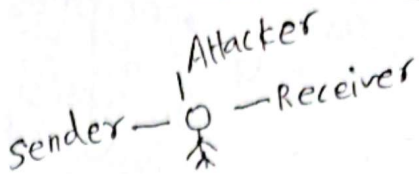
-Behrouz A. Forouzan

Chpt 1.



3 principles of security:
1) Confidentiality
2) Integrity
3) Availability

* 1.1 Security Goals

Fig. 1.1 Taxonomy of security goals

* Confidentiality

In ~~the~~ industry, hiding some .... kept secret.

* Integrity

Information needs to change constantly.
Integrity means that changes ..... in some information.

* Availability

A third component .... customers could not access their accounts for transaction.
-authorized entities

* Fig 1.2 Taxonomy of attacks with relation

- Snooping
- Traffic Analysis

Threat to confidentiality

* Snooping
  - unauthorized access
  - made nonintelligible to the interceptor by using encipherment techniques

* Traffic Analysis
  guess nature of transaction
  ∴ একজন আরেকজন কে msg transfer করে।
  interceptor - attacker
  - Obtain information by monitoring online traffic

* Attacks Threatening Integrity
  Several kinds of attacks:
  1) Modification
  2) Masquerading ÷ Pretend
  3) Repudiation
  4) Replaying

* Modification
  - a customer sends a message to a bank to do some transaction.
  - The attacker intercepts the message and changes the type of transaction to benefit herself.

* Masquerading
  For eg: Full
  attacker pretends instead to be the receiver entity.

* ~~Repudiation~~

* Replaying
  The attacker intercepts the message and sends it again to receive another payment from bank

4) Repudiation
the sender of the message deny the receiver of the message might later deny that he has received the message.
example....

Threat to Availability

* Denial of service (DOS)
The attacker might intercept and delete a server's response to a client, making the client to believe that server is not responding.

* Table 1.1 Categorization of passive and active attacks

* Passive attacks
the attacker's goal is just to obtain information.

* services and mechanism

Fig 1.3 Security services

1) Data Confidentiality
- Service is defined by X.800
- Prevent snooping & Traffic analysis attack

2) Data Integrity
- modification, insertion, deletion - appends to data a short checkvalue
- Replaying by an adversary

3) Authentication
- Connection-oriented communication

4) Nonrepudiation
Nobody can deny by either the sender or the receiver data

5) Access control
- Provides protection against unauthorized access to data.

* Fig 1.4 Security mechanisms

1) Encipherment – hiding or covering data can provide confidentiality

2) Data Integrity – a short check value

3) Digital Signature

sender has private key & public key

similarity & dissimilarity

To prove ~~x~~ is the sign.

4) Authentication Exchange

– exchange some msgs to prove their identity to eachother

5) Traffic Padding

inserting some bogus data into data traffic

6) Routing Control

continuously changing different

7) Notarization

deny করার ~~জন্য~~ সুযোগ নাই।

8) Access control

Access right to the data or resources owned

* Table 1.2 Relation between security services and security mechanisms

p1.4

* Techniques

1) Cryptography – এমন ভাবে লিখবো ~~যে~~ jemon পড়া যাবে না

2) Steganography

* cytography – secret writing

– encryption and decryption

secret form to main form

* Symmetric-key Encipherment
  Secret key
* Asymmetric-key Encipherment
  Public key & Private key

To send a secured msg to Bob .. private key.

* Hashing
  mapping
  - variable length msg is created into a fixed length msg
  - The digest is much smaller than the message

13 July 2025

Pg 82

Chapt-3

Pg 82

* Fig 3.1 shows the general idea of Symmetric key cipher

→ ciphertext - Encrypted → shared secret key
→ plaintext
→ Insecure channel
→ Encryption algorithm
→ Decryption algorithm
→ secure key-exchange channel

Note that....
→ single key
→ inverses of eachother

$E_K(x)$ $x \rightarrow$ plain text

Encryption Algorithm ← $E_K(x)$ → key

Pg 82

$D_K(x)$ $c \rightarrow$ ciphertext

$C = E_K(P)$

$P = D_K(C)$

$D_K(E_K(x)) = E_K(D_K(x)) = x$

$C = E_K(P)$ $\quad D_K(C) = D_K(E_K(P))$

$= P$

$a(a^{-1})$

→ face-to-face exchange of the key

$(m \times (m-1))/2$

⑤ 1 2 3 4 5

$4+3+2+1$ ⑩

$\frac{5 \times 4}{2}$

* Kerckhoff's Principle

guessing the key should be so difficult that there is no need to hide the encryption/decryption algorithm.

* Cryptanalysis

not to break other people's codes, but to learn how vulnerable our cryptosystem is.

* Fig. 3.3

1) Ciphertext-only Attack

Have ciphertext need to find key and plaintext

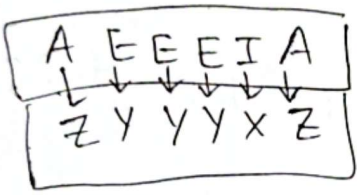
C ← key
  ↘ plaintext

Fig 3.4

1) Brute-Force attack → Also known as domain, key range

2) Statistical Attack

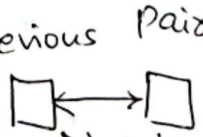
E is most frequently used letter in English Text



3) ~~Plain~~ Pattern Attack

4) known Plain text attack

Fig 3.5



New(C)
|
P

5) Chosen Plaintext Attack

Fig 3.6

~~Fig 3.7~~

Alice hardware

(C,P)

New(C)
|
Plain

6) chosen ciper text attack

New(c)
↓
P

3.2 * Substitution ciphers → replaces one symbol with another

(1) Monoalphabetic Ciphers (one to one)

A
↳ XYZ

A → Z
B → Y

(2) Polyalphabetic Ciphers (one to many)

Example 3.1

plaintext: hello

ciphertext: KHOOR

Example 3.2

plaintext: hello

ciphertext: ABNZ

* Additive cipher

· Fig 3.8 Representation ·

Fig 3.9

$C = (P + k)$

$P = (C - k) \bmod 26$

14+5

19 mod 26

19

Encryption

key = 15

plaintext ~~message~~ = "hello"

$C = (7 + 15) \bmod 26$

$(4 + 15) \bmod 26$

$(11 + 15) \bmod 26$

$(14 + 15) \bmod 26$

WTAAD

Cipher — plaintext — Key = 15

WTAAD — hello

26 % 26

26 = A
0 = A

7 $(22-15) \bmod 26$ — h

4 $(19-15) \bmod 26$ — e

Exam

11 $(00-15) \bmod 26$ — l

26 − 15 = 11 $(00-15) \bmod 26$ — l

-15 becomes 11 $(03-15) \bmod 26$ — o

15 − 3 = 12 ; 26 − 12 = 14

* Shift cipher
* Ceasar cipher

Example 3.5 Brute force attack

* Table 3.1 Frequency of occurence of letters in an English text

hello
heeo

* Fig 3.10 Multiplicative cipher

19 July 2025

Multiplicative ~~ceasar~~ Ciphers : ← k

enc → Multiply * k

Dec − 11 * k^{-1}

9 ≡ 3 (mod 6)

a ≡ b (mod m)

Fig 3.10 Multiplicative cipher

$c = (p \cdot k) \bmod 26$

Encryption

$c = (p \cdot k^{-1}) \bmod 26$

Modular inverse

Decryption

Example If K = 7

P = hello

h − 7
e − 4
l − 11
l − 11
o − 14

14 × 7 = 98

$c = (P * k) \bmod 26$

~~$= (\cdot * 7) \bmod 26$~~

h − 49 mod 26 = 23

e − 4 × 7 mod 26 = 2

l − 11 × 7 mod 26 = 25

l − 11 × 7 mod 26 = 25

o − 14 × 7 mod 26 = 20

Affine Cipher

encryption ↗

$(P * k_1 + k_2) \bmod 26$ and $P = (((C - k_2) * k_1^{-1}) \bmod 26$ ↘ Decryption

Combines (additive + multiplicative cipher)

Fig 3.11 Affine Cipher

$T = (P \cdot k_1) \bmod 26$

$C = (T + k_2) \bmod 26$

Ex 3.10 $k_1 = 7 \quad k_2 = 2 \qquad (7, 2)$

h → 7
e → 4
l → 11
l → 11
o → 14

$(7 \times 7 + 2) \bmod 26 = 51 \bmod 26 = 25$
$30 \bmod 26 = 4$
$79 \bmod 26 = 01$
$7a \bmod 26 = 01$
$100 \bmod 26 = 22$

Ex 3.11

$25 - 2 \quad 23 \times 7^{-1}$
$= 23$

$7^{-1} \equiv 15 \pmod{26}$
$7 * \frac{1}{7} = 7 * 15 \pmod{26}$
$1 = 105 \pmod{26}$

$23 * 15$
$\text{Decry}((25-2) * 7^{-1}) \bmod 26$
$= \cdot 7$

C: Z → 25
C: E → 4
C: B → 1
c: B → 1
c: W → 22

$(2 \times 7^{-1}) \bmod 26 = 4$
$(-1 * 7^{-1}) \bmod 26 = 11$
$(-1 * 15) \bmod 26 = 11$
$((22-2) \times 7^{-1}) \bmod 26$

$-2 \equiv 24 \pmod{26}$
$-2 - 24 \equiv 0 \pmod{26}$
$-26 \equiv 0 \pmod{26}$

$-2 \to 24$
$7^{-1} \to 15$
$-1 \equiv 2$
$-1 - 24 \equiv 2 \pmod{26}$
$-1 \equiv 25 \pmod{26}$

× Cryptoanalysis ⊗

* Monoalphabetic substitution cipher

Pg 94

Ex 3.8

hello
XBCCW
BDEEF

Hello
↳ same cipher value
advantageous to attacker

Fig 3.12 An example key for monoalphabetic substitution cipher

key = 5

abc

a +5 → E
b +5 → F
c +5 → G

a b c
14 15 31
↓ ↓ A
N O

26!
26 × 26
26 factorial

a 4→ E
b 14→ I
c 15→ O

* Poly alphabetic ciphers (Pg 95)

$k = \{k_1, k_2, k_3 \cdots\}$

Polyalphabetic ~~cipher~~ substitution

index
~~char~~
diff. key use

a → D
a → N

based on position

a b a c Monoalphatic
↓ ↓ ↓ ↓
E F E G

* Autokey Ciphers (Pg 95)

h e l l o

$k_1 = p_1$, $k_2 = p_2$, $k_3 = p_1$, $k_4 = p_3$

a b a c

a b a c
| | | |
E F N G

4 টার ভাবস 4 টার diff. key

$C = C_1 C_2 C_3 \quad K = (k_1, P_1, P_2, \cdots)$

Example 3.14 (Pg 96)

additive { 00 19 19 00 02
12 00 19 19 00

12

additive এর সাথে সার্থক হল polyalphabetic
key different addive same

* playfair Cipher (Pg 96) 2টা 2টা করে কাজ

Fig 3.13

3 rules for encryption

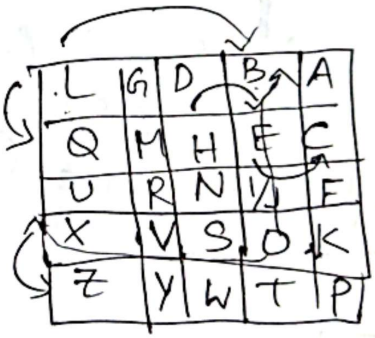
a.
b.
c. Same row, column

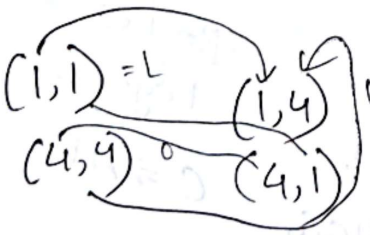
hello

helalo

Example 3.15

he → EC





L Z
I
I
Q L

LO

odd হলে even বানাতে হবে
next row wrap ~~rack~~ করে দিবো
column next row ~~rack~~ wrap

wrap with next character

hello
same থাকলে আলাদা করে দিবো diff. value দিয়ে

helxlo

L(1,1) – L এর cipher (L এর row, 0 এর col)
O(4,4) – O এর cipher (O এর row, L এর col

~~Linear conduence~~

{ Linear congruence
Modular inverse

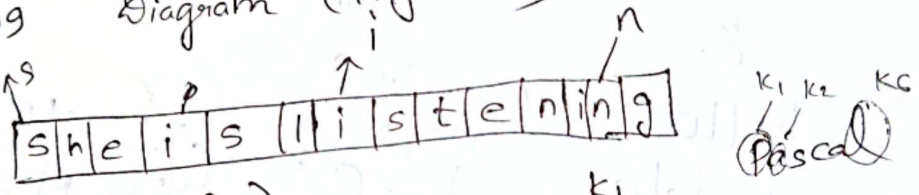
20 June 2025

* Vigenere Cipher
key এর সাথে একটা value which is m
$k_1, k_2 k_3, k_4$

Encryption
$C_i = P_i + k_i$

Decryption
$P_i = C_i - k_i$

Pgg 99 Diagram (Fig. 3.14)



$k_1 - k_6$
1 2 3 4 5 6
k-2 (k_2)
h s g সাবে

k_1
s i n

Table 3.3

sin
key-P
Cipher HXC

hsg
key-a
Cipher HSG

p ⇒ i e
key ⇒ s
C ⇒ AW

X Hill Cipher (4th)

3.3 Transposition Ciphers

- keyed (combined) → P by R, by C
- keyless → C
  - Permutation or combination

Example 3.22 (পৃষ্ঠা)

→ row by row

→ colum by column

column by column

column দিয়ে সাজানো

row দিয়ে পড়িবো

Example 3.23

meet me at the park

m	t	a	h	a	
e	m	t	e	r	
e	e	t	p	k	

- column by column (capital for cipher) → mtahaemtereeetpk
  - → row No
  - → organize column wise
  - → row by row sending

m → e (column e)

memateakeetethpr

- row by row

plaintext = Meet me at the park

column = 3

~~meet~~

m	e	e
t	m	e
a	t	t
h	e	p
a	r	k

MTAHAEMTEREETPK

* keyed Transposition

3	1	4	5	2
1	2	3	4	5

Encryption ↓ ↑ Decryption

Pg-109 Diagram
→ row by row
→ key, shuffle
→ C by C

enemy attacks

e a k i
n t s p
c t k o n t z
n a o
y c

26 July 2025

* statistical attack

* Brute-Force Attack

* Double Transposition Cipher
R by R
C by C

concept দেখবে

* Stream and Block ciphers
- stream ciphers

$P = P_1 P_2 P_3, \ldots$ $C = C_1 C_2 C_3, \ldots$ $k = (k_1, k_2, k_3, \ldots)$

$C_1 = E_{k_1}(P_1)$ $C_2 = E_{k_2}(P_2)$ $C_3 = E_{k_3}(P_3) \ldots$

Characters in plaintext are fed ....
Fig 3.26

Example 3.30
Additive cipher

Example 3.31
monoalphabetic
A-Z
B-X
independent on mapping table

Pascal
1-6 P encrypted.

Example 3.32 $k = (k_1$
stream cipher
vigenere cipher

points :

* Block cipher
2 points, example :

Fig 3.27 a group of plaintext

Example 3.34 playfair

Example 3.35 Hill Cipher

Example 3.36 polyalphabetic cipher

CT on chpt 3

Review

Linear congruence
Modular inverse congruence

Fig 3.1, eqns
Kerchoff's Principle
Cryptanalysis Fig 3.3
Brute-force Attack
Cipher ... Affine

chapter :- 6. Data Encryption Standard

* Fig 6.1 Encryption and decryption with DES
At the encryption site, ...

* Fig 6.2 General structure of DES

64-bit plaintext → 64-bit ciphertext
32
56 bit key
48 and xOR
Round-key generator
↑
56-bit cipher key
↓
48 a convert
p box → permutation

Permutation box (p box)

56
48 48 48
16টা generate 2বার।

Key ⇒ 56
48 bit এর key generate করবে।

* Fig 6.3 Initial and final permutation
* Table 6.1 Initial and final permutation tables

Example 6.2
The initial & Final ... DES

* Fig 6.4 A round in DES (encryption site)

S-box → round-16 এ Mixer (xOR)
round 48 bits
56 starting swapper

64
1
8টা বাদ

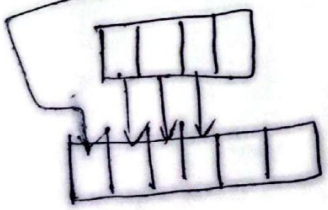
56
32, 48

* Fig 6.5 DES function

Expansion p-box
48 bits 32 bits by s-box

48 → 6 6 6 6 6 6 6 6
32 32
1 1 1 1 1 1 1 1
4 4 4 = 32

* Fig 6.6 Expansion permutation
From bit 32

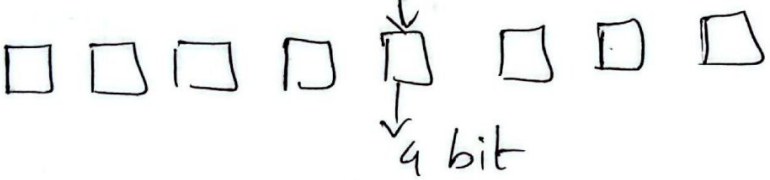


* Table 6.2 Expansion p-box table

* DES Function
expansion p-box, whitener (that adds key)
a group of s-boxes, straight p-box
48 bits ↓ 32 bits
f(32, k1)

48 = 6×8

6 bit



4 bit

10 11

* Fig 6.8 s-box rule

s-box - 8টি

0 0
0 1
1 0
1 1

r = 4
c = 16

4×16

bit 1 and bit 6 → row
bit 2 - bit 5 → column

* straight Permutation
32-bit will be there

CamScanner

10 Aug 2025

Chapter 7.

Advanced Encryption Standard (AES)

* 7.1 Introduction

The advanced Encryption standard .... in Dec 2001.

block cipher

128 bits

First AES conference, 2nd AES conference,

3rd AES conference

3 version key sizes - 128, 192, 256 bits

block size → 128

key → 128, 192, 256

pg 218

* Criteria

- Security - focused on resistance to cryptanalysis
- Cost - covers computational efficiency and storage requirement such as hardware, software, smart cards
- Implementation

  simple and flexible

AES has defined 3 version .... alway 128 bits

1st	2nd	3rd
128	128	128
128	192	256
10	12	14

Round key always 128 bits

64 → 48

16 different key

16 Round key

* Fig 7.1 General design of AES encryption cipher

(n) (r) $Nr+1 = 10+1 = 11$

k0 ——— k10

11 ta key

k0 ——— k12

k0 ——— k14

Number of round keys = $Nr+1$

* Data units
  - Bit :- binary digit (0 or 1)
  - Bye : 8 bits

    1 byte = 8 bit

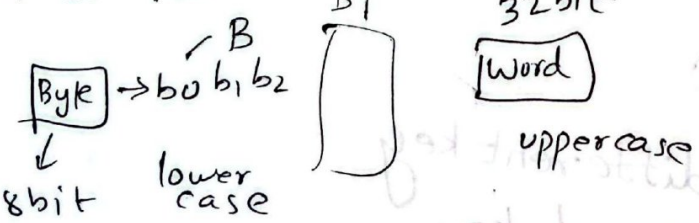
    ↳ [1011 0010] → Row matrix 1×8

    $\begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$ 8×1 column matrix

  - Word : a group of 32 bits

    1 word
    32 bit
    2 byte

* Fig 7.2 Data units used in AES

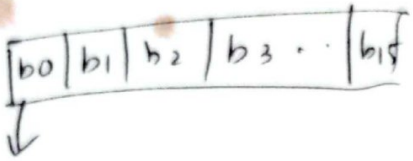


* Block

AES encrypts & decrypts data blocks

A block in AES is 128 bit

~~1 Bit~~ [1 block
128 bits
16 byte]



b0 - b7

16 × 8 = 128

* state

Fig 7.3 Block to state

$$\text{State} = \begin{bmatrix} s_{0,0} = b_0 & s_{0,1} = b_4 & s_{0,2} = b_8 & s_{0,3} = b_{12} \\ s_{1,0} = b_1 & & & \\ s_{2,0} = b_2 & & & \\ s_{3,0} = b_3 & & & \end{bmatrix}$$

$s_{0,0}$ (R C)

b_{12}

$1 \bmod 4 = 1$

$i \bmod 4,\ i/4 \rightarrow 12 \bmod 4,\ 12/4$

$0, 3$ $\quad (0, 3)$ matrix no.

Pg 221 $\quad 0, 3 \quad b_{12} = 0 + 4 * 3 = 12$

CamScanner

* Fig 7.4 changing plaintext to state

A = 00
E = 04
S = 12

12
0001 0010
8 bit

$$\begin{bmatrix} 00 \\ 04 \\ 12 \\ 14 \end{bmatrix}$$ state

Pg 122 Structure of Each Round

* Fig 7.5

last round uses only 3 transformations

~~shift~~ Sub Bytes
ShiftRows
MixColumns
AddRoundKey

CamScanner

17 Aug 2025

Chapt 1.

1.1 security goals - কোনটা মানে কি with examples. 3টা

1.2 Attacks

কোন category under এ আছে

Threat to confidentiality - Snooping, Traffic analysis

" " Integrity - 4টা

" " Availability - 1টা

1.3 services and Mechanisms (না পড়লে চলবে)

এর আর কি

× Relation

Chapter-3 : Traditional Symmetic key Cipher

→ Symmetic key Cipher — 3.1 Introduction & Fig.

→ kerchhoff's principle

key algorithm

→ Cryptoanalysis attacks

4টা attack

→ Additive Cipher

→ Multiplicative cipher

→ Affine cipher

→ shift cipher

→ Ceasar Cipher

→ Monoalphabetic

কেন বলা হয়

Book এর example practice

→ Transposition cipher < keyless / keyed

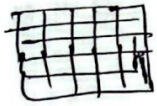
→ Polyalphabetic (Autokey, playfair, Vigenere ✗)

Math ভালো না কিভাবে কাজ করে, কেন polyalphabetic কেন stream cipher)

playfair 5×5

keyword দিয়ে থাকে

~~Secure~~



Network

N	E	T	W	O
R	K	A	B	C
D	F	G	H	I/J
L				

5×5

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

If I J together given only put one from these two

FAJIL

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

CamScanner

Transposition < keyless / keyed → বেশি marks)

R by R organise
পাঠাতে হবে c by c

⑥ Meet me at the park

M E E T M E
A T T H E P
A R K X X X

MAAETRETK THX MEXEPX

c by c

MEET ME AT THE PARK

M T A H A
E M T E R
E E T P K

Row = 3

MTAHAEMTEREETRK

keyed

Encryption ↓

3	1	4	5	2
1	2	3	4	5

↑ Decryption

1 2 3 4 5
SECURE

CERSU

Encryption process

1	2	3	4	5
4	2	1	5	3

1 2 3 4 5 6 7
NETWORK

EKNORTW

1	2	3	4	5	6	7
3	1	6	7	4	5	2

*Combining Two Approaches

R by R

According to keyed

7 টি column এ সাজাবে

NET WORK

MEET ME AT THE PARK

7টি column Row by Row

M	E	E	T	M	E	A
T	T	H	E	P	A	R
K	X	X	X	X	X	X

Plaintext কে cipher এ then R by R and shuffling

From the Network table

Network keyword এ column exchange

E	A	M	M	E	E	T
T	R	T	P	A	H	E
X	X	K	X	X	X	X

এখন C by C সাজাবে

Cipher- E TX ARX MTK MPX EAX EHX TEX

Encryption for plaintext to ciphertext

So R by R

C by C সাজাবো

≤ Stream cipher, block cipher
কোনো কি বলে

chpt - 6 → with explanation in steps the process

DES - কাজ, Fig, basic structure, DES algorithm

X Weakness - no need

Book ✓

Shuffling column এর জন্য, ROW এর জন্য

31 Aug 2025

Chapter-7 . AES

Convert keysize	Key Amount
128	Key = 11
128	Key = 13
128	key = 15

Nr	keysize
10	128
12	192
14	256

Nr+1

Block - 128 bit
16×8

word
B0
↓
Bit

State
16 byte করে

Structure
SubBytes, ShiftRows, MixColumns, AddRoundkey

PreRound

Nr
(one round)
~~প্রত্যেকটা~~ round এটা transformation
এটা কিন্তু pre-round আর Nr round
ছাড়া (2-9)

the translation
AddRoundkey should be in Preround key.
In last round just mix Column not happening
rest all also happen.

CamScanner

* Substitution
It is invertible transformation

SubBytes
Byte by Byte কাজ করে,
2 Types substitution —
1) SubByte
2) GF(2^8)

..... 128

01001100
Hexa → 4C

same কাজ 16 বার

Fig 7.6

The subByte .... 16 independent byte-to-byte transformations.
8×16 = 128

row no.
(5)A 16 — BE
5B 16 — 39

16 because it is already converted in hexa

Table 7.1 - For Encryption
Table 7.2 Inv SubBytes Transformation table
↳ Decryption

* InvSubBytes — Decryption

*Fig 7.7 SubBytes transformation for ex 7.2
in state each in 8-bit

* Transformation Using the GF(2^8) Field

algebraically — kind of Affine cipher

Only procedure no math

subbyte → $d = X(s_{r,c})^{-1} \oplus y$

invsubbyte → $[X^{-1}(d \oplus y)]^{-1} = [X^{-1}(X(s_{r,c})^{-1} \oplus y \oplus y)]^{-1}$

$= [(s_{r,c})^{-1}]^{-1} = s_{r,c}$

* Fig 7.8

state = 4×4

8 bit করে

$[0\ 1\ 0\ 0]$ – Row Matrix

$\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ – Colum matrix

steps Encryption

$(src)^{-1}$ Byte-to-Matrix

convert in matrix

$c = x \cdot b$

$d = c + y$

↓ Matrix to Byte

$(src)^{-1} \cdot x + y$

Decryption

b Matrix to Byte

$b = x^{-1} \times c$ → cipher

$c = d - y$

↑ Byte to Matrix

Example 7.3

CamScanner

7 September 2025

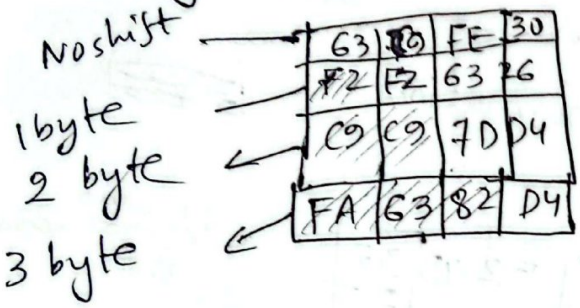
* MixColumns → 8 Questions will come for exam.

* Fig 7.6
State - 128 bit

* Permutation
ShiftRows
element same থাকতেছে নতে ছড়ে যাতেছে

Fig 7.9

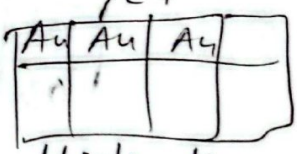
Fig 7.10 ShiftRows transformation in Example 7.4



DES থেকে কোনো Q আসার way আছে

* MixColumns
interbyte ; intrabyte transformation
main content change হয়ে যায়।
each new byte is different.

8bit
EA
A4
E4



* Fig 7.11 Mixing bytes using matrix multiplication

Q will come for exam
Matrix willbe given

* Fig 7.11 Mixing bytes using matrix multiplication

column-to-column কাজ করে

A shift 1110

x	a	c	I
y	b	F	J
z	c	h	k
t	d	H	L

state

Inverse এ সময় c-1 multiply For decryption

$$\begin{bmatrix} L \\ W \\ P \\ K \end{bmatrix} = \begin{bmatrix} \quad \end{bmatrix} \begin{matrix} (0) \\ \\ \\ \\ c^{-1} \end{matrix}$$

state (4x4) matrix

* Fig 7.12 Constant matrices

* Fig 7.13 Mixcolumns transformations

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

Constant

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

state

87 value change করার জন্য

8421

02 * 87 ⊕ 03 * 6E ⊕ 01 * 46 ⊕ 01 * A6

00 01 0101 ⊕ 1011 0010 ⊕ 01000110 ⊕ 10100110

00→00

11→00

odd-binary 8 bit কে binary 87 এ রূপান্তর করতে হবে।

02 = 0000 0010 = x

87 = 1000 0111 = $x^7 + x^2 + x + 1$

02 * 87 = $x(x^7 + x^2 + x + 1)$ mn

$= x^8 + x^3 + x^2 + x$

$= \boxed{x^4 + x^3 + x + 1} + x^8 + x^2 + x$ 2nd key

$= x^4 + x^2 + 1$

0001 0101

03*GE

03 = 0000 0011 = x + 1

GE = 0110 1110 = $x^6+x^5+x^3+x^2+x$

03*GE = $(x+1)(x^6+x^5+x^3+x^2+x)$

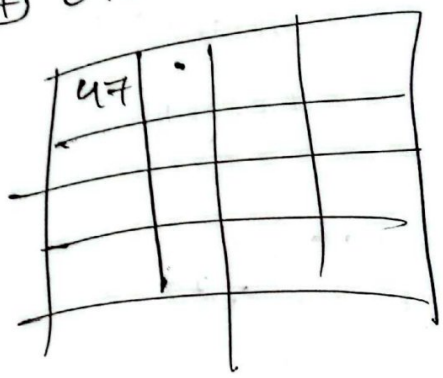
$x^7+x^6+x^4+x^3+x^2+x^6+x^5+x^3+x^2+x$

$x^7+x^4+x^5+x$

1011 0010

02*87 ⊕ 03*GE ⊕ 01*46 ⊕ 01*A6

0001 ⊕ 1011 0010 ⊕ 01000110 ⊕ 10100110



0001 0101
1011 0010
0100 0110
1010 0110

0100 0111

4 7

0001 1010

* Add Roundkey (see the examples well (Q will come for exam)
* Fig 7.15 replace binary convert and XOR

steps
AES → mathematical type is imp

CT-2 AES

13 september 2025

Chapter - 10
Asymmetric-key Cryptography

Symmetric
addition
(key)

substraction
(key)

same key.

Asymmetric
Different key use করে encryption & decryption use করবো

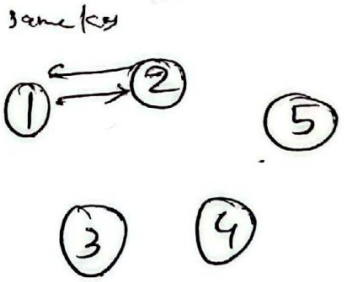
Public key Cryptography

Public key
Private key

$\frac{n(n-1)}{2}$

$\frac{5 \cdot 4}{2}$

10 keys

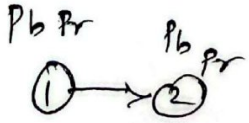


1 2
1 3
1 4
1 5
2 3
2 4
2 5
3 4
3 5
4 5

Pg 320

$\frac{10 \cdot 9}{2}$

$= 45$



5*2=10

3
4
5

10*2=20

CamScanner

small text

combination / Permutation → Symmetric

Symmetric	asymmetric
1) Sender, Receiver use same key for encryption, decryption	1) Different key for encryption, decryption
2) No. of key $n(n-1)/2$	2) No. of key $n * 2 \approx n$
3) Faster (Permutation)	(3) Slower (Mathematical function)
4) Used for encrypt large text.	(4) Used to hide very important content (small text)
(5) Known as sharing secrecy.	(5) known as personal secrecy.

Encryption → Public key

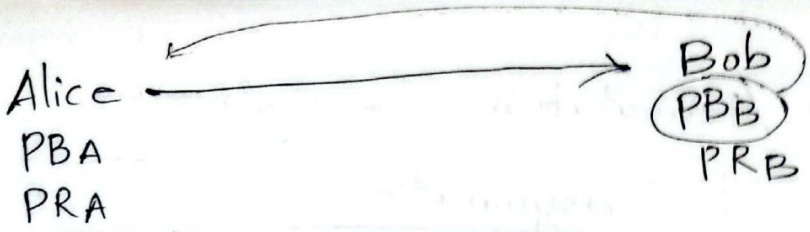
Decryption → Private key

Padlock

lock → Public key

Unlock → Private key

CamScanner



Bob PB key send and encrypt
PR key দিয়ে decrypt

Alice send ~~put~~ PB key to Bob . Alice PR key দিয়ে decrypt.
Sender এর কাজ বেশি

* Fig 10.1
* Pg 321 Fig 10.2 Authentication, Authorization

eve cipher publickey
public

* plaintext / ciphertext
The message must be encoded as an integer.

* Encryption / Decryption
.. mathematical function

$C = f(k_{public}, P)$ → Ciphertext

$P = g(k_{private}, C)$ → plaintext

f and g

trapdoor one-way function - only one way possible.

f^{-1}

$f(x) = x^3 + x^2$

$f'(x) =$

$5 \cdot 7 = 35$

$p \cdot q = n$

Encryption → Public key

(5) 7 = 10000000000 · square root

PB key

* Functions

$f(x) = x^2 + 2$

$f(1) = 3$

* One-way Function
  1. f is easy to compute
  2. f^{-1} difficult to compute

* Example 10.1

10.2 RSA cryptosystem → Math আসবে

14 Sept 2025

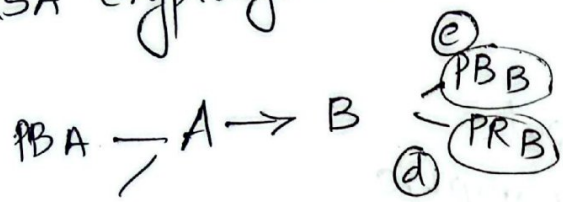
Recap

A → B

receiver { Public → encryption
Private → Decryption

Trapdoor one-way functions (Rivest, Shamir, Adleman)

* RSA Cryptosystem



encryption ला Bob चा key use करू।

encryption PB →

← Decryption PRB

Introduction

* Fig 10.5

Alice $C = P^e \bmod n$

Bob $P = C^d \bmod n$

Eve — e, n

Computational complexity

$\sqrt[e]{n}$

Bob

$e \cdot d \bmod n \equiv 1$

e th rest

$\sqrt[e]{n}$

Pg 328

* Fig 10.6

1) Encryption / Decryption Ring +, ×

2) key-Generation group

group multiply use करू

CamScanner

* Algorithm 10.2 RSA key generation

$p = 3 \quad q = 7$

$n \leftarrow p \times q = 3 \times 7 = 21 \quad n = 21$

$\phi(n) \leftarrow (p-1) \times (q-1) = 2 \times 6 = 12$

Select e such that $1 < e < \phi(n)$ and

e is coprime to $\phi(n)$ — 2 - 11

$\boxed{gcd(e, \phi(n)) = 1}$

$gcd(5, 12) = 1$

$d \leftarrow e^{-1} \bmod n$

$d = e^{-1} \bmod n$

$de = 1 \bmod n$

$de \bmod n = 1$

5 5 12

12

7 7

$c = p^e \bmod n$

plaintext

$c^d \bmod n$

* Example 10.5

one-way Trapdoor

$p = 7 \quad q = 11$

$n = 77$

(e) $\phi(n) = (p-1)(q-1)$

$= 6 \cdot 10$

$= 60$

$ed \bmod 60 = 1$

$13 \cdot d \bmod 60 = 1$

$d = 37$

Cannot do 13^{-1}.

* Example 10.7

"NO"

13 14

$(1314)^{343} = 33677 \bmod 159197$

13 14

Q) $p = 3, \quad q = 11$

$n = p \times q = 33$

$\phi(n) = (p-1)(q-1)$

$= 2 \times 10$

$= 20$

$\gcd(7, 20) = 1$

$e = 7$

$7 \times d \bmod 20 \equiv 1$

~~$d = 3$~~ $7 \times 3 \bmod 20 \equiv 1$

$d = 3$

$d = e^{-1} \bmod n$

$d = \frac{1}{e} \bmod n$

$de = 1 \bmod n$

$C = p^e \bmod n$

$M = 31$

$C = 31^7 \bmod 33$

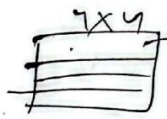
$= 27512614111 \bmod 33$

CamScanner

CT-2 Review
chpt-7 AES

1) Fig 7.1
2) Data units
3) state – Matrix প্রত্যেকটা byte
4) Block
5) Bit
6) Byte
7) Fig 7.5 Basic structure with description
replace state
depends on marks & time

Fig ✗ Subbytes
Fig 7.6
math আসবে না

shift Row
math আসবে


No Fig
Fig 7.9
১ করে, ২ করে

* Mix columns → Final must come
Constant matrix দেওয়া থাকবে
math আসবে


Fig 7.13

* Fig 7.15 Add Round key

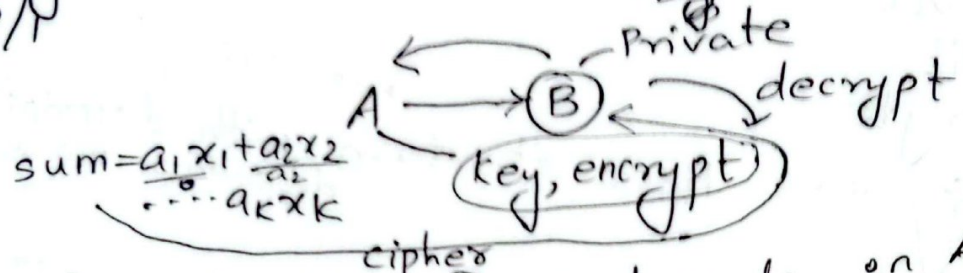
20 September 2025 * Definition

Pg 324

$a = [a_1 \ a_2 \ \cdots \ a_K]$ → Public

msg → $X = [x_1 \ x_2 \ \cdots \ x_n]$

o/p



কোনো value নিবো, নিবো depends on Alice's message

$a = [3 \ 6 \ 9]$

$X = [0 \ 1 \ 1]$

Sum = 6 + 9

= 15

15 [3 6 9]

* Superincreasing tuple

1 2 3

$a_i \geq a_1 + a_2 + \cdots + a_{i-1}$

array টা কিভাবে দিয়া আছে

0	1	0	1
1	2	3	6
0	1	0	1

⇒ 2 + 6 = 8

8 > 6 in place of 6, 1 and subtract

* Table 10.1 values of i, a_i, s, and x_i in Example 10.3

[17 25 46 ⋯ 400]

272

CamScanner

400 > 272

400 %6 = 0

01010

Inverse sum

Pg 325

* Fig

knapsack sum → simple/superincreasing [n, r]

b = [b1, b2, ... bk] → superincreasing

b1	b2	b3	b4
1	2	7	15

n = 20

r = 3

public

bk > n

r < bk

r * b1 mod n = a1

r * b2 mod n = a2

.

[a = a1, a2, ... ak] → hard

b = [b1, b2, .. bk] → simple/superincreasing

n, r

a = [a1, a2, ... ak] → hard

it will be given, s, n, r, b

$s' = r^{-1} \times s \bmod n$

s = knapsackSum (x, a) → s

Encryption (s, a)

c.

d.

e. permutation not there ×

*Example 10.4

$1 \le r \le n-1$

$n > b_1 + b_2 + \cdots + b_k$

$b = [7, 11, 19, 39, 79, 157, 313]$ simple

$n = 900 \quad r = 37$

$\gcd(900, 37) = 1$

$t_i = r \times b_i \bmod n$

$t = [259, 407, 703, 543, 223, 409, 781]$ hard

replace t with a

d.x

Encryption

$s = \text{knapsackSum}(a, x) = 2165$

$s' = s \times r^{-1} \bmod n = 2165 \times 37^{-1} \bmod 900 = 529$

x কে r দিয়ে গুণ করে

Inv knapsack এর উত্তর যোগ আছে এটা answer.

Another Book -

$b = [1 \quad 2 \quad 4 \quad 8]$

$n = 20, \quad r = 7$

$\gcd(20, 7) = 1$

14
16
30

Hard knapsack বানানো

$a = [7 \quad 14 \quad 8 \quad 16]$

$7 \times 3 \bmod 20 = 1$

Alice

$p = [0 \quad 101 \mid 0110 \mid 1000]$

x মানে

Exp.

$X = [0101]$

Sum = 30

$s' = s * r^{-1} \bmod n$

$= 30 \times 3 \bmod 20$

$= 90 \bmod 20$

$= 10$

CamScanner

inv (5, b)

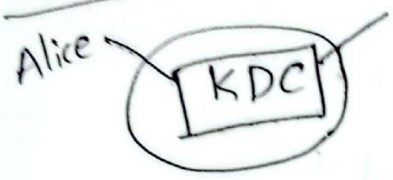
(10, 5)

8	10	1	2
4	2	0	2
2	2	1	0
1	0	0	0

0101

21 September 2025

Diffie hellman



Key Distribute

Prime number $n = 11 \rightarrow (1-10)$

Alice, $g = 7$ BOB

$g < P$

$(1-P-1)$

$3^1 \bmod 11 = 3$

$3^2 \bmod 11 = 9$

$3^3 \bmod 11 = 5$

⋮

$3^{10} \bmod 11 =$

$7^1 \bmod 11 = 7$

$7^2 \bmod 11 = 5$

$7^3 \bmod 11 = 2$

$7^4 \bmod 11 = 3$

$7^5 \bmod 11 = 4$

$7^6 \bmod 11 = 6$

$7^7 \bmod 11 = 1$

$7^8 \bmod 11 = 8$

$7^9 \bmod 11 = 9$

$7^{10} \bmod n = 10$

$$\{1-(n-1)\}$$
$$1 \cdot 2 \cdot 3 \cdots (n-1)$$

Power

g mod n =

$3^1 \bmod 11 = 3$

$3^2 \bmod 11 = 9$

$3^3 \bmod 11 = 5$

$3^4 \bmod 11 = 4$

$3^5 \bmod 11 = 1$

$3^6 \bmod 11 = 7$

$3^7 \bmod 11 = 9$

$3^8 \bmod 11 = 5$

$3^9 \bmod 11 = 8$

$3^{10} \bmod 11 = 1$

Alice

X

private

$g^x \bmod n$

$7^3 \bmod 11$

$= 2$

Bob

Y

private

$g^y \bmod n$

$7^5 \bmod 11$

$= 10$

2

10

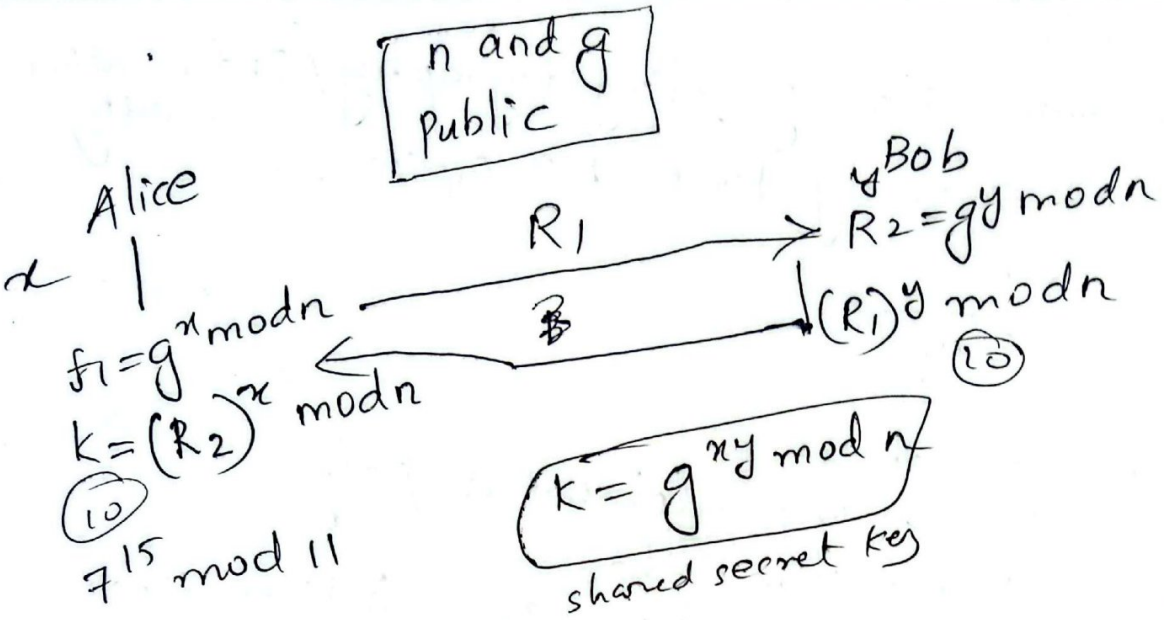
$10^3 \bmod 11$

$\Rightarrow 10$

$2^5 \bmod 11$

$\Rightarrow$

CamScanner



$k = g^{10} \bmod n$

$= 7^{10} \bmod 11$

$=$

27
28
04
11
12 → CT

27 – hashing

28 – Digital signature

04 – Theory

11 – Review class

12 → CT

complex Eng. Asg → 22.10.25

27 Aug 2025

Network Security / Cryptography / Information Security

Network Security Most IMP Topics for GTU Exam -

Chirag's Blog

- one time pad cipher
- Differentiate b/w monoalphabet & poly
- Columnar Transposition cipher
- Differentiate Transposition & substitution cipher
- stream ciphers and Block cipher
- Feistel cipher structure (DES)
- DES Algorithm
- strength & weakness of DES
- AES
  - Sub Byte
  - Shift Rows
  - Mix Column
  - Add Round key
  - Key Expansion in AES

Unit 2

Unit 3

- Double DES
- Triple DES

Unity

- Public key cryptosystems with Application Requirement and Cryptanal
- RSA algorithm
- Diffie-Hellman key Exchange algorithm

CamScanner

Unit 5 SH-512

- Hash.
- Secure Hash Algorithm (SHA-1)
- Introduction of Hash function
- Application of Hash Function

কি, প্রয়োজনীয়তা, কাজ

× Unit 6

Unit 7

Unit 8
- ~~Rec~~ Diffie

Not impt

× 3, 6, 8, 9, 10
Not there

1, 2, 4, 5, 7
very impt

Introduction Of Hash Function / Properties of Hash Function / Characteristics of Hash Function

* Introduction

$h(x) = 2x+1$
$= 3$
$= 5$

* Properties of hash function
- Compression
- Pre-image resistance

$x = H(m)$

x → hash value, m → msg

* Weak collision Resistance $H(m_1) = H(m_2)$
* Strong collision Resistance

* Characteristics of hash function

P = 101
$x^4 + x^2 + 1$
313

- it is impossible to generate message from given hash value

- Applications

Diagram not needed if more marks then need

- Secure Hash Algorithm - 1 | working of SHA 1 |

compare different versions of SHA

* Introduction

SHA-1, SHA-256, SHA-384 and SHA-512

produces a 160-bit output called message digest.

264 bits

* Features of SHA-1

Padded
fixed length এর জন্য 0 or 1 add করি last e

multiple of 512

10000
20000

1000 + 24 = 1024
512 × 2

* Steps

step-1 : Padding
step-2 : Append length → 1000 | 24 | 00000 | 00 | 00
msg padding

how will we know the length
101 1010 10
101000

msg padding original msg length

101 000 011
512 64 bit

CamScanner

$[\ ]_x \oplus [\ ]_y$

011

Step-3 Divide the input into 512-bit blocks

1024
512 512

~~Step-4~~

2048
512×4

2048

32×5
=160

step-4 Initialize chaining variables

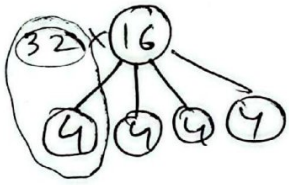
step-5: Process Block & output

ABCD E = E + Process P + $S^5(a)$ + W(t) + K(t)

1000 + 24
1024
512 512
32×16 4×4
20 80

16টি 32-bit এর block
generate হবে।

1 round এ 4টি



A
|
S^5

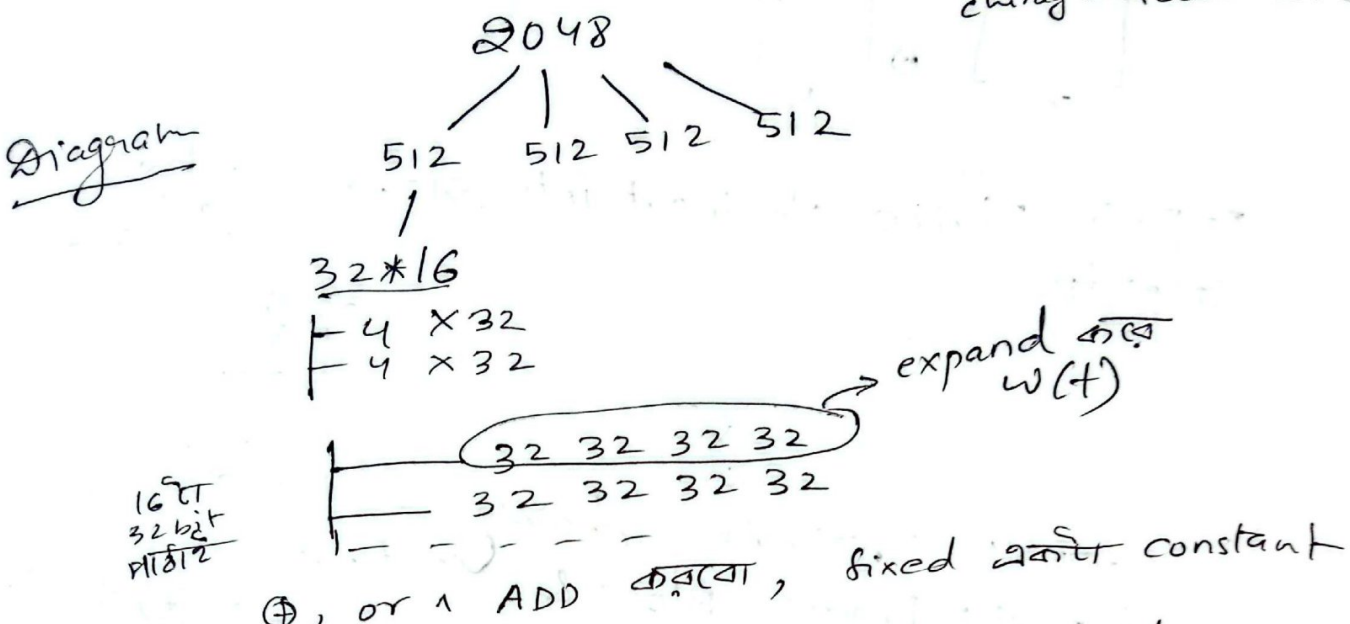
5 বার
left shift

Process P
logical process / function / Boolean function

$(B \oplus C) \wedge (B \wedge C) \vee (B \oplus D)$

W(t) → Expanded message word of round t
K(t) → round constant of round t

Diagram



⊕, or ^ ADD করবো, fixed একটা constant

Fig, Hash function, steps, intro, character, Hash value কেনো লাগে

CamScanner

5 October 2025

Chapter 13. Digital Signature

CT-3 next sunday
classtime 11 am on Digital Signature

msg → A... → signature

msg ফাংশন যাবে

13.1 comparision

Diff. name

inclusion - msg, signature

VIMP verification - msg key signature

417 Pg Relationship - one to many (এক মূলে document এ একটা signature) signature msg থেকে তৈরি করা হয়, Different msg থেকে different signature তৈরি হয়,

Duplicity

↳ ২টা signature এ diff থাকে।

Process

Fig. 13.1

Fig 13.2

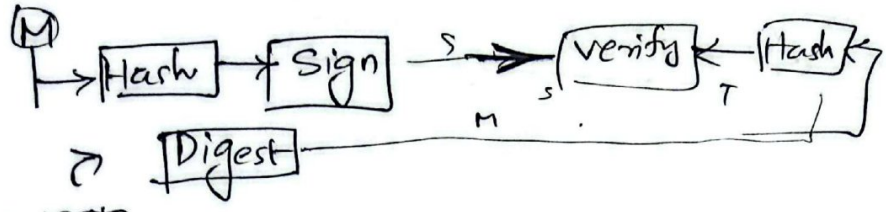
Signing ↓ Private key — Alice

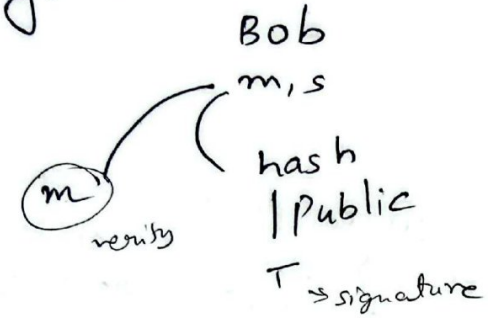
Alice → Bob — verifying ↓ Public key — Alice

C D secret key জানতে হবে

Asymmetric use করা হয়। No symmetric

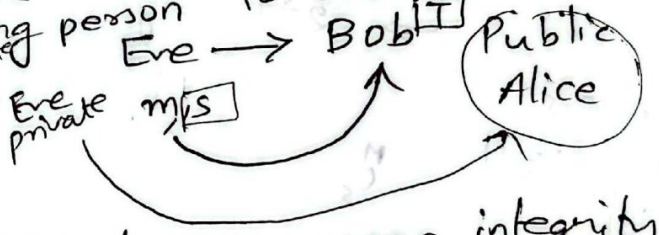
* Fig 13.3 Basic structure





13.3 Services

* Message Authentication
  If it comes from wrong person to check that.



* Message Integrity

A digital signature provides message integrity
→ h1
→ h2
message change করলে hash value change হয়ে যায়।

* Non repudiation
Third party → ~~Translate~~ Trusted center
↓
সবকিছু save করে রাখে

Fig 13.4

* Confidentiality
ভাঙ্গি যে msg পাঠাচ্ছি confidential থাকা so that they can't catch

Fig 13.5

CamScanner

Encrypt
Receiver এর public key encrypt করে

Receiver এর private key দিয়ে decrypt করে.

Draw figures 13.4 , 13.5

Figure, and theoretical.

ncs theory

1 set

Computer and Network Security: Threats, Malware, Attacks, vulnerability

For Theory read this pdf

Assets, unlocked door is a vulnerability, thief is a threat, malware-

* Network security Threats

1.

8. Man-in-the-Middle

Malware – Malicious software

* Types of Malware
* Vulnerabilities (weaknesses - bugs, unpatched code

* Attacks
* Common Attack types

* Countermeasures
Keeping software patch
Firewall
Enforcing
Encrypting sensitive data
Conducting Regular backups

Firewall

Defn
Why do we need firewall
Types of firewall
- Hardware
- Software

Install
Hardware firewall
software firewall

Packet filter

Application gateway

Legal and Ethical Issue

- Security aspects of computer
right এর বিপরীত unethical
- Copyrights (unethical)
- Patents
protect করা
- Trade secret
- Comparison
- computer crime
- Law

Ethics and Laws difference

- Ethics
- Comparison
- Ethical reasoning
scenario : case study
case

CamScanner

18 Oct 2025

chpt - 1 Introduction (10 marks)

1) Taxonomy of security goals (CIA)
2) Confidential, Integrity, Availability
3) Fig 1.2
4) Active & Passive attacks
5) Service and Mechanism

Point গুলো মনে রেখো

Fig 1.3
- security services
- Table 1.2

Fig 1.4

If not direct then short Question আসবে

chapt 2 : Mathematics of Cryptography

(Congruence)

↓

কিভাবে বের করে জানতে হবে

MI

$-$ = 7 (mod n)

$15 = 7 \pmod{26}$

chapt 3 : Traditional symmetric key ciphers

same key encrypt & decrypt use হয়

1) Fig 3.1 General idea of symmetric-key cipher.
2) Fig 3.3 Cryptoanalysis attacks (scenario based like CT)
   4 attacks
3) Substitution cipher - Monoalphabetic, Polyalphabetic ciphers
4) Additive cipher
   Fig 3.9

5) Multiplicative cipher

Fig 3.10 (7, 4)

6) Affine cipher ← Multiplicative + Additive

7) Polyalphabetic cipher

autokey cipher Example 3.14

8) playfair – should be even number

2jon করে করা

Pair

aa+s

ab at

sabatsx

Rules to use cipher for encryption

a a

(1,1) (1,1)

9) Vigenere cipher

10) Table 3.3

11) Fig 3.14

key : Pascal

| | | | | |

she is l

is ten i

she is Reading

	P	a	s	c	a	l
H	s	h	e	i	s	R
T	e	a	d	i	n	g

12) Transposition ciphers

Meet me at gate

c by c নিয়ে যাবো

R by R বাড়াবো

R=4

M	m	g
e	e	a
e	a	t
t	t	e

keyed & keyless transposition ciphers

13) Combining two approach

Fig 3.21

CamScanner

Network

27
6 1 2 3 4 5 6 7

Fig 3.22 Double Transposition cipher

14) Stream and Block ciphers
why it is called ?