After MidSem

(Missed 2 classes - 24th, 25th Sept)

26th Sept

Play fair Cipher (Used by British Army during IInd World war :o)

Secret key → of 25 alphabets arranged in 5×5 matrix

- Different arrangement of letters in matrix can create many different secret keys

Before encryption, use bogus characters if required

Rules: If 2 letters in a pair ~~aa~~ are located in same row of secret key, corresponding character for each letter is next letter ~~for character on~~ to the right in same row

If 2 letters are located in the same column of secret key, corresponding encrypted character for each letter is letter in same column

If 2 letters in a pair are not in same row or column, corresponding encrypted character is in its own row but column of other letter

26th Sept

Secret key

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

hello → Add bogus character → helxlo → Varna ll ka pair ban jayega

1) he → same row → ec (EC)
2) lx → same column → qz (QZ)
3) lo → diff row, diff col → bx (BX)

Cipher text generated → ECQZBX (Plain text cipher)

Vignere Ciphere

Use of keystream → Repitition of initial secret key stream

P = P_1 P_2 P_3 C = C_1 C_2 C_3

K = [(K_1, K_2, K_3 ...), (K_1, K_2, K_3 ....)...

Encryption : $C_i = P_i + k_i$

Decryption : $P_i = C_i - k_i$

Eg: "She is listening"

keystream = "PASCAL"

So keystream is (15, 0, 18, 2, 0, 11)

Plaintext:	s	h	e	i	s	l	i	s	t	e	n	i	n	g
P's value	18	07	04	08	18	11	08	18	19	04	13	08	13	06
keystream:	15	00	18	02	00	11	15	00	18	02	00	11	15	00

26th Sept

C's value : 33 07 22 10 18 22 23 18 11 06 13 19 02 06

↓ Add karke % 26 karo

↓ 07

h h w k s w x s l g n t c g

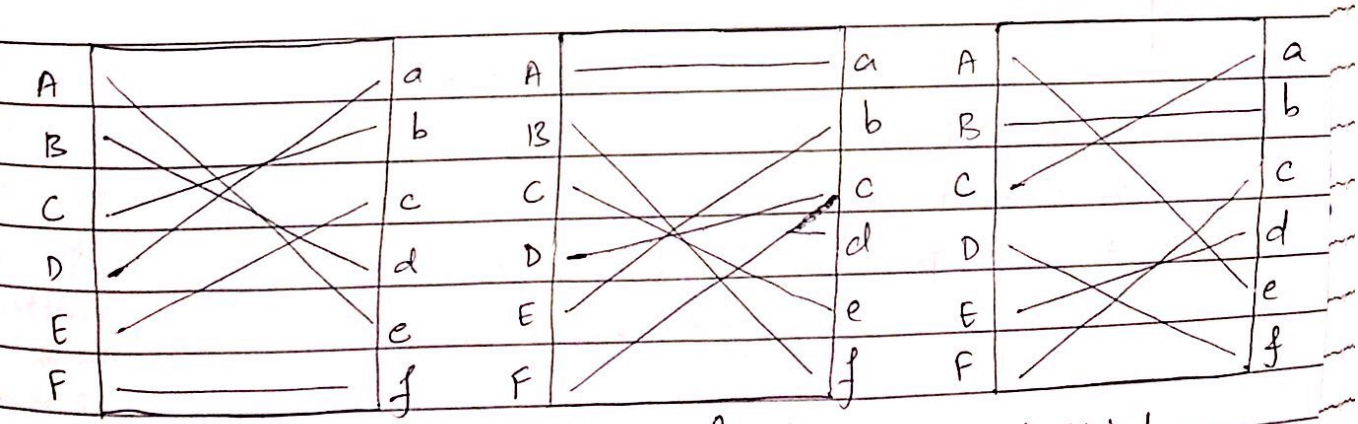
One time pad

1. For per feet secrecy
2. By shannon - Each plaintext symbol is encrypted with a key randomly chosen from key domain
3. Eg. In additive cipher, same key is used to encrypt but for perfect secrecy we have to choose randomly from key

* Eg. I^st ~~chamber~~ characters encrypted using key 04 & second with 21

Rotor Ciphers

Uses mono-alphabetic idea but changes mapping between plain text & cipher text characters



bee → BCA → (Poly-alphabetic cipher)

bee: initial, after first, after second

If we use only initial setting → BAA (mono-alphabetic)

27th September

Transposition Cipher

1. It does not substitute one symbol for another, instead it changes location with another.
2. eg 1st position may appear at 5th position
   9th position may appear at 7th position
3. Transposition ciphers reorder symbols

Keyless transposition ciphers

1. Text may be written column by column and read row-wise

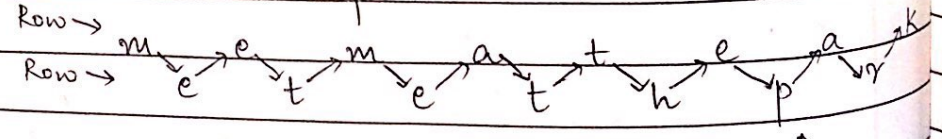
OR

Text may be written row by row and read column-wise

2. Eg. Rail-fence ciphers

"meet me at the park"

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



memate.aketethpr

Ciphers text

Written column-wise & read row-wise

7th September

Keyed Transposition Ciphers

1. Divides plaintext into blocks
2. Then use a key to generate cipher text

Eg. e n e m y a t t a c k s t o n i g h t
1 2 3 4 5

to complete 5 we add a bogus character

i g h t z

Key used

3	1	4	5	2
1	2	3	4	5

1st position is uss block ka 3rd character

e e m y n t a a c t t k o n s h i t z g

Combining two approaches - (Keyless & Keyed)

1. Text written into table (row by row)
2. Permutation done by reordering
3. New table is read column by column

e n e m y a t t a c k s t o n i g h t z → bogus character added

↓ write row by row

e	n	e	m	y
a	t	t	a	c
k	s	t	o	n
i	g	h	t	z

↓

e	e	m	y	n
t	a	a	c	t
t	k	o	n	s
h	i	t	z	g

3	1	4	5	2
1	2	3	4	5

27th September

↓ Read column-wise

ettheakimaotycnznts g

Cipher text: ETTHEAKIMAOTYCNZNTSG

- Always write cipher text in capitals

ON RECEIVER SIDE

① Write column-wise

e e m y n
t a a c t
t k o n s
h i t z g

② Apply decryption key
1st position becomes 3rd

key				
3	1	4	5	2
1	2	3	4	5

e n e m y
a t t a c
k s t o n
i g h t z

③ Read row-wise

enemyattacketonightz

Missed a class (1st October)

3rd October

AES (Advanced Encryption Standards)

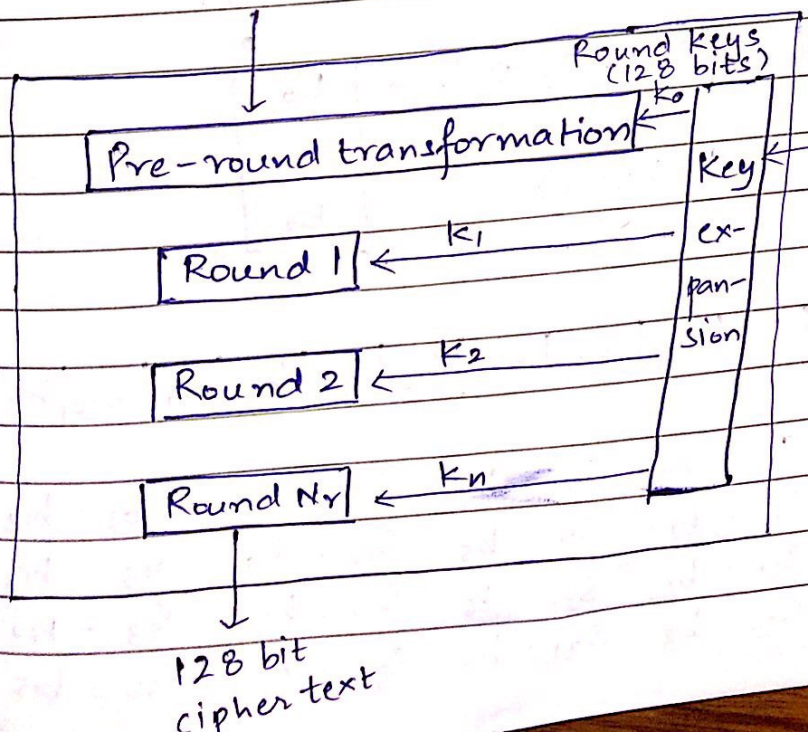
- Symmetric key Block Cipher
- NIST (National Institute of Standard & Technology)
- Block-size (128 bits)
  Key sizes → 128, 192 & 256 bits

1st Conference ← (15 out of 21 algorithms selected)
2nd Conference (5 out of 15 algorithms selected)
3rd Rijndaer selected as AES (October 2000)

Criteria

- Security → 128 bits
- Cost → H/W, S/W, Implementation Cost technology
- Implementation → flexibility, simplicity

General design of AES encryption cipher



3rd October

(Relationship between number of rounds & key sizes)

Nr	Key sizes
10	128
12	192
14	256

AES → AES-128, AES-192, AES-256 } Versions of AES

Data Units

Byte

Byte → b0 b1 b2 b3 b4 b5 b6 b7 → [b0, b1, b2, b3, b4, b5, b6, b7]

b (1 byte) — b (8 bits) — b

Word

Word → B0 B1 B2 B3 → [B0, B1, B2, B3]

w — w (4 bytes) — w

Block

b0	b1	b2	b3	b4	b5	b6	b7	b8	b9	b10	b11	b12	b13	b14

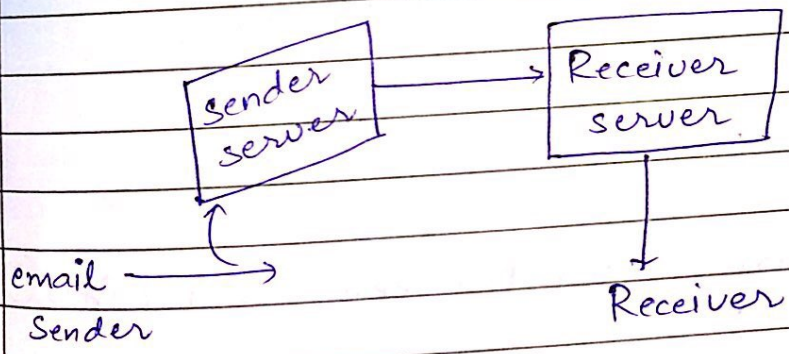
State

$$\begin{bmatrix} S_{00}=b_0 & S_{01}=b_4 & S_{02}=b_8 & S_{03}=b_{12} \\ S_{10}=b_1 & S_{11}=b_5 & S_{12}=b_9 & S_{13}=b_{13} \\ S_{20}=b_2 & S_{21}=b_6 & S_{22}=b_{10} & S_{23}=b_{14} \\ S_{30}=b_3 & S_{31}=b_7 & S_{32}=b_{11} & S_{33}=b_{15} \end{bmatrix} \rightarrow [W_0, W_1, \ldots]$$

7th October

SMTP (Simple Mail Transfer Protocol)

→ SMTP is application level protocol
→ SMTP is connection-oriented protocol
→ SMTP is text-based protocol
→ It handles exchange of messages between email server over TCP/IP network
→ It also provides notification regarding incoming mail



SMTP Response

• Sent from sender to client → between sender & receiver

1. positive completion reply (connection established successfully)
2. positive intermediate reply (some action may be pending)
3. Transient negative completion response (temporary error condition)
4. Permanent negative completion reply (connection establish nahi ho paa raha)

17th October

SMTP Commands (Inke functions dekh leno)

1. Hello
2. E·Hello
3. MAIL FROM
4. RCPT TO
5. SIZE
6. DATA
7. QUIT
8. VERFY
9. EXPN (same as VERFY except that valid users ki list bhi display hogi)

PROXY SERVER

- An intermediary server between client & internet

Functionality →

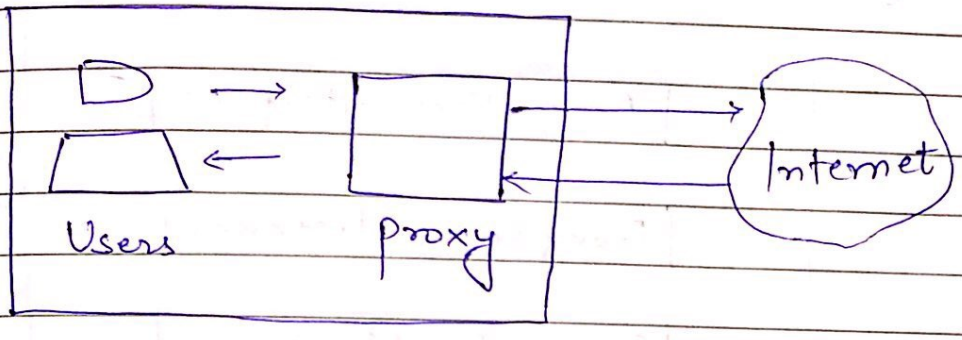
- Firewall & network data ~~fillo~~ filtering
- Network connection sharing
- Data caching

Purposes →

- Monitoring & Filtering
- Improving performance
- Translation
- Accessing services anonymously
- Security

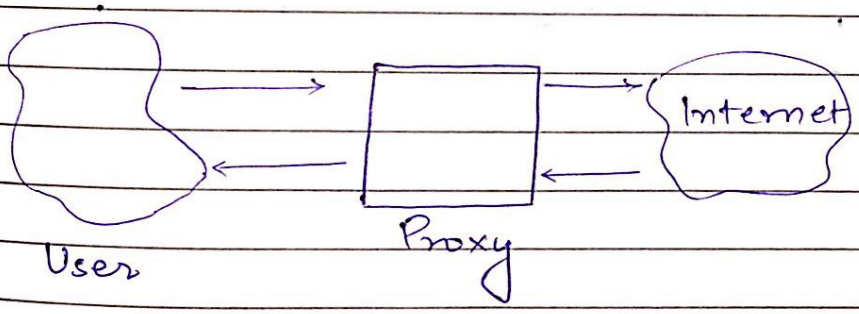
4th October

Forward Proxies



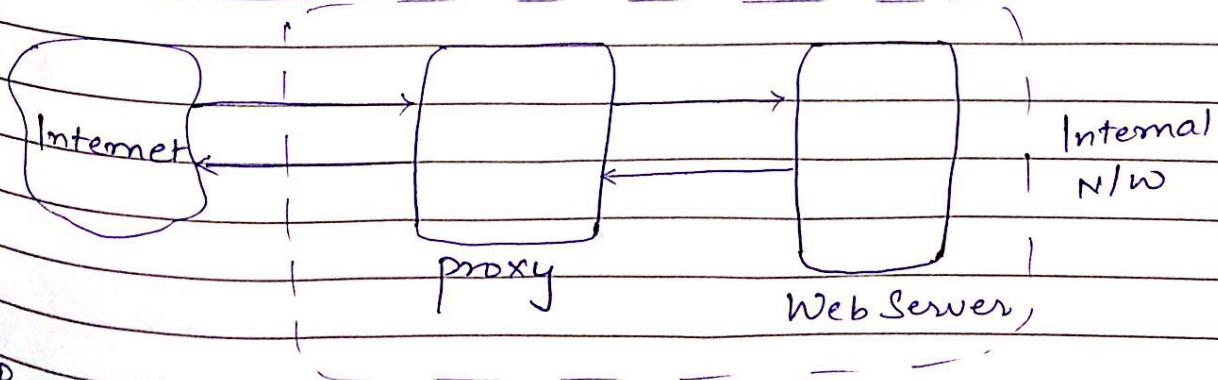
- In this, client requests ~~intermediate~~ network server to forward to internet

Open Proxies



Open proxies help clients to conceal their IP addresses while browsing web address.

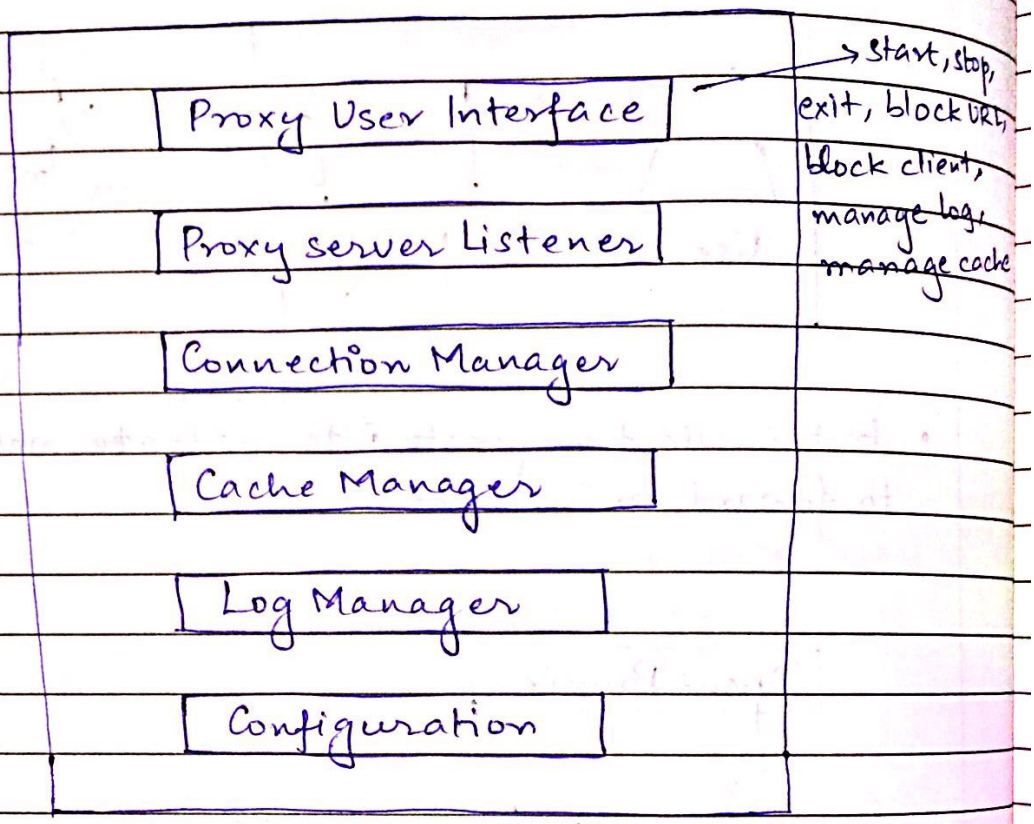
Reverse Proxies



Requests are forwarded to one or more proxy servers & response from proxy server is retrieved

17th October

Proxy Architecture



DNS (Domain Name System)

→ when DNS did not existed, one had to download a host file containing host names & their corresponding IP address

→ It is a hierarchical naming system & distributed database of IP addresses and associated names

IP Address

→ Unique logical address assigned to a machine over a network

→ Unique address assigned to each host on network

→ IP address is of 32 bits (4 bytes) long

→ Consists of 2 components : network component
host component

→ Each byte is a no. from 0-255 and each byte is separated from the other by a dot

Eg. 137.107.27.124

→ Domain names (are linked to IP addresses)

www.tutorialpoints.com
URL

18th October

URL Types

Absolute URL

- Complete address of a resource on the web

Eg. http://www.tutorialpoint.com/internet_technology/index.htm

where (1) http is the protocol
(2) tutorialpoint.com is servers (commercial servers)
(3) index.htm is filename
(4) internet_technology → koi directory hogi

- Absolute URL mein directory ka poora path dena padta hai
- Used to link web pages on different websites
- Difficult to manage
- Changes when server name & directory name changes
- Takes time to access

Relative URL

- This is partial address of webpage

Server name & protocol are omitted from URL

Eg. To link an image on website tutorialpoint.com/internet_technology/internet_reference_models/internet_technologies/internet_OSI_model.jpg

- Used to link web pages within same website.
- Easy to manage
- Remains same even if we change server name or directory name
- Comparitively faster to access

18th October

Domain Name System Architecture

→ Domain Names : Symbolic string associated with an IP address

↓

Country type domain

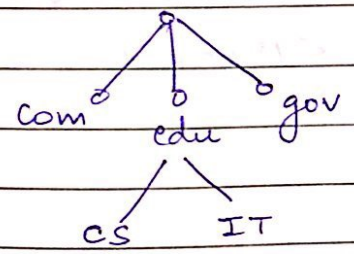
com - commercial, edu - education

Eg in - india, us - United states

→ Domain Name Space : refers to hierarchy in internet naming structure

hierarchy : 0 to 127, with root at the top

→ Name Server



23rd October

(entered very late)

- HTML

```
<HTML>
  <HEAD>
    <TITLE> Book </TITLE>
  </HEAD>
  <BODY>
    <H1> ——— </H1>
    <B> ——— </B>
    <UL>
      <LI> ———
      <LI> ———
      <LI> ———
    </UL>
    <P> ———
    <P> ———
  </BODY>
</HTML>
```

- Main focus on Structure

- XML

```
<XML version="1.0" ?>
<BOOK>
  <BOOKNAME> ———
  </BOOKNAME>
  <AUTHORS>
    <AUTHOR1> ——— </AUTHOR1
    <AUTHOR2> ——— </AUTHOR2
    <AUTHOR 3> ——— </AUTHORS
  </AUTHORS>
  <PRICE> ——— </PRICE>
  <PUBLISHER> ———
  </PUBLISHER>
</BOOK>
```

- Focus on hierarchy
- User defined tags