quad (M < n)$

3- Decryption

$M = c^d \bmod n$

Ex $p = 3$, $q = 11$

→ $n = p * q = 33$

M < n

→ $\phi(n) = (p-1)(q-1) = 20$

→ let $e = 7$

as $1 < 7 < 20$

$\gcd(7, 20) = 1$

→ $d \equiv e^{-1} \bmod \phi(n)$

$de \equiv 1 \bmod \phi(n)$

$7 * d \equiv 1 \bmod 20$

$7 * d \bmod 20 = 1$

Public key = $\{e, n\} = \{7, 33$

Private key = $\{d, n\} = \{3, 33$

Encryption

Let $m = 31$

then $c = 31^7 \bmod 33 = 4$

Decryption

$M = c^d \bmod n = 4^3 \bmod 33 = 31$

d → multiplicative inverse of $7 = 3$

↳ use extended ecludian algo here

- Symmetric vs. Asymmetric Algorithms

① Symmetric Algo

- single shared secret key
- key has dual functionality: encryt & decrypt
- Equation used to calculate the number of symmetric keys needed is:

  $N(N-1)/2$ = number of key
- Only provide confidentiality, no authentication or nonrepudiation.
- Very fast and hard to ~~breck~~ break.
- encryp and decrypt quickly large amounts of data

Strengths:

1- Much faster than asymmetric system.

2- Hard to break if using a large key size.

Weakness

1- Each pair requires a unique key, so number of indivdus increases, number of keys will increase

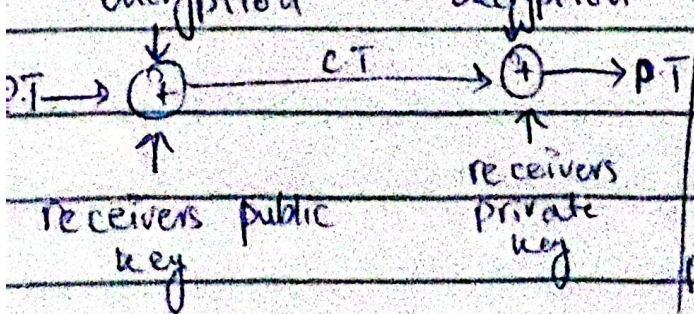
2- Requires secure machanism to deliver keys.

3- Provides confidentiality but not authenticity or nonrepudiation.

E.g: DES, Tripple DES (3DES), RC4, AES

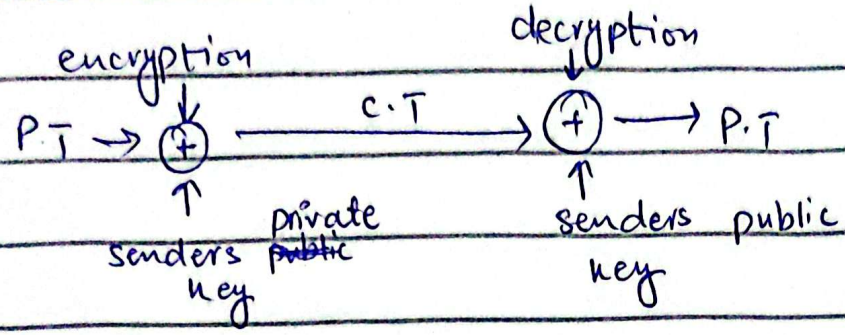
② Asymmetric Algo

- aka public key system
- pair of keys used, one public - publicaly shared, one private - secret key
- It is not possible to encrypt and decrypt using the same key because the two keys are not the same.
- For confidentiality



- called secure message format
- because only the person having corresponding private key can decrypt the C.T.

For authentication



- called an open message format because anyone with a copy of the corresponding public key can decrypt the C.T. This ensures authenticity not confidentiality

Strength

1- Better key distribution than symmetric systems
2- Better scalability than symmetric systems.
3- Can provide authentication and non repudation.

Weakness

1- Work very slower than symmetric system
2- Mathmatically intensive tasks (Complex)
3.

RSA (Rivest - Shamir - Adleman)

Initialization Vectors

- Random values that are used with algorithms to ensure patterns are not created during the encryption process.

Info Security Services

① Confidentiality ② Data Integrity ③ Authentication

Types of Authentication

① Msg encryption

② Msg authentication code (MAC) $C(M,k)$ = Mac Code

③ Hash function $h = H(M)$ {Fixed size}

Through Encryption

Confidentiality only

① M → E → C·T → D → M

Sender (A) — K_1 — K_1 — Receiver (B)

② Asymmetric : Confidentiality only

③ Asymmetric : Authentication only

M → E → C·T → D → M

② $kPu(B)$ — $kPv(B)$

③ $kPv(A)$ — $kPu(A)$

④ Both

M → E → C·T → E → C·T → D → [ ] → D → M

Sender (A) — $E(M, kP_A)$ — Receiver B

$kPr(A)$ — $kP_b(B)$ — $kPr(B)$ — $kP_b(A)$

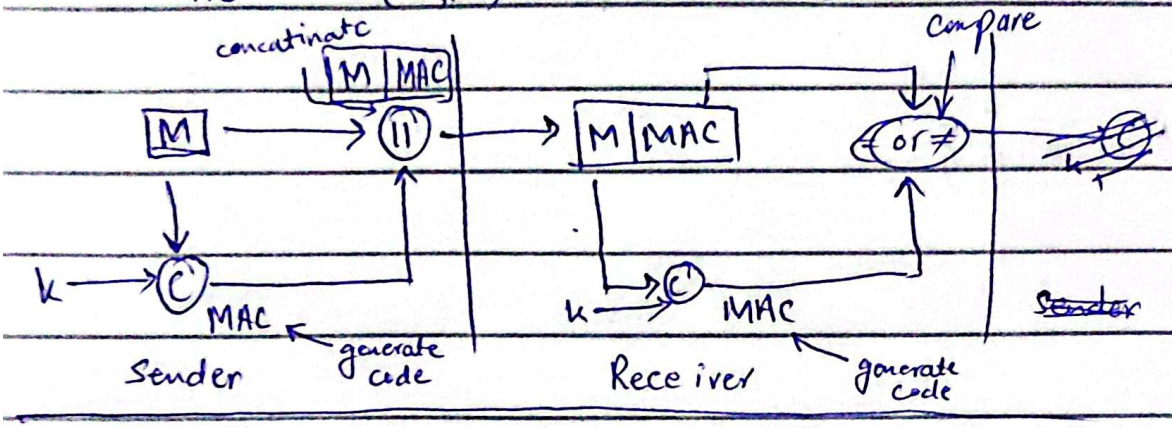
① Authentication — ② Confidentiality

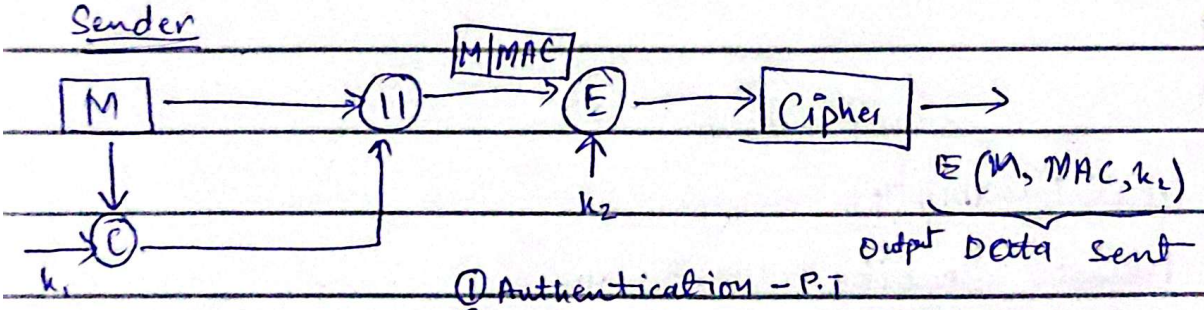
Decryption in reverse order

① Authentication then ② Confidentiality

Message Authentication code (MAC)

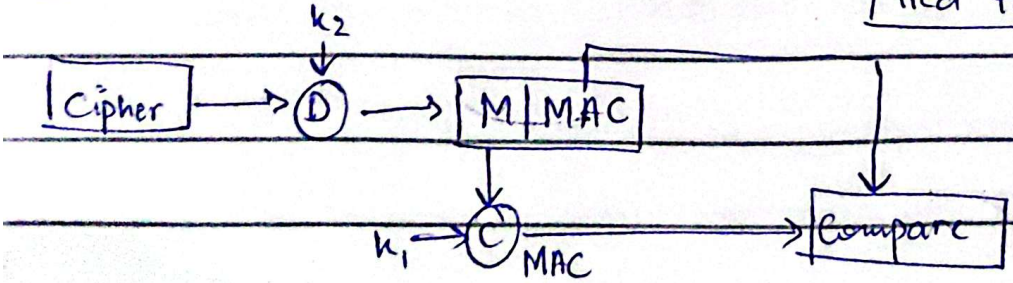
MAC = C(k, M) ① Authentication

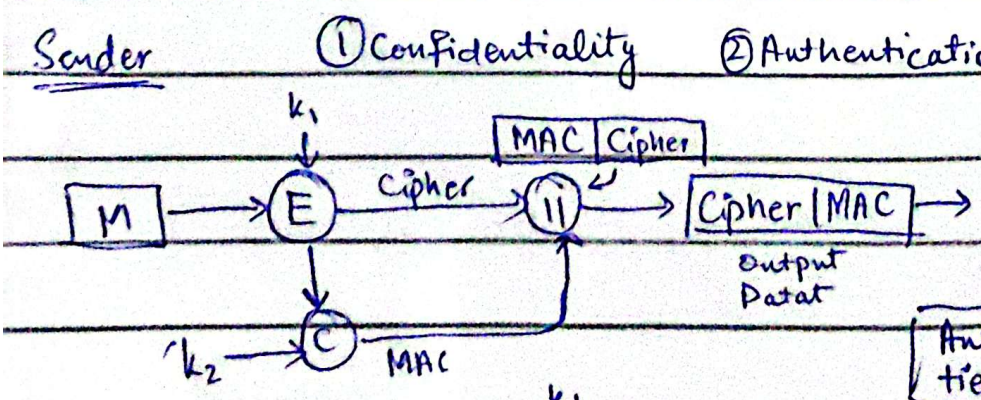


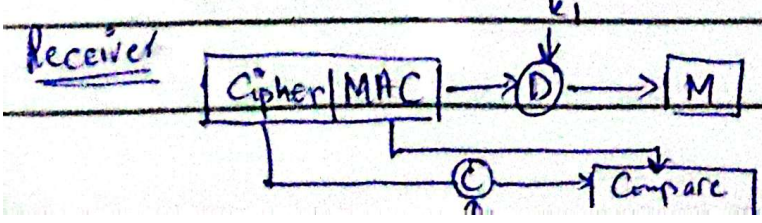


① Authentication – P.T
② confidentiality

Authentication tied to P.T





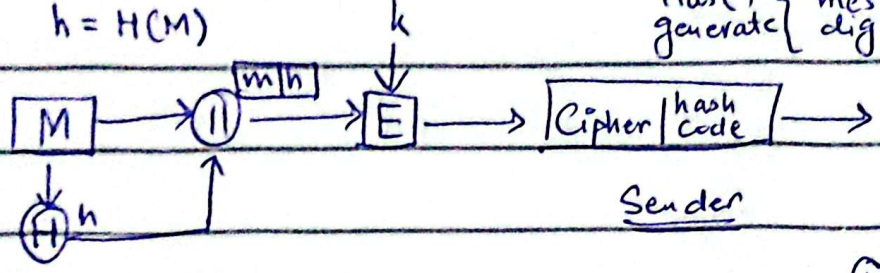


1208 bytes vs 1105 bytes

Hash Function

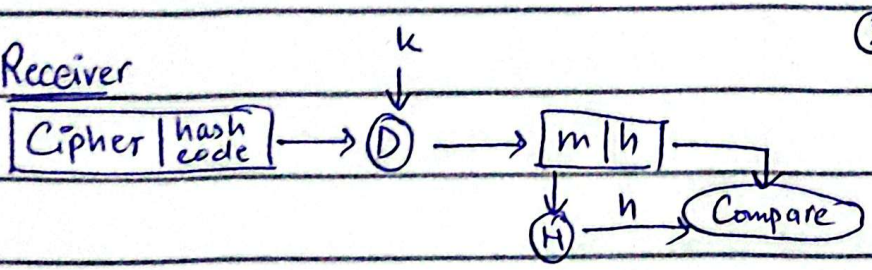
Has() generate { hash code / message digest }

① $h = H(M)$

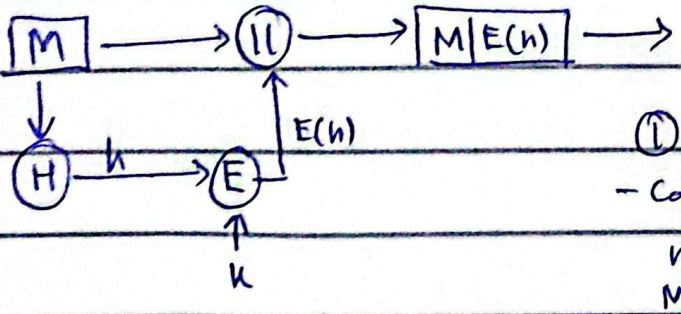


① Confidentiality
② Authentication

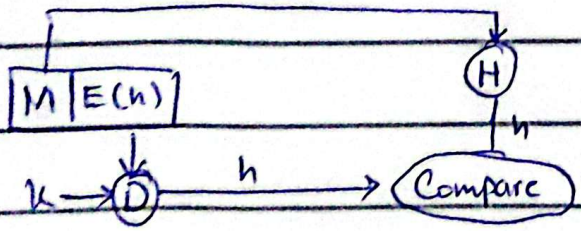
Receiver



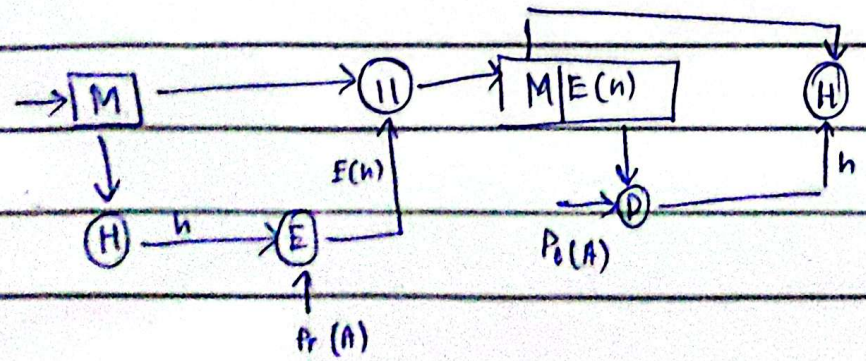
②



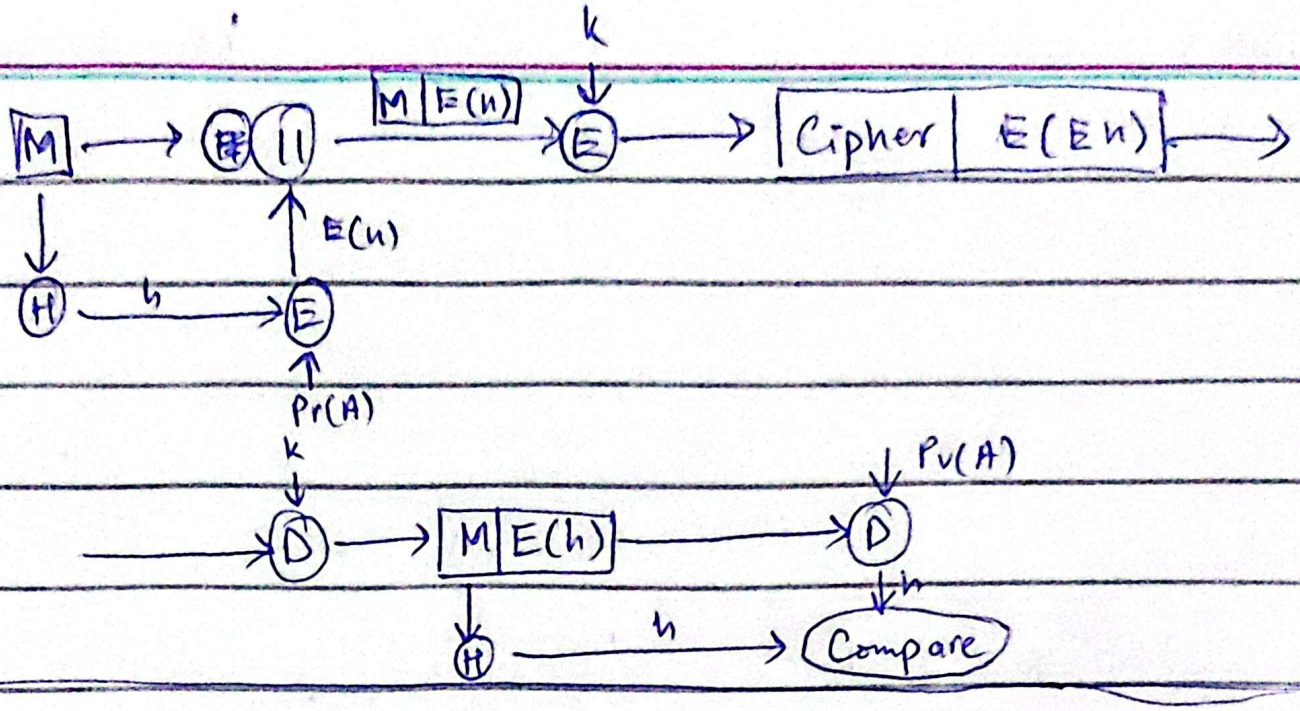
① Authentication only
- Confidentiality is not achieved bez Msg is not encrypted instead hash code is encrypted which is still authentication



③



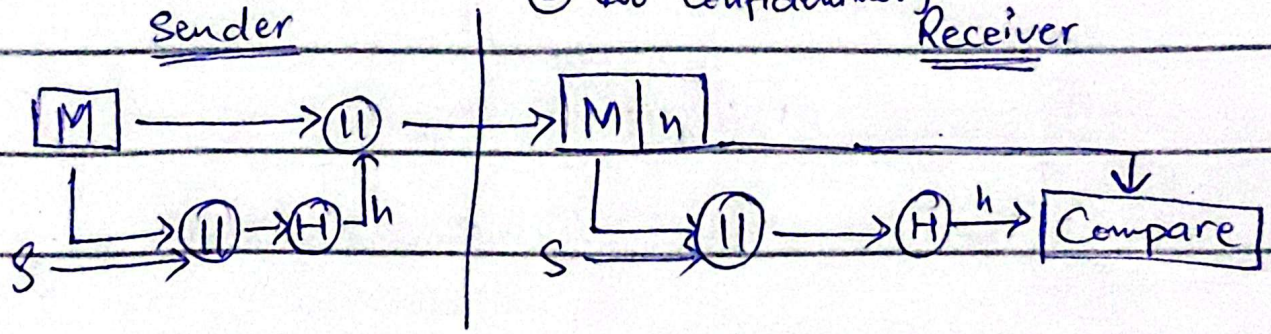
④



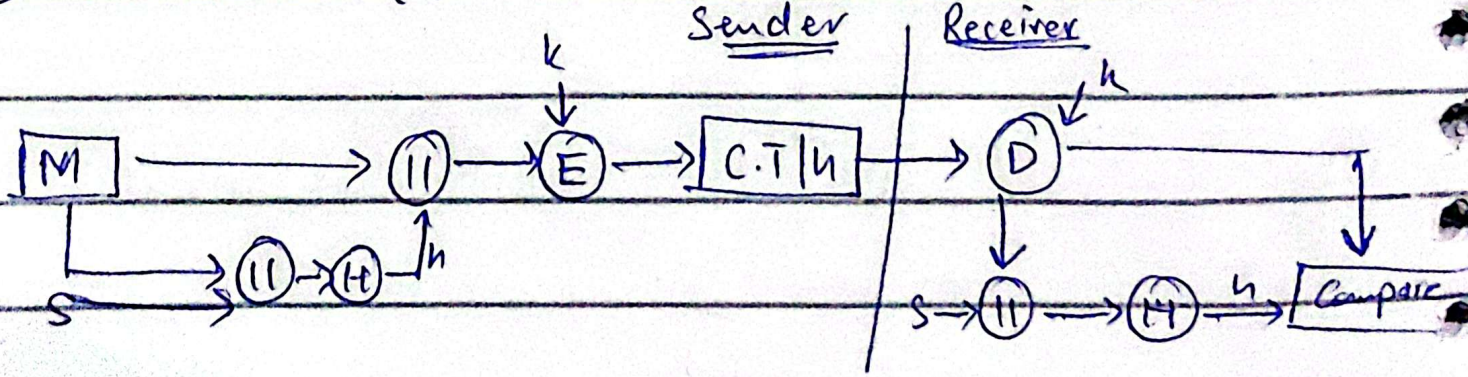
⑤ Secret code (S)

① Authentication only

② No Confidentiality



⑥ Secret code (S)

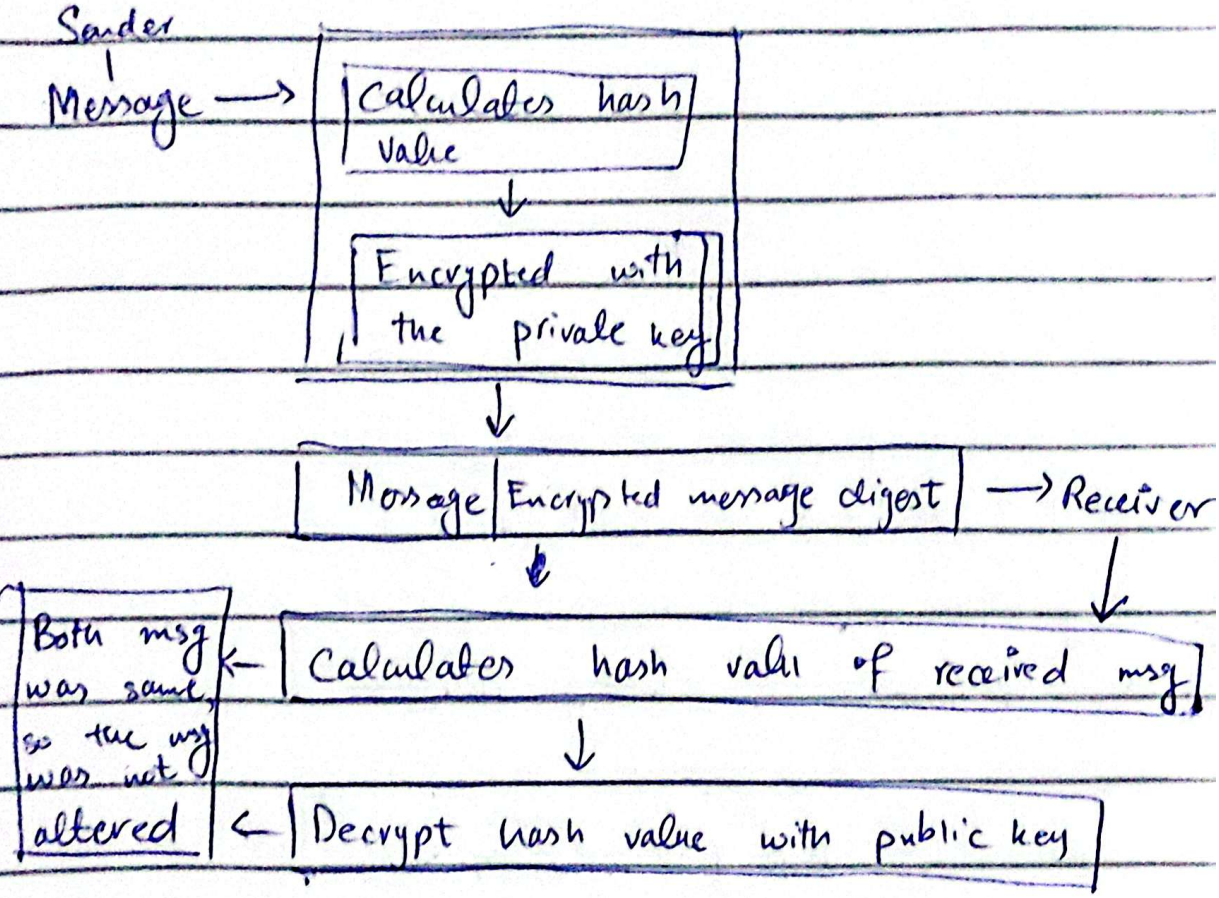


→ Digital Certificate → Digital Signature

IS - HomeTask

Digital Signatures

- Is a hash value that has been encrypted with the sender's private key



- RSA
- Key management

Digital Certificate

- A certificate is the machanism used to associate a public key with a collection of components in a manner that is sufficit to uniquely identify the claimed owner

→ Digital Signature Algorithm (DSA)

- used for digital signature
- asymmetric algo
- Steps

① Parameter Generation

- find p such that $2^{L-1} < p < 2^L$

p → prime number L → $512 <= L <= 1024$

- find q which is prime divisor of (p-1)
- compute $g = h^{(p-1)/q} \bmod p$

h → $1 < h < p-1$ g → $g > 1$ or $h^{(p-1)/q} \bmod p > 1$

② Key Generation

- Private key, a is any random number such that $0 < a < q$
- public key, $A = g^a \bmod p$

③ Signature Generation

① choose k in range [1, q-1]

② $X = g^k \bmod p$ and $r = X \bmod q$. If $r = 0$ then go to step 1

③ $k^{-1} \bmod q$ calculate.

④ $h = \text{hash}(M)$ range: $0 \leq h < q$

⑤ $s = k^{-1}(h + ar) \bmod q$. If $s = 0$ then go to step 1

⑥ Returns (r, s)

④ Signature Verification

Access Control

① Identification ② Authentication ③ Authorization

- Ex Access Control Models

① MAC model - computer decides

The person who created can only access no one else cannot access.

② DAC - user decides

The person can allow other authorized person to access

③ RBAC Model - (similar to MAC)

- Admin can read, write, execute
- other user can only read from In home/*
- If admin is changed then no need to create new admin's account.

ACL (Access Control Lists)

Rule based Access Control

① Content - based ② Context based

Wednesday IS 24-4

Web Security

OSI Model

Attacks

- Web Security Threat : DOS, Malware, SQL Injection
- Classifications : 2 types

① System Security ② Web security

	~~Threats~~ Consiequences	Countermeasures
Integrity	- Breach	- changed data info.
Confidentiality	- Eavesdropping - Breach	- Encryptions
Araliability	- killing user threats	- Difficult to prevent
Authentication	- Data forgery	- Cryptographic tech.

- Socket Programming

- SSL : (Secure Socket Layer) used for Integrity confidentiality.

• Deffie Hellman

Diffie-Hellman Key exchange algorithm

Steps:

1. Consider a prime number "q"
2. Select "α" such that α is a primitive root of "q" and $\alpha < q$
   - 'α' and 'q' are public elements known to everyone
   - X → Private key
   - Y → Public key
3. Assume X_A, i.e., $X_A < q$
   - compute $Y_A = \alpha^{X_A} \bmod q$
4. Assume X_B, i.e., $X_B < q$
   - Compute $Y_B = \alpha^{X_B} \bmod q$
5. Compute secret key
   $k_A = (Y_B)^{X_A} \bmod q$, $k_B = (Y_A)^{X_B} \bmod q$
   $k_A = k_B$ = always
   ↳ else wrong

→ **How to find primitive root of 'q'**

→ q = 7 Primitive root of 7 = ?

a is Primitive root of q if :-

$a \bmod q$
$a^2 \bmod q$
$a^3 \bmod q$
⋮
$q-1$ mod q

give result $\{1, 2, 3, \ldots q-1\}$

→ sort the result; no missing value or repeating

→ if a repeats end it

a = 1	a = 2	a = 3 → p.r
$1 \bmod 7 = 1$	$2^1 = 2 \bmod 7 = 2$	$3^1 = 3 \bmod 7 = 3$
$1^2 \bmod 7 = 1$	$2^2 = 4 \bmod 7 = 3$	$3^2 = 9 \bmod 7 = 2$
X	$2^3 = 8 \bmod 7 = 1$	$3^3 = 27 \bmod 7 = 6$
a = 4	$2^4 = 16 \bmod 7 = 2$	$3^4 = 81 \bmod 7 = 4$
$4 \bmod 7 = 4$	X	$3^5 = 243 \bmod 7 = 5$
$16 \bmod 7 = 2$	a = 5	$3^6 = 729 \bmod 7 = 1$
$64 \bmod 7 = 1$	$5 \bmod 7 = 5$	{1, 2, 3, 4, 5, 6}
$256 \bmod 7 = 4$	$25 \bmod 7 = 4$	{1, 2, 3, 4, 5, 6}
X	$125 \bmod 7 = 6$	P.R = 3, 5
	$625 \bmod 7 = 2$	
	$3125 \bmod 7 = 3$	
	$15625 \bmod 7 = 1$	

Now

$q = 7, \alpha = 5$	$q = 7, \alpha = 5$
$X_A = 3$ $X_A, X_B < q$	$X_B = 4$
$Y_A = \alpha^{X_A} \bmod q$	$Y_B = \alpha^{X_B} \bmod q$
$= 5^3 \bmod 7 = 6$	$= 5^4 \bmod 7 = 2$
$k_A = (2)^3 \bmod 7 = 1$	$k_B = (6)^4 \bmod 7 = 1$
$(Y_B)^{X_A} \bmod q$	$(Y_A)^{X_B} \bmod q$

$$k_A = k_B$$

=> k = 1 => is secret key