IT-401

Internet & Web Engineering

Date 27/8/18

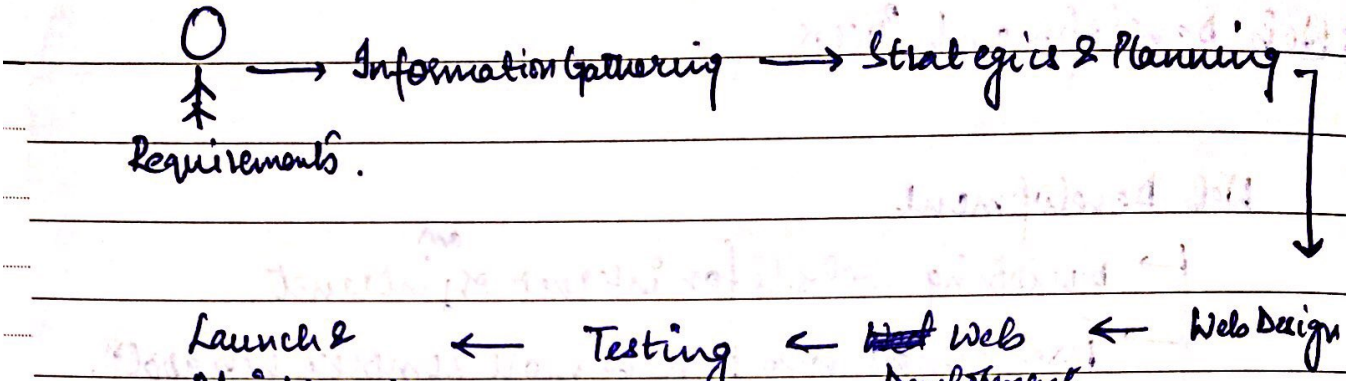
* Web Development Process

Web Development
- → Developing website for internet or an intranet.
- → From simple web page to more complex web appln.
- → CMS (Content Management System).
- → Web developers → Front End Developers
  - → Back End Developers.
- → Software → LAMP (Linux, Apache, MySQL, PHP)
  - Stacle, Adobe Dreamweaver,
  - ~~Micro~~ Microsoft Visual Studio, HTML.

Basics of Web development process.
- Graphic design / Web design.
- Information gathering and copy writing / copy editing with web usability, accessibility & search engine optimization.
- Mobile responsiveness
- ServerSide (functionality)
- Client Side (Layout design).
- Testing - To test whether product satisfies with customer's requirements or not.

MATRIKAS

Date: 29/8/18



Each Phase has its i/ps & o/ps.

(1) Innovative Requirements

Inputs → Interviews with clients, initial emails, discussion notes, estimated budgets.

Outputs → development process, estimated cost. H/w, s/w requirements, report documents, Team requirements, final client approval.

(2) Information Gathering

Inputs → Reports from clients, documentation from Bussiness analyst.

Outputs → complete project final documentation. with requirement specification.

MATRIKAS

Date : / / /

③ Strategies & Planning

Inputs → Final project documentation.

Outputs → Sitemap containing all web pages.

④ Web Design.

Designs website that supports good look, feel and makes different from other website.

⑤ Web development. → HTML, CSS.

Inputs → Websites with forms & complete requirement specifications.

Outputs → Website with database driven functions, coding documents.

Tools → Dreamweaver, CSS, HTML, Javascript. etc.

⑥ Testing

Inputs → website, requirements specifications, supporting documents, technical specifications & technical documentation.

Outputs → Testing reports.

Tools → GT matrix, Validation.

MATRIKAS

Date: / / /

⑦ Launch & Maintenance.

Inputs → Live website, analysis reports

Outputs → Updated website, maintenance reports.

* World Wide Web (WWW)

It is an information space where documents & other web resources are identified by URL (Unified Resource Locator)

↳ websites, webpages & web applications.

↳ interlinked by hypertext links and accessible via internet.

- Embedded hyperlinks permit user navigation.
- Multiple webpages with common theme, domain name make a website.

↳ primarily text documents formatted & with HTML (in addition have pictures, multimedias, video, audio & ~~&~~ components) that are rendered in the user's web browsers as coherent pages of multimedia content.

* Key Layers of Internet

Maturing of these 7 layers led to Youtube & Social N/wing

Content → how users are connected to content & served by content providers

Search Engines Important as if content cannot be found it is indistinguishable to content not existing from user's perspective.

Browsers Engaging User interface, displaying images etc along with hyperlinks & text.

WWW significant advancement in accessing information on the internet, by implementing HTTP

MATRIKAS

Date: / / /

Internet

Internet is the formation consisting of N/W of N/s enabled globally through a standard Internet Protocol (IP)

Network

N/W formed when multiple computers are linked together.

Computers

* USES of WWW

- publicity, marketing, advertising
- direct online selling
- Research & development
- Communication
- Collaboration.
- Use of multimedia.
- Electronic Mail, Educational needs

* Features of WWW

- Hypertext information system.
- platforms (cross-platform)
- Distributed
- Open standards, open source (TCP/IP, HTTP, HTML, CSS)
- Web browsers (provides single interface)
- Dynamic, Interactive, Evolving
- Rich user experience

MATRIKAS

Date: 30 / 8 / 18 /

* Introduction to Internet.

Internet → Global system of interconnected computer networks which uses protocols (TCP/IP) to link device worldwide.

ARPANET - Jan 1, 1983 (first internet).

Browsers → Programs of computer to access www.

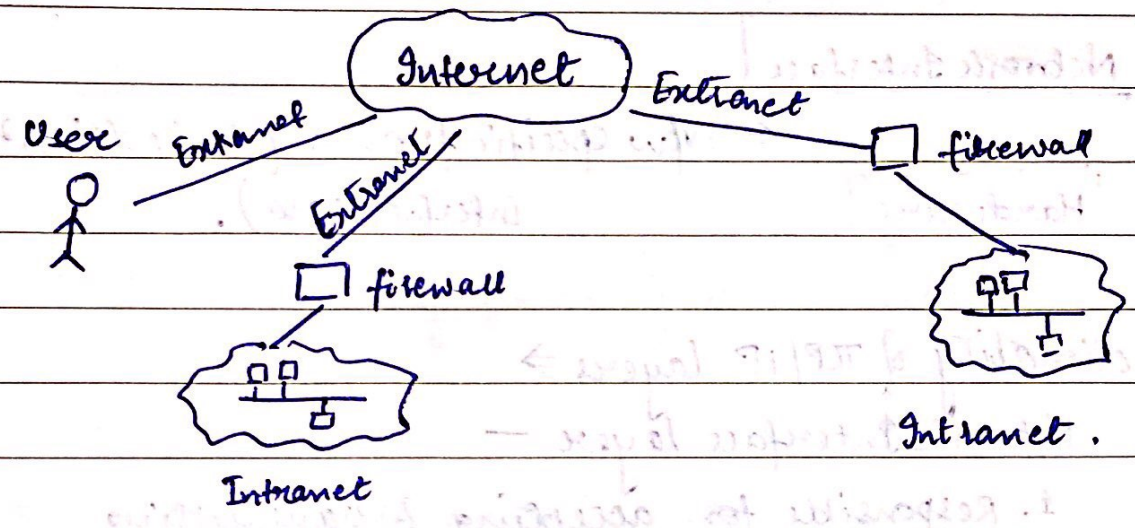
Internet connection →
- Dial up
- DSL (Digital Subscribes Line)
- Cable (with modem)
- Wireless or wi-fi
- Satellite
- Cellular.

Intranet →
- Intranet refers to collection of networks within logical body.
- It can be simple as two computers connected at home or as vast as two branch offices connected to each other
- Intranet has firewall or router.

Extranet →
- Extranet is private n/w that uses internet protocols, network connectivity
- Extranet can be viewed as part of company's intranet that is extended to users outside company.

MATRIKAS

Date : / / /



* Introduction to Internet Model.

- TCP/IP Model
- OSI Model.

TCP/IP ⇒

- TCP/IP Protocols originally developed by department of defence to connect networks.
- Services → file transfers, e-mail, remote logons.
- Packets → Information that travels across internet must broken down into smaller packets.

Packets = data + destination address + packet order.

Layer — objects passed b/w layers.

Application ← Messages for streams (TELNET, FTP emails etc)

Transport ← Transport protocol packets (TCP, UDP)

Internet ← IP datagrams (IP, ICMP)

MATRIKAS

Date: / / /

Network Interface

← N/w specific frames (device drivers & interface card).

Hardware

Functionality of TCP/IP layers ⇒

- Network Interface layer –
  1. Responsible for accepting & transmitting IP datagrams
  2. Contains device drives in OS & corresponding network interface card
  3. Handles h/w details.
- Internet Layer –
  1. Handles communication from one machine to other.
  2. Routing algorithms.
- Transport layer –
  1. Provides flow of data
  2. TCP/UDP
  3. Packet transmission
  4. Checksum added to packets.
  5. Regulates flow of ~~data~~ information.
- Application Layer.
  1. Invoke application layer
  2. Choose kind of transport needed i.e message or stream of bytes.

MATRIKAS

Date: 4/09/18

CRYPTOGRAPHY

It is an art & science of making a cryptosystem that is capable of providing information security.

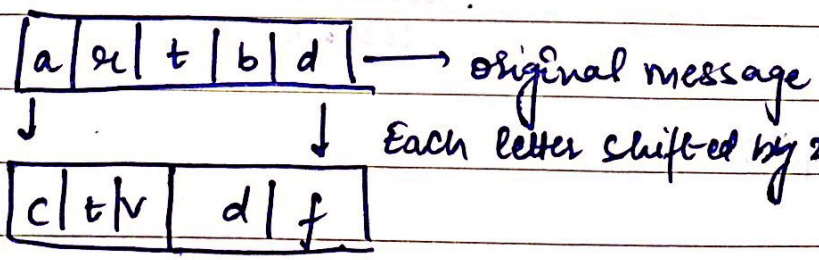
* Cryptanalysis

Art and science of breaking cipher text is known as cryptanalysis

- To test cryptographic techniques
- Confidentiality
- Data integrity
- Authenticity
- Non-repudiation.

* Caesar shift cipher

↳ Relies of letter shifting



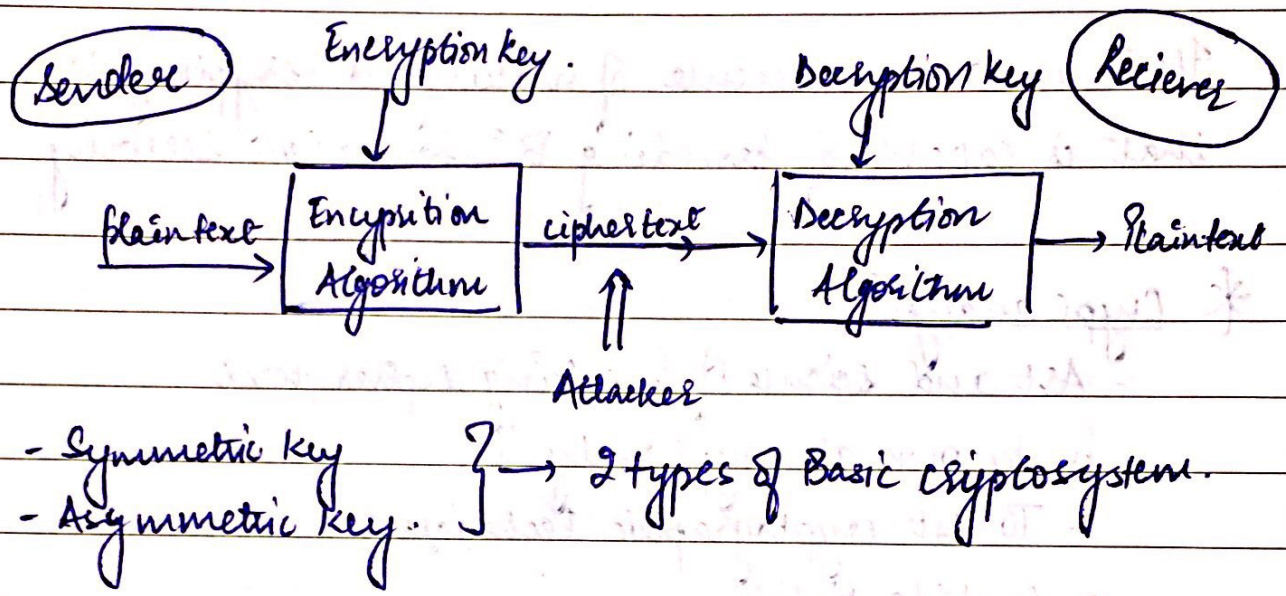
* Steganography

Use of images to hide message and send it.

MATRIKAS

Date: / / /

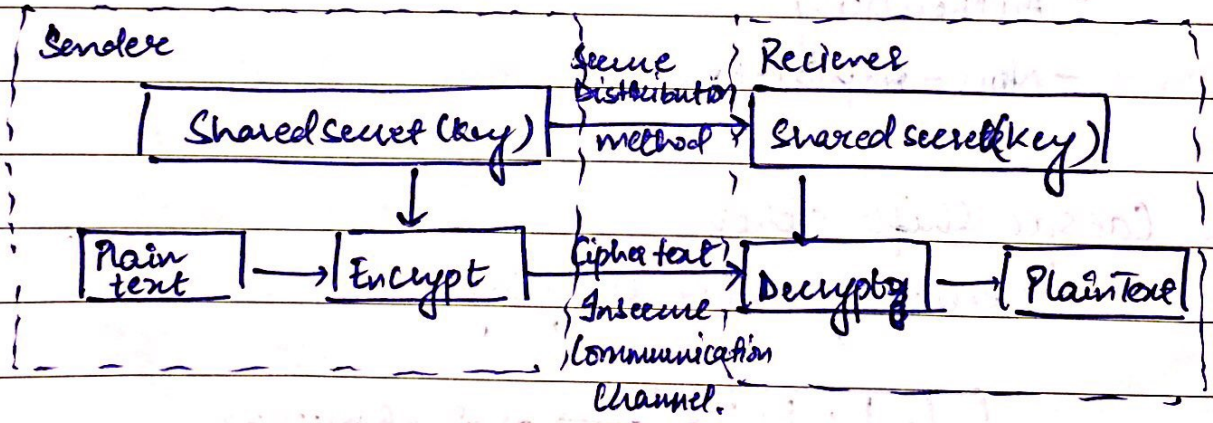
* Cryptosystem



- Symmetric key
- Asymmetric key.

} → 2 types of Basic cryptosystem.

* Symmetric key Algorithms



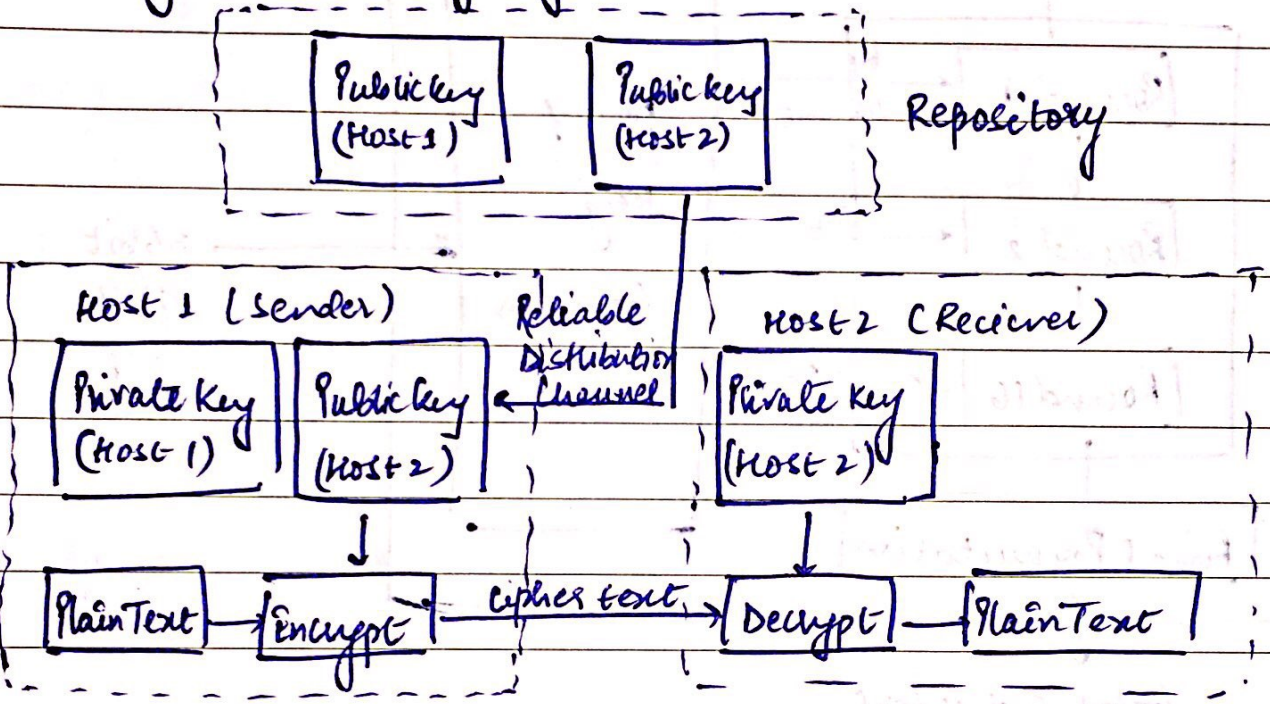
- Blowfish
- DES
- 3-DES

etc.

MATRIKAS

Date: / / /

* Asymmetric Key Algorithms.

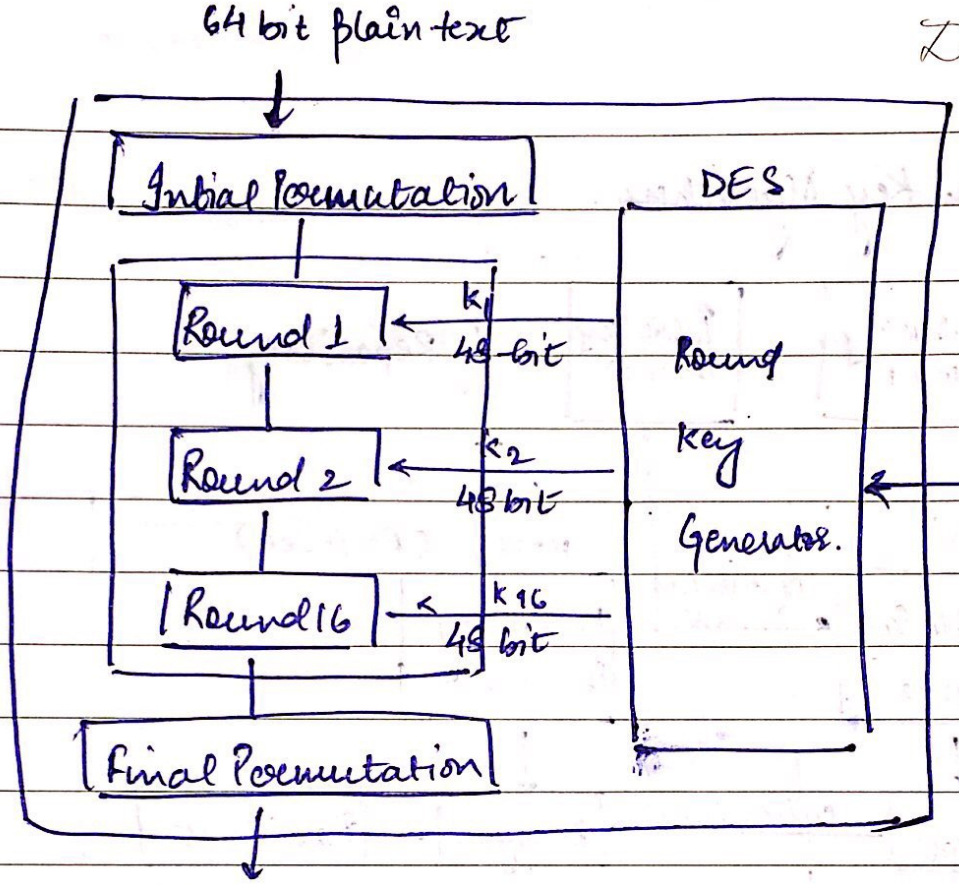


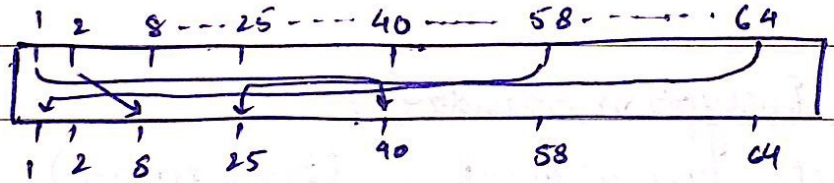
* DES (Data Encryption Standard)

- Symmetric key algorithm (Block cipher).
- Use of Feistel Cipher.
- Use 16 Round Feistel cipher.
- Key length is 56 bits.
- Use of round function & key.

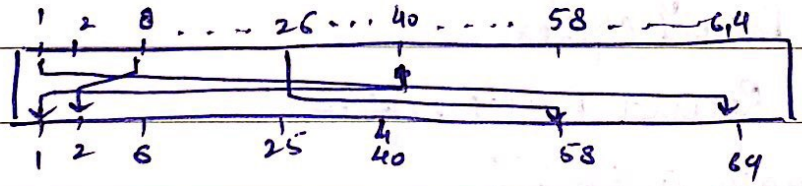
MATRIKAS

Date: / / /



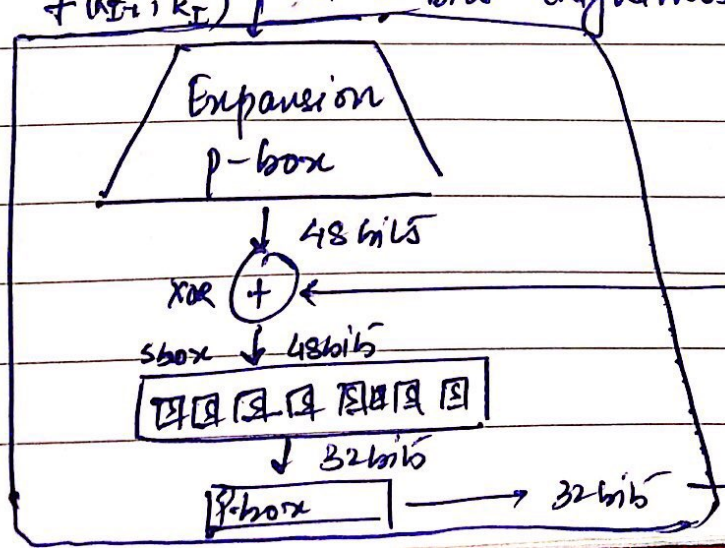


Initial Permutation.



Final Permutation.

Round function $f(R_{I-1}, k_I)$ In 32 bits (Rightmost bits).

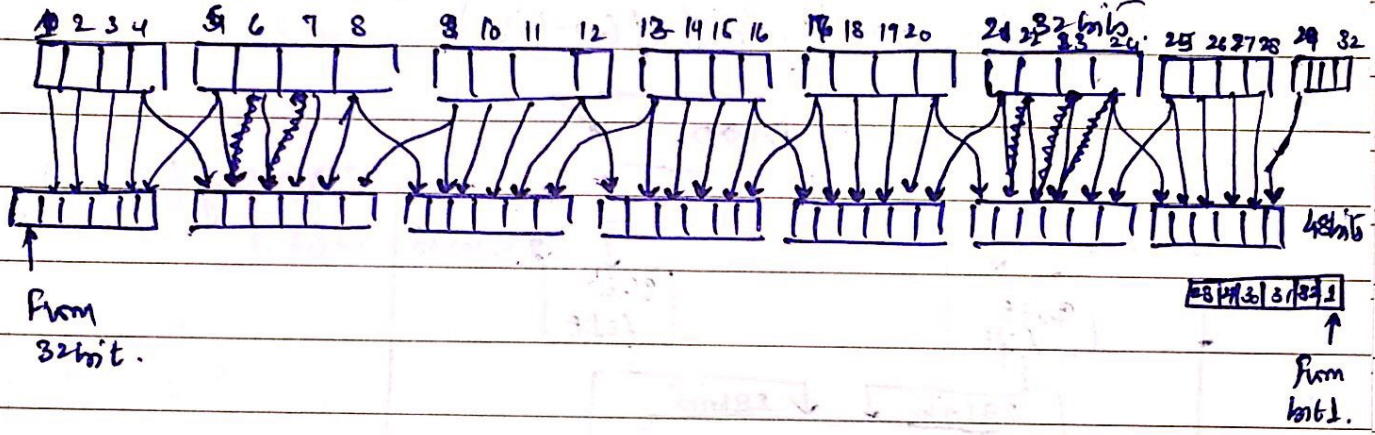


MATRIKAS

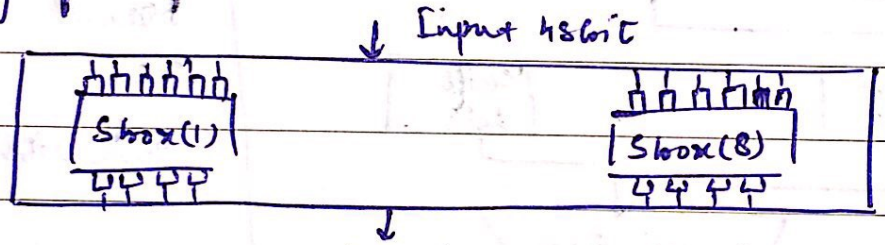
Date: 5/9/18/

Round function.

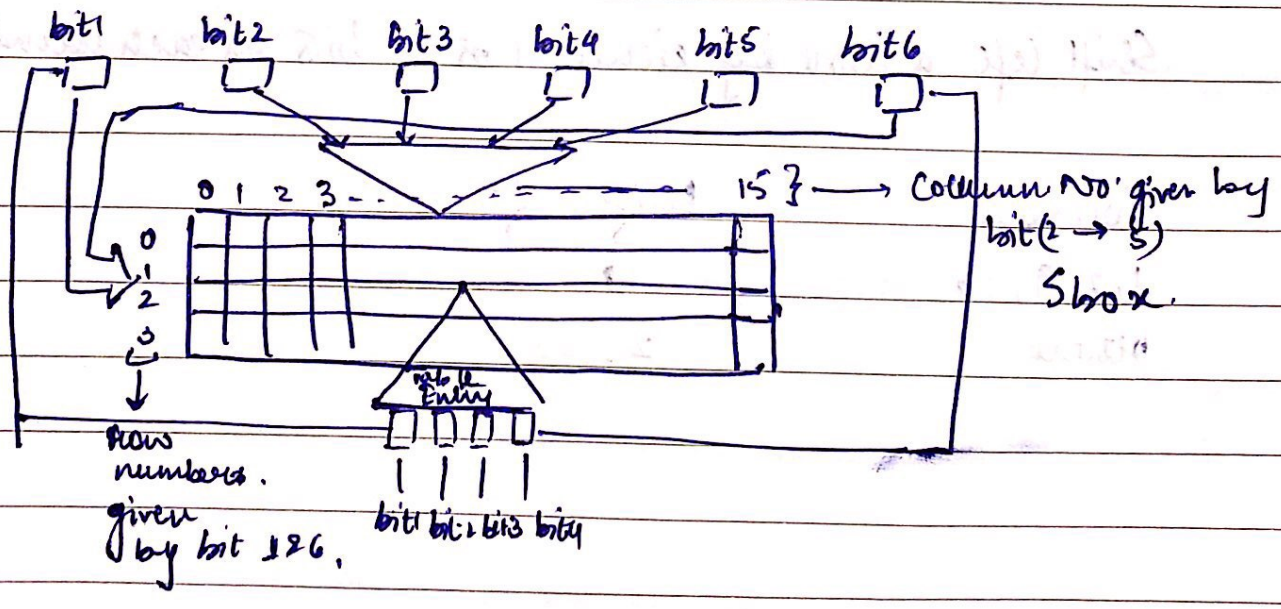
Expansion p-box. ⇒



Array of 8-Sboxes ⇒



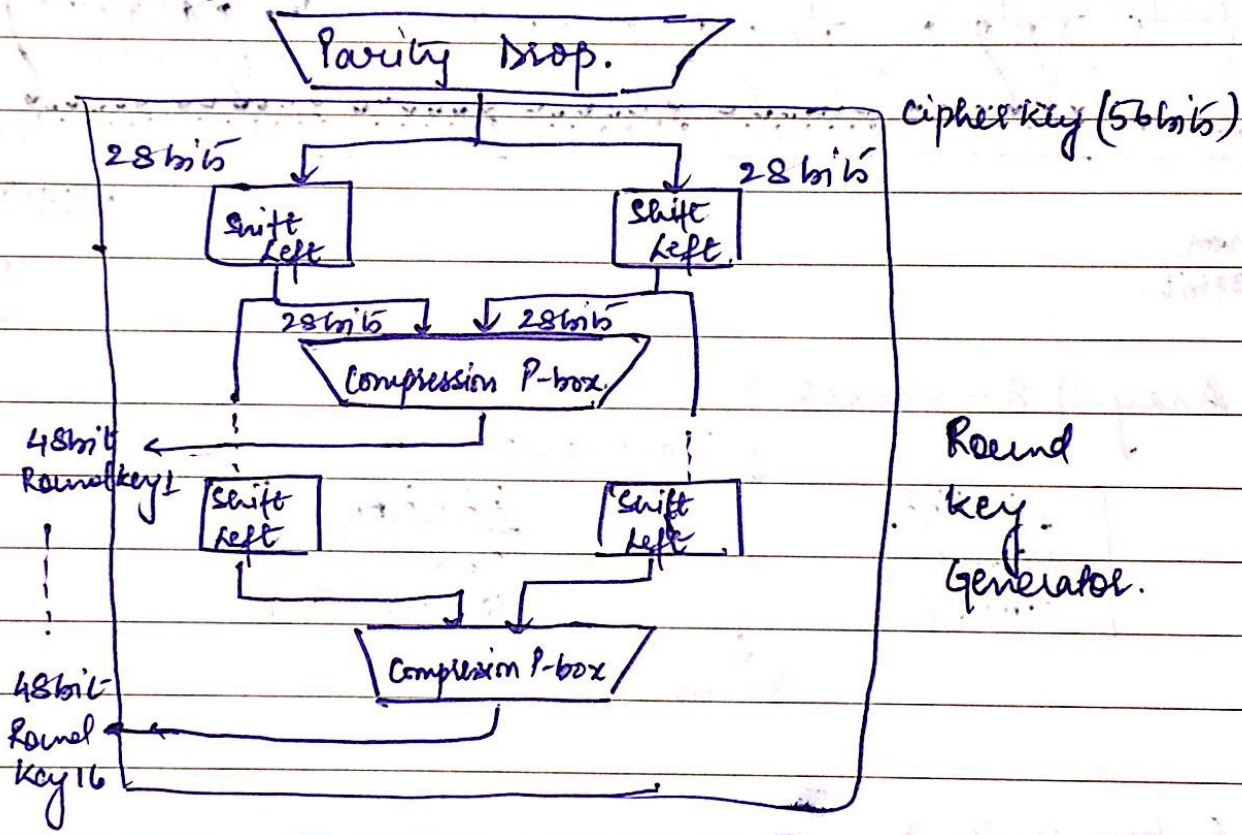
S-box rule ⇒



MATRIKAS

Date: 6 / 9 / 18 /

DES Key Generation. ⇒



Shift left is done by either 1 or 2 bits on each round

Rounds	Shift Left
1, 2, 9, 16	1
Others	2.

MATRIKAS

Date: / / /

Example key generation.

Let k is key K = 13345779 9BBCDFF1.

0001 0011 0011 0100 0101 0111 0111 1001 1001
1011 1011 1100 1101 1111 1111 0001

24/9/18

Types of Encryption. → Symmetric
Asymmetric.

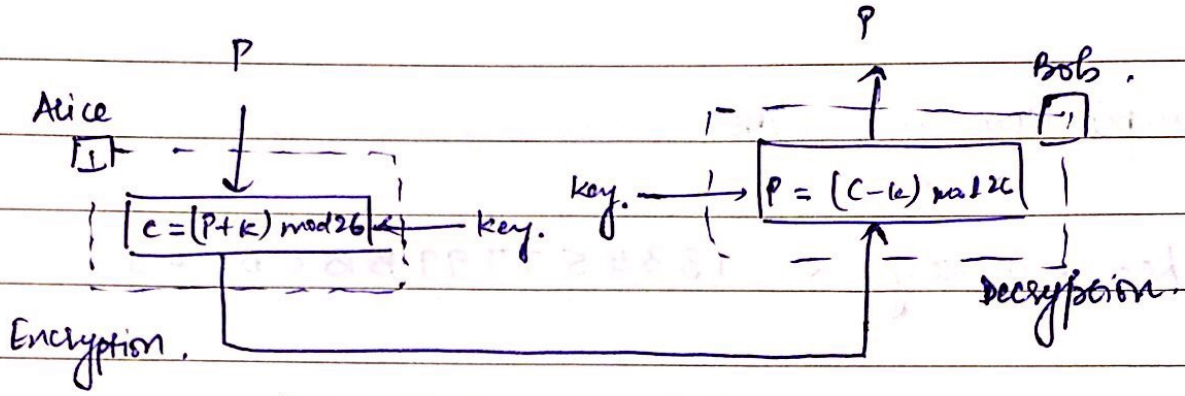
Categories of Traditional Symmetric key algorithms
→ Substitutional ciphers → replaces one symbol with another. A→D F→I.
→ Transpositional ciphers.

Substitutional ciphers: → • Monoalphabetic ciphers
— Relationship b/w a symbol in plaintext to symbol in ciphertext is always to one to one.
hello → KHOOR
1.— Additive Cipher / Shift cipher / Ceaes ar Cipher.

plaintext	a	b	c	. . . .		z
ciphertext	A	B	C	. . . .		Z
value :	00	01	02	. . . .		25

MATRIKAS

Date: / / /



ex: key = 15 to encrypt hello.

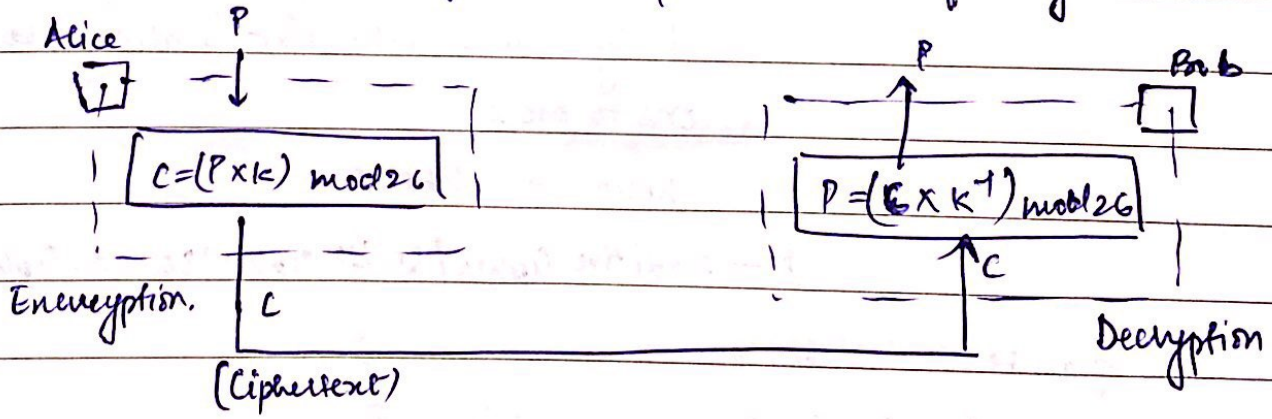
plaintext	h → 7	$(7+15) \bmod 26$	22	W
	e → 4	$(4+15) \bmod 26$	19	T
	l → 11	$(11+15) \bmod 26$	0	A
	l → 11	$(11+15) \bmod 26$	0	A
	o → 14	$(14+15) \bmod 26$	8	D

25/9/18

2. – Multiplicative ciphers.

encryption algorithm
- Multiplication of plaintext using key.

Decryption algorithm
- Use of multiplicative inverse of key.



$Z_{26}^{*} = 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25$

(Domain of keys)

MATRIKAS

Date: / / /

eg: hello key = 7.

h - 7	(7×7) mod 26 = 23	X
e - 4	(4×7) mod 26 = 2	E
l - 11	(11×7) mod 26 = 25	Z
l - 11	(11×7) mod 26 = 25	Z
o - 14	(14×7) mod 26 = 20	U

$(k \times k^{-1}) \bmod 26 = 1$

$k^{-1} = 15$

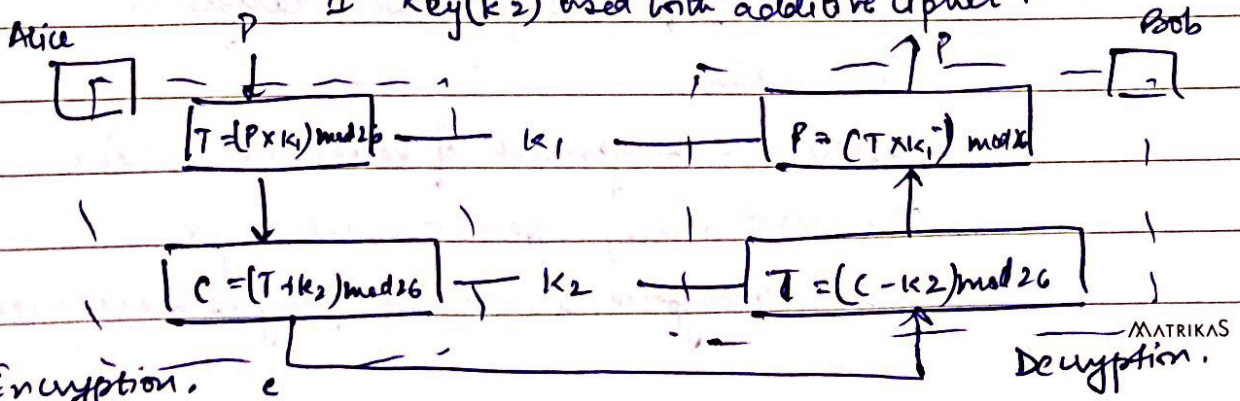
X - 23	(23×15) mod 26	7	h
E - 2	(2×15) mod 26	4	e
Z - 25	(25×15) mod 26	11	l
Z - 25	(25×15) mod 26	11	l
U - 20	(20×15) mod 26	14	o

3. Affine Ciphers –

Combination of both additive & multiplicative cipher.

Ist key (k_1) used with multiplicative ciphers.

IInd key(k_2) used with additive cipher.



Date: / / /

4. Monoalphabetic substitution cipher.

plaintext a b c d . . .

ciphertext N Q S U . . .

- Polyalphabetic Cipher.

1. → Autokey cipher.

key is stream of key $K = k_1, k_2, k_3 \ldots$

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

Encryption $C_i = (P_i + k_i) \bmod 26$

Decryption $P_i = (C_i - k_i) \bmod 26$

Initial key value $k = 12$

plaintext	a	t	t	a	c	k	i	s	t	o	d	a	y	
P's value	0	19	19	0	2	10	8	18	19	14	3	0	24	
keystream	12	0	19	19	0	2	10	8	18	19	14	3	0	
C's value	12	19	12	19	2	12	18	0	11	7	17	3	24	
Ciphertext	M	T	M	T	C	M	S	A	L	H	R	D	Y	

26/9/18

2. Play fair cipher.

- Used by British army during WW2.
- Secret key of 25 alphabets arranged in 5×5 matrix
- Different arrangement of letters in matrix can create many different secret keys.
- Before encryption, if need use of bogus characters.

MATRIKAS

Date: / / /

Rules:

① If 2 letters in a ~~particular~~ pair are located in same ~~next letter to right in same row~~ same row of secret key, corresponding character of each letter is next letter to right in same row.

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

③ If 2 letters in a pair not in same column or row, corresponding encrypted character is in its own row but but same column of other letter.

$P = P_1 P_2 P_3 \ldots \quad C = C_1 C_2 C_3 \ldots \quad K = [(k_1, k_2)(k_3, k_4) \ldots]$

Encryption: → $C_i = k_i$ & Decryption $P_i = k_i$

Eg: hello → bogus character.

Plaintext: he | el | lo

Rule 1 ← | Rule 2 ← | Rule 3 ←

Ciphertext: EC | QZ | BX

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

3. Vigenere Cipher.

- Use of key stream - Repition of initial secret key stream.

$P = P_1 P_2 P_3 \ldots \quad C = C_1 C_2 C_3 \ldots$

$K = [(k_1, k_2, k_3 \ldots), (k_1, k_2, k_3 \ldots)]$

Encryption $\Rightarrow C_i = P_i + k_i$ Decryption $P_i = C_i - k_i$

MATRIKAS

Date: / / /

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
c's value	7	7	22	10	18	22	23	18	11	6	13	19	2	6
Ciphertext	H	H	W	K	S	W	X	S	L	G	N	T	C	G.

One Time Pad.

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

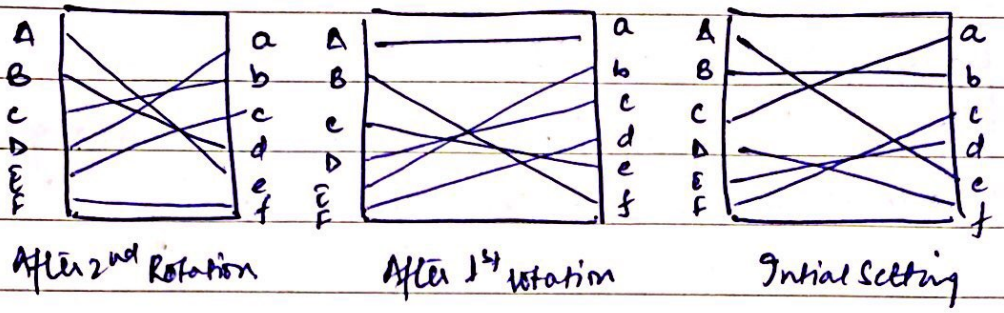
Ex: I[st] character encrypted using key 04 & second with 21.

Rotor Ciphers.

- Uses monoalphabetic idea but changes mapping b/w plaintext & ciphertext characters.

MATRIKAS

Date : / / /



Message

bee

Intial → After 1st → After 2nd.

Encrypted Message

(BAA) according to Intial setting

B C A

27/9/18

Namrata Note's Pictures

1/10/18 Manan Note's Pictures.

3/10/18 AES (Advanced Encryption Standards).

- Symmetric key block cipher
- NIST (National Institute of standards technology).
  - I^st Conference – 15 out 21 algorithms selected.
  - II^nd Conference → 5 out of 15 " "
  - Rijndael selected as AES (October 2000)
- Block size – 128 bits
- key sizes – 128, 192 & 256 bits.

MATRIKAS

Date: / / /

Criteria
- Security – 128 bits
- Cost – h/w, s/w implementation cost, technology.
- Implementation – flexibility, simplicity.

15/10/11

* Signing digest

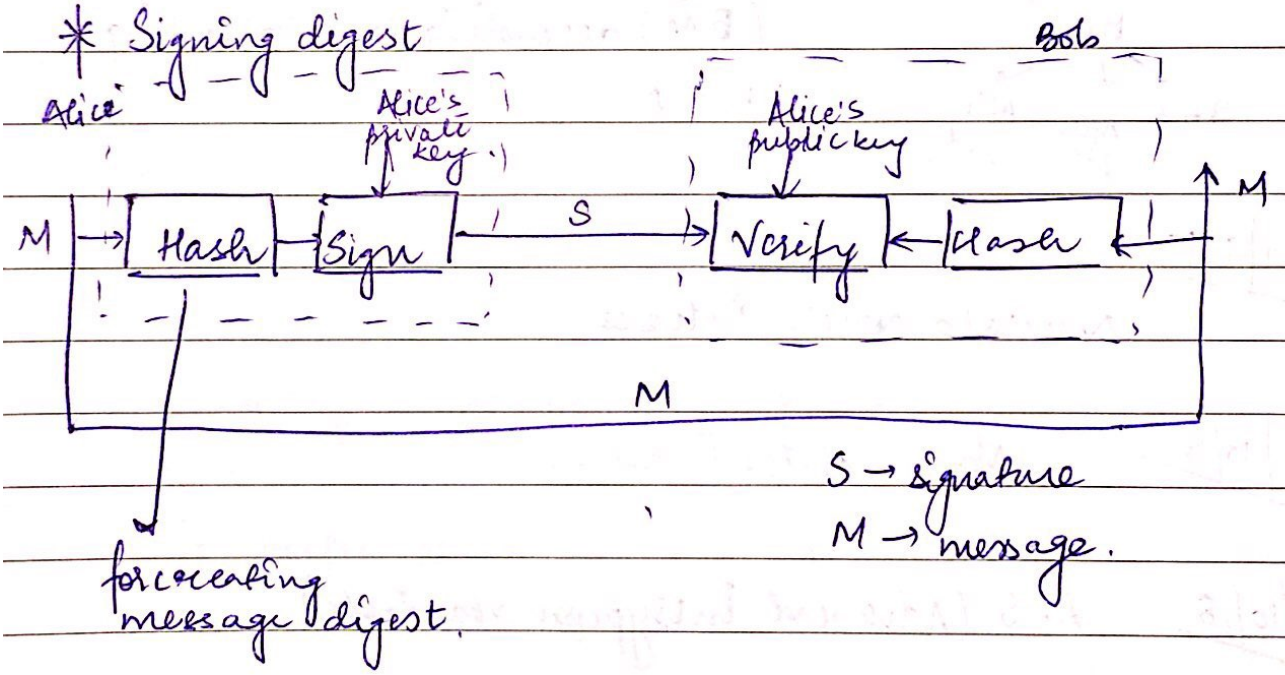


Fig 13.4, ~~39~~ Pg 394.

① RSA digital Signature Scheme.

Fig 13.7, Pg 397

Date: / / /

② Digital Signature Standard (DSS)

Fig 13.13, Pg 405.

Fig 13.4 Pg 406 → See functions inside box

16/10/18

E-MAIL

- To → Reciever of mail.
- Cc, Bcc → Any other reciever
- Subject → Describe in brief the topic
- Body. → ~~Describe the~~ Main body of the mail.
- Attachments → Any files that need to be sent along to the receiver.

→ Components.

E-mail

E-mail Message Components

- Header, Greeting, Text, Signature etc.

E-mail system

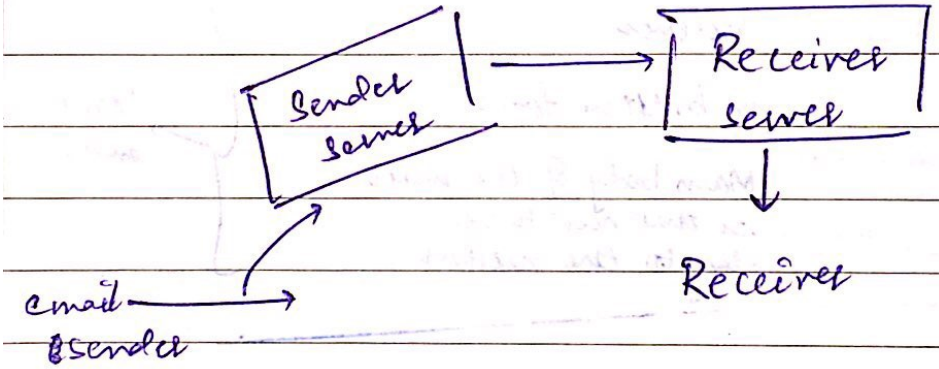
- Mailer, Mail Service, Mailbox.

MATRIKAS

Date: 17/10/18

* SMTP (Simple Mail transfer Protocol).

- It is application level protocol.
- It is connection-oriented protocol.
- It is text-based protocol.
- It handles exchange of ~~~~ messages b/w email server over TCP/IP n/w.
- It also provides notification regarding incoming mail.



SMTP Response →

Sent from sender to client.

1. Positive completion reply.
2. Positive intermediate reply. [some action pending].
3. Transient Negative completion response. [Some problem in connection established].
4. Permanent Negative completion reply. [connection can't be established].

MATRIKAS

Date: / / /

SMTP Commands

1. Hello
2. E Hello
3. MAIL FROM.
4. RCPT TO
5. SIZE
6. DATA
7. QUIT
8. ~~VERIFY~~. VERFY.
9. EXPN.

* PROXY SERVER.

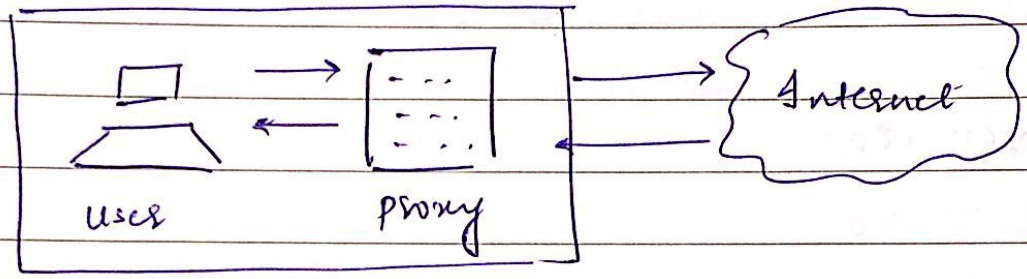
- Is an intermediary server b/w client & internet.
- Functionality
  - → Firewall & n/w data filtering
  - → N/w connection sharing
  - → Data caching
- Purposes
  - → Maintaining & filtering
  - → Improving performance
  - → Translation.
  - → Accessing services anonymously.
  - → Security.

MATRIKAS

Date: / / /

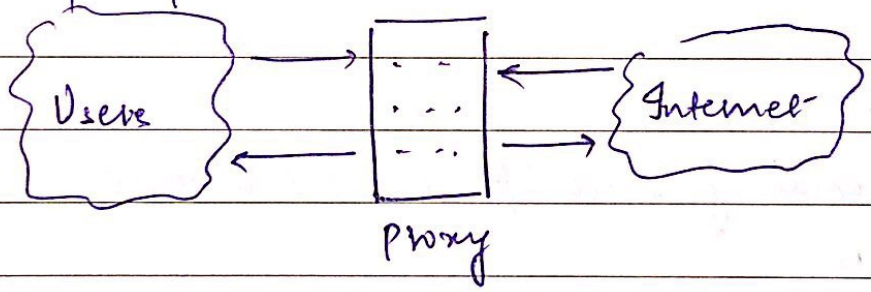
- Types

→ Forward Proxies.



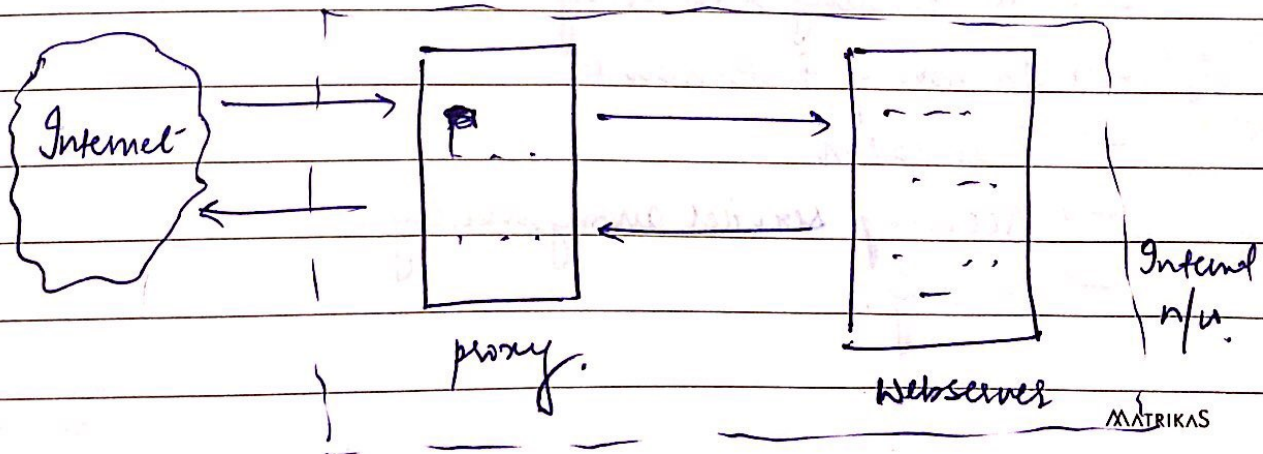
In this client requests internal n/w server to forward to internet.

→ Open proxies.



Open proxies helps clients to conceal their IP addresses while ~~browsing~~ browsing web addres.

→ Reverse proxies.

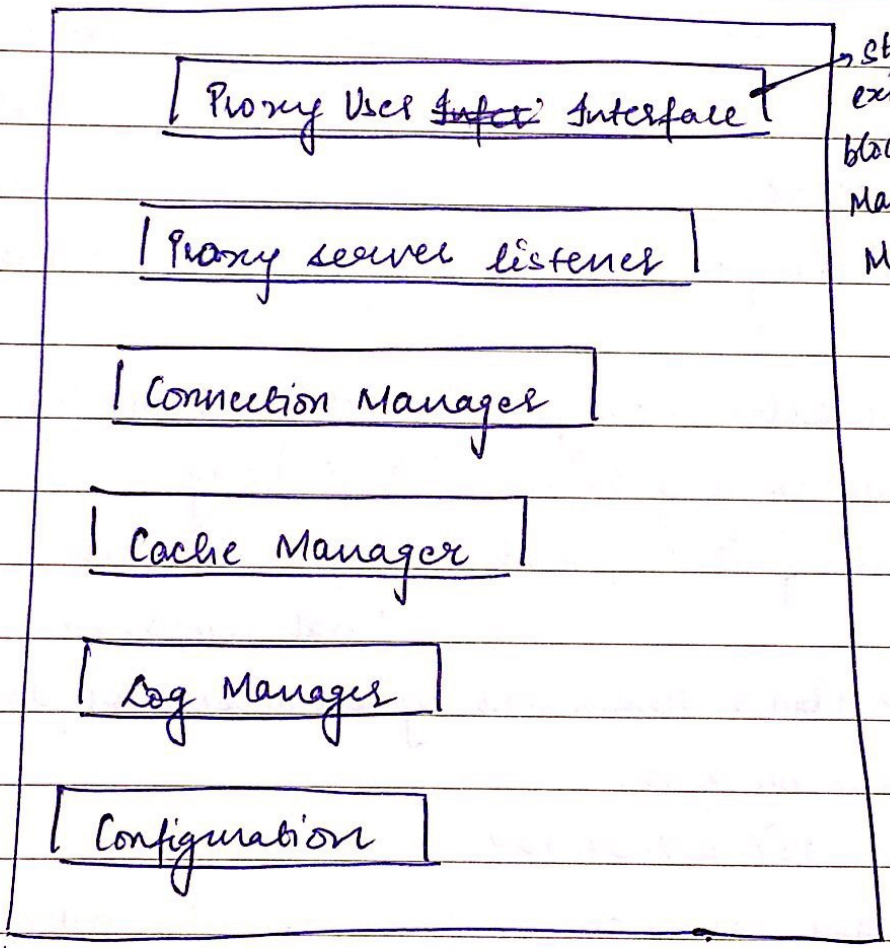


MATRIKAS

Date: / / /

requests are forwarded to ~~one~~ One or more proxy servers and response from proxy server is retrived.

- Proxy Architecture



MATRIKAS

Date: 18/10/18

* DNS (Domain Name System)

- When DNS not exists, one had to download a Host file containing host ~~nam~~ names and their corresponding IP addresses.
- It is a hierarchical naming system & distributed database of IP addresses & ~~asso~~ associated names.

* IP Addresses

- Unique logical addresses assigned to a machine over n/w.
- Unique addresses assigned to each host on n/w.
- IP address is of 32-bits (4 bytes) long
- Consists of 2 components → n/w component
  → host component
- Each 4 bytes represented by a number for 0 to 255 seperated by dots.

  eg:- 137.107.27.124

→ domain names → www.tutorialpoints.com.
↳ URL.

MATRIKAS

Date: / / /

* URL

URL Types.

Absolute URL	Relative URL
- Complete address of a resource on the web.	- This is partial address of webpage
eg: http://www.tutorialpoints.com/internettechnology/index.html	- Server name & protocol are ommitted from URL.
where, http is the protocol tutorialpoints.com is server index.html is file name.	- eg:- To link an image on website • tutorialpoints.com/internet_technology/internet_different_models. • /internet_technologies/internet_OSI_model.jpg.
- Used to link webpages on different website.	- Used to link web pages within same website
- Difficult to manage.	- Easy to manage.
- Changes when server name & directory name changes.	- Remains same even if we change server name or directory name.
- Take time to access	- Comparatively faster to access.

Date: / / /

* ~~DOMAIN~~ Domain Name System Architecture

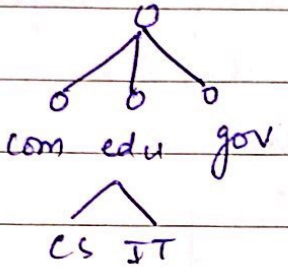
Domain Names → Symbolic string associated with an IP addresses

→ ex: com - commercial

edu - education

gov - government agency

net - networking organization



- Country type domain

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.

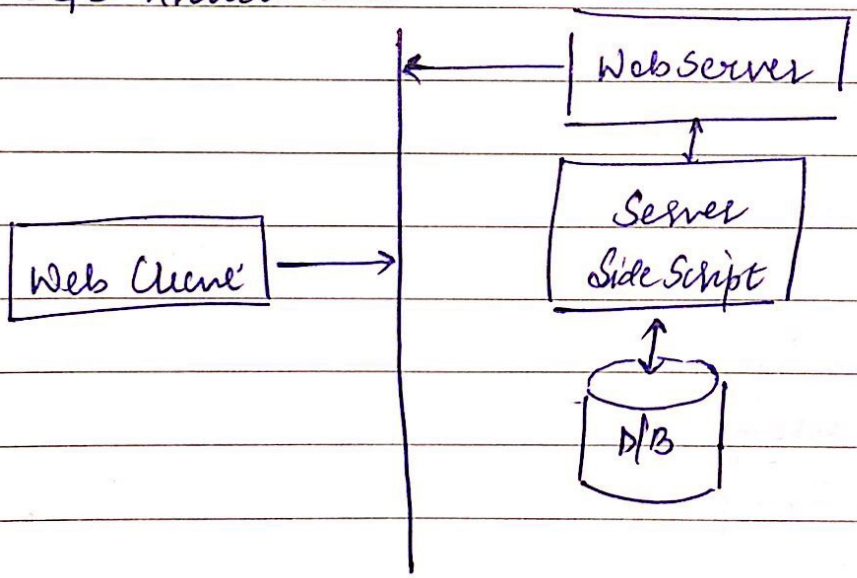
Date: 22/10/18

CGI Perl.

CGI → Common Gateway Interface

- → Set of standards that define how information is exchanged b/w web server & custom script
- → To interface with information server such as HTTP servers.
- → Current version CGI/1.1 & CGI/1.2.

CGI Architecture



Date: / / /

First CGI Program.

```
#!/usr/bin/perl
print "content-type: text/html \r\n\r\n";
print '<html>';
print '<head>';
print '<title> HelloWorld - first CGI program </title>';
print '</head>';
print <Hellow World! This is my first CGI program </h2>;
print `</body>`;
print `</html>`;
```

header & description:

contenttype : string
Expires : Date string
Location : URL string
Set cookies : string

MATRIKAS

Date: 23/10/18.

Cookies.

- A cookie is a piece of text that web server can store on user's hardisk
- piece of information → Name-Value pair
- C:\Windows\Cookies. — USERID & site name.
- timestamp, expiration, path.
- Session Cookies & Persistent Cookies

HTML & XML.

XML (Extensible Markup Language).

- Shows information in hierarchy

Chapter
Session
paragraph
sentence
word
characters.

Here Book is first level of hierarchy
root element.

MATRIKAS

Date: 29/10/18

* IP Security

IPSec → Secured n/w protocol suite that authenticate & encrypts packets of data sent over ~~Internet~~ internet protocol n/w

→ Mainly used in VPNs (Virtual private n/w s).

→ Established mutual authentication b/w agents at beginning of session & negotiation of cryptographic keys to use during session.

→ Can protect data flows b/w a pair of hosts (host to host) or b/w pair of security ~~or~~ gateways (n/w to n/w) or b/w security gateway & a host (n/w to host).

→ Uses security services.

IPV4 suite →

protocols →

→ Authentication Header (AH)

↳ Connectionless data integrity & data origin, authentication of ~~data~~ IP datagrams

→ Encapsulating Security protocols (ESP) . . .

→ Security Association (SA) . . .

MATRIKAS

Date : / / /

IPSec Modes →

- Transport Mode
- Tunnel Mode.

3-DES.

MATRIKAS