04 2015 MARCH
WEDNESDAY
WEEK 10 DAY 063-302

MARCH 2015

Wk	M	T	W	T	F	S	S
9	30	31					1
10	2	3	4	5	6	7	8
11	9	10	11	12	13	14	15
12	16	17	18	19	20	21	22
13	23	24	25	26	27	28	29

Security

- Network security - protection of our network and allow only authorised people to access the network.

Security layers
- Physical security — Security to physical objects
- Private Security — Security to individual or group
- Project security — Security to details of any project such as design, code

Information security includes security of data or information in different forms. Also covers the security of all infrastructure related to computer system and internet.

Notes * Denial of service attack - The attackers make the system busy so that the authorised users are unable to get the service. At the same time, they may access the information.

APRIL

Wk	M	T	W	T	F	S	S
14	6	7	8	9	10	11	12
15	13	14	15	16	17	18	19
16	20	21	22	23	24	25	26
17	27	28	29	30			
18							

MARCH 2015
THURSDAY
WEEK 10 DAY 064-301
05

Elements of information Security

Confidentiality - Most important service. Makes sure that only authorised user can access the data.
Confidentiality can be defined as protection of data from unauthorised disclosure

Integrity - checks validity of data. Integrity gives information whether there is any change in the data or not. It means assurance that data received are exactly as sent by an authorised sender.

Availability - Measure to which a system or information is accessible and usable upon request by an authorised user at any particular time. It means functioning condition of a system at any particular instance.

Security Policy

Information security or computer security is concerned with control of threats related to use of information or computer. We can permit only authorised users of any particular system to use that system. At the same time restrict these users to misuse their rights. This is called access control.

06 2015 MARCH
FRIDAY
WEEK 10 DAY 065-300

MARCH 2015

Wk	M	T	W	T	F	S	S
9	30	31					1
10	2	3	4	5	6	7	8
11	9	10	11	12	13	14	15
12	16	17	18	19	20	21	22
13	23	24	25	26	27	28	29

Security Techniques (Mechanism)

Strong security provided by using cryptography and authentication techniques.

Crypto - This prevents modification of data in transit.

Authentication technique - Used to guarantee communication endpoints.

Some of the secure techniques are -

Series of confidence - ensures that all software use has been authentic.

Access control - The access to the data or computer is controlled.

Ability to detect - when an application provides unpatched known flaws no way to scrap already known security issues, in such condition do not use it.

Backup of data - Secure our data by taking regular backup.

Antivirus software - Security from malicious software

Notes

Firewalls - Used to protect internal network from external attacks. If any attack found then it blocks the attack.

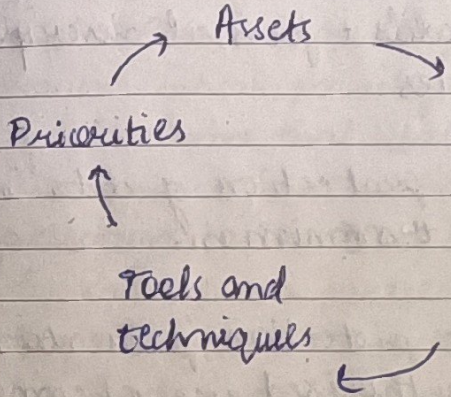
07 SATURDAY
WEEK 10 DAY 066-299

Encryption - Cryptographic technique. Allows only authorised user to read the data. Can be of symmetric or asymmetric type.

Intrusion-detection systems (IDS) - helps to detect internal as well as external attacks there are two types - misuse based and anomaly based IDS. Also classified as host-based and network based. IDS just detects the attack and sends alarm. Cannot protect the system from attack directly.

Information security awareness - educates people about use of computer and internet. and precautions to be taken while using internet.

Steps for Better Security



SUNDAY 08

Notes

MONDAY
WEEK 11 DAY 068-297

Assets - Identify what data and computer is to be protected.

Risks - Identify the threat, attacks, vulnerabilities and and risks

Protections - Solution for protection of information

Tools and techniques - Select appropriate tools

Priorities - decide order of tools and techniques.

Category of Computer Security

Cryptography - Secret writing used to hide original message. Original message called 'plaintext'. This is converted to some meaningless 'ciphertext'.

Data security - protective measures which ensure that data or computer is kept safe from modification or corruption.

Computer security models - formal description of security policies.

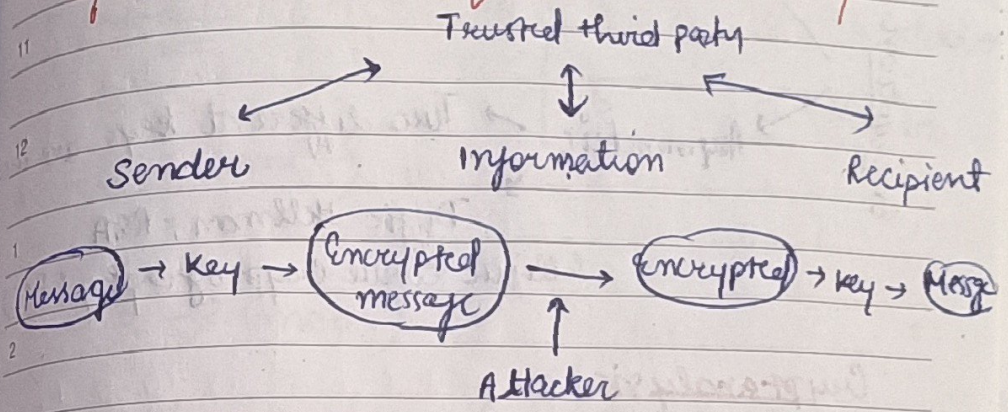
Network security - protection of data in network during transmission.

Notes

Computer security - protection, prevention and detection of unauthorised use of computer systems as well as data.

Security exploit - related to computer security vulnerabilities and their exploits.

Operational model of Network Security



Security Services

Authentication - Process of verifying that someone is who he claims he is.

Data confidentiality - Process of protection of data or information from unauthorised disclosure.

Access control - ensures privileged access is withdrawn when privileges are revoked

Integrity - Assurance that data received is exactly as sent by an authorised sender.

Non-repudiation - Assurance against denial by one of the parties.

Availability - measure to which system is accessible and usable on request by an authorised user

Notes

11 2015 MARCH
WEDNESDAY
WEEK 11 DAY 070-295

Wk	M	T	W	T	F	S	S
9	30	31					1
10	2	3	4	5	6	7	8
11	9	10	11	12	13	14	15
12	16	17	18	19	20	21	22
13	23	24	25	26	27	28	29

Encryption

Encryption
- Symmetric → Only one key. Same key is used for encryption and decryption
  - eg DES, AES, IDEA
- Asymmetric → Two different keys are used
  - Diffie-Hellman, RSA, Elliptic curve cryptography (ECC)

Cryptanalysis

Chosen plaintext - key not known to attacker

known plaintext - knows about plaintext, tries to decrypt ciphertext.

Ciphertext only attack - knows only ciphertext, tries to find original message

Man in the middle - Related to key transmission

THREAT - A potential for violation of security, which exists when there is circumstance, capability, action, event that could breach security and cause harm. That is a threat is a possible danger that exploit a vulnerability.

Notes

Threat

Act that seeks to steal or damage data or decompose the system.

Modular → $a \equiv b \pmod m$

m	a	$a = km + b$
	b	

$-8 \equiv 7 \pmod 5$

$-8 = 5 + 7$

$-3 \equiv -8 \pmod 5$

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

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

$[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

Commutative → { add, multipl
Associative

Notes

13 2015 MARCH
FRIDAY
WEEK 11 DAY 072-293

MARCH 2015

Wk	M	T	W	T	F	S	S
9	30	31					1
10	2	3	4	5	6	7	8
11	9	10	11	12	13	14	15
12	16	17	18	19	20	21	22
13	23	24	25	26	27	28	29

OSI Security Architecture

Security Attack → Passive / active

Security Mechanism →

Security service.

DES

- block cipher
- symmetric
- 64 bit plaintext block
- 16 rounds - fiestel round.

Steps - i) initial permutation (ii) 16 fiestel rounds
(iii) swapping / left right swipe
(iv) final permutation / inverse initial permutation

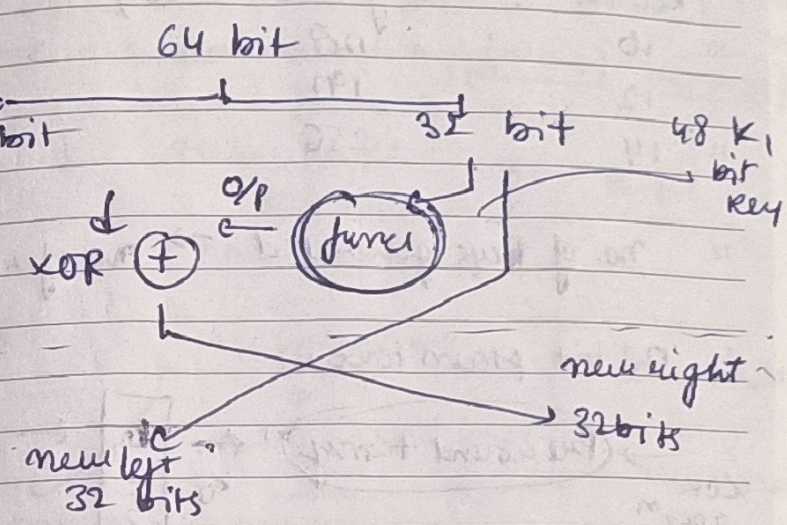
Basic structure

64 bit plain text
↓
initial permutation
↓
Round - 1 ← 48 bit key (initially 64.)
!
Round 16 ← 56 bit key
↓
inverse initial permutation
↓
64 bit cipher.

Notes

SATURDAY
WEEK 11 DAY 073-292
14

Fiestel round



Function.

32 bit data
↓
expension box
↓ 48 bit
48 bit key K1 → ⊕ XOR
↓ 48 bit
substitution
8 S-box ← S box
↓ 32 bit
Permutation box
↓
32 bit O/p

SUNDAY 15

Notes

Unit 6.

Malicious software (malware or malicious code) a software purposely designed to damage the computer system or data stored in that system.
Various types are -
1) Viruses 2) Worms 3) Trojans 4) Spyware
5) Ransomware 6) Bot.

Viruses

- Intends to damage the computer system.
- damages software residing in comp or any storage.
- damage may be deletion, corruption or modification
- Replicate themselves, spread rapidly.

Types of viruses

1) PARASITIC: propogated by attaching itself to particular program or file. known as executable files at start or ending of a file.
prepending → appending
- .com and .exe easiest to inject
- example - Jerusalem - slows down the system and deletes the file that user tries to execute.

2) BOOT SECTOR: Spreads when injected floppy disc or pen drive are used to boot the comp.
Example - Polyboot.B, Disk killer, Stone virus.

3) Polymorphic virus: change itself with each infection and creates multiple copies.
Example - Involuntary, Stimulate, Phoenix, Emil.

4. MEMORY RESIDENT: Installs code in the computer memory. Activated when OS runs and damages all the files opened at that time.
Example - Randex, CMJ, Meve.

5. STEALTH VIRUS: hides it's path after infects the comp. system. After injec^n modifies itself. Masks the size of injected file.
Examples - Frodo, Joshi, Whale.

6. MACRO VIRUS: infects files that are created using some applications, which contain macros. Activates when .docx or .xls files are opened by user and inject normal templates.
Examples - DMV, Melissa.A, Relax

7. HYBRIDS: features of diff type of virus combined
example - Happy 99 - email attack.

8. E-MAIL VIRUSES: Virus sent with the attachment
exam. - Melissa and Klez.

Antivirus software and Counter Measures

- Two approaches used - Signature or pattern based and behaviour based.

Signature - uses signature of virus
Behaviour - suspicious behaviour of comput program

Drawback -
Signature - New virus cannot be detected
Behaviour - creates of lot of false positives

Worms

- It can execute and spread itself whereas virus needs a host program.
- Use security loop holes within networks to reproduce itself.
- Self replicating does not make any change in files or documents.
- resides in active memory.
- affects the performance of computer by using it's resources and shuts down the computer.
- Expands quickly

Types

1) E MAIL WORM: infected email attachments.

2) INSTANT MESSAGING: spreads in instant messaging network using loop holes.

SUNDAY 22

3) INTERNET WORM: spread across internet.

4) INTERNET RELAY CHAT: spreads via IRC channels

5) FILE SHARING 6) PAYLOAD

7) WORM with GOOD INTENT - eg. Nachi worms

23 2015 MARCH MONDAY
WEEK 13 DAY 082-283

MARCH 2015

Wk	M	T	W	T	F	S	S
9	30	31					1
10	2	3	4	5	6	7	8
11	9	10	11	12	13	14	15
12	16	17	18	19	20	21	22
13	23	24	25	26	27	28	29

Spyware

- installed on computer without owner's knowledge
- gathers secret and private information
- used for advertising
- performance of computer affected
- can be done by installing additional software, redirecting web browser search, changing settings, reducing speed of internet.
- Can be used as type of adware - software delivers unsolicited pop up ads in addition to tracking the behaviours of the user.
- installed with some free software from internet.

Ransomware

- enters the computer and threatens the user.
- blocks user access to data stored on computer.
- asks money in term of bitcoin.
- can spread through injected software, malicious email attachments, compromised websites.

DoS Hack

- flooding the network with useless traffic.
- Makes memory resources too busy to serve legitimate network requests denying access to users.
- Back, neptune, ping of death, teardrop, land, pod, smurf.

use of limitations in TCP/IP protocols ↺ DOS attacks on this

Notes

APRIL 2015

Wk	M	T	W	T	F	S	S
14			1	2	3	4	5
15	6	7	8	9	10	11	12
16	13	14	15	16	17	18	19
17	20	21	22	23	24	25	26
18	27	28	29	30			

MARCH 2015 TUESDAY
WEEK 13 DAY 083-282

24

~~Hacking~~ DDOS →

A multitude of compromised systems attack a single system.

Intrusion Detection System

Security system that monitors the network traffic and analyses the data for possible attacks outside as well as inside the network.

Depending on architecture:

1. Network IDS – works on the network and performs an analysis of all traffic passing on entire subnet.
2. HOST IDS – It works on the host, monitors system events, audits event log. compares existing system files with previous snap shots. If any of these files found to modified or deleted, then alert sent.

On method of detection →

1) Misuse based V/s anomaly based.
2) Network based V/s host based
3) Passive V/s active system.

Notes

25 2015 MARCH
WEDNESDAY
WEEK 13 DAY 084-281

MARCH 2015

Wk	M	T	W	T	F	S	S
9	30	31					1
10	2	3	4	5	6	7	8
11	9	10	11	12	13	14	15
12	16	17	18	19	20	21	22
13	23	24	25	26	27	28	29

WEB SECURITY

Secure Socket Layer

- Certificate based general purpose protocol.
- developed by Netscape.
- Manage encryption of information transmitted over the internet.
- public key encryption

Transmission and routing of data on Internet controlled using TCP/IP

- SSL executes above TCP/IP and below higher level protocols like HTTP or IMAP.

On behalf of higher level protocol, SSL uses TCP/IP -

- SSL allows the server to authenticate the client by showing it's certificate.
- Client authenticated by user id and password
- Communicate securely.
- Issuing authority responsible for distribution of SSL key and certificate.
- Client and server exchange information regarding encryption using SSL handshake protocol.

SSL - also Transport layer security

Notes

THURSDAY
WEEK 13 DAY 085-280
26

SSL is a set of protocols:

RECORD protocol - Ensure security and integrity to the data. Defines the format used to transmit the data

CHANGECIPHER SPEC PROTOCOL : Sent by both server and client to inform other party that subsequent records will be protected under just negotiated Cipher Spec and keys

ALERT protocol : SSL related alerts to communication parties

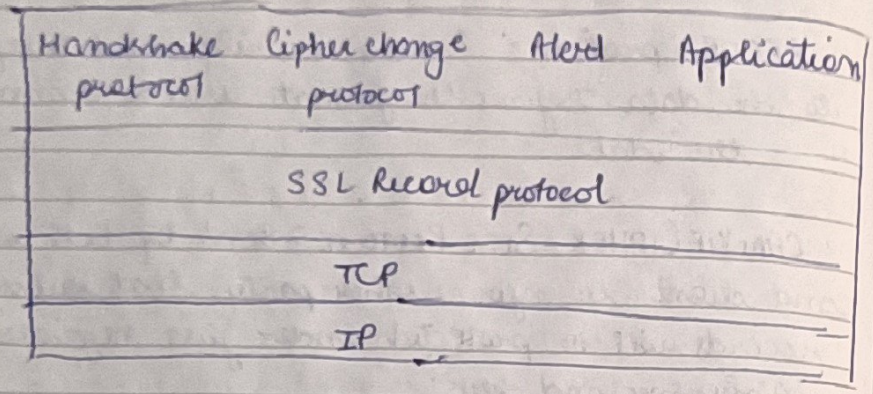
HANDSHAKE protocol : Responsible for establishing an SSL connection. To establish connec" for first time it uses record protocol

Objectives of SSL

1) AUTHENTICATION - Supports authentication of server and client to each other.
2) DATA INTEGRITY - data should be recieved as it is.
3) DATA PRIVACY - data should be protected from the attacker such that only authorised users can read it.

Notes

Protocol stack



SSL Record → format for the message
- encryption, integrity, encapsulate

Handshake → session management
Cipher change → Cryptographic parameter mang.
Alert → transferring of SSL messages.

SSL Session and Connection

1) Establishing connection between server and the client. Logical link between them. SSL connection should be between two network nodes and is peer to peer.

2) An association b/w server and client is called session. Includes session number, diff algorithms used, etc. Handshake protocol used to create SSL session, when session starts, sharing parameters.

Single session shared by multiple connections but single connection cannot have multiple sessions.

3) a) Session identifier - generated by server and used for identifying session with a client
b) Peer certificate - X.509 certificate
c) Compression - compress the data
d) Algorithm specification - encryption algorithm
e) Master secret - Client and server share secret data of length 384 bits.
f) "is resumable" - flag indicating whether session can be used to initiate new connections.

4) Connection state
a. Server and client random - both client and server generate random data
b. Server write MAC secret - indicates secret key used by server.
c. Client write MAC secret → secret key used by client
d. Server write key → indicates key used by server for encryption and by client for decryption.

e. Client write key → key used by client for encryption and server for decryption
f. Sequence number → Maintains sequence number separately for each message transmitted and received during data session.

30 2015 MARCH MONDAY
WEEK 14 DAY 089-276

MARCH 2015

Wk	M	T	W	T	F	S	S
9	30	31					1
10	2	3	4	5	6	7	8
11	9	10	11	12	13	14	15
12	16	17	18	19	20	21	22
13	23	24	25	26	27	28	29

SSL Record Protocol

- SSL Record layer protocol takes data from application layer and divides the data into different parts of fixed length.

detailed procedure -

1) Fragmentation - Divide the message into number of parts or fragments of fixed size. If part size is less than requisite size, then necessary number of padding bits are added at end of message

2) Compression

3) Append MAC - Calculate the MAC
MAC = Hash function
Append MAC value to each part of message.

4) Encryption - encrypt the complete part with MAC using symmetric key encryption algorithm.

5) Attach header - to the packet.

Notes

APRIL 2015

Wk	M	T	W	T	F	S	S
14			1	2	3	4	5
15	6	7	8	9	10	11	12
16	13	14	15	16	17	18	19
17	20	21	22	23	24	25	26
18	27	28	29	30			

MARCH 2015 TUESDAY 31
WEEK 14 DAY 090-275

Email security

Pretty Good Privacy (PGP)

- uses a combination of symmetric and asymmetric algorithm for encryption and decryption
- an encrypted digital signature sent to the receiver using PGP.
- most popular program used by individuals
- available as freeware and also at low cost commercial version.
- Used for authentication of the sender.

Need to use PGP

1) Financial data to send over the internet
2) data related to trade 3) Personal information
4) information related to some product.

Working

1. AUTHENTICATION - sender uses a digital signature -
   - create the message
   - Msg digest or hash value generated by sender
   - encrypted using sender's private key - digital signature - RSA algo used.
   - receiver decrypts using sender's public key
   - Msg digest generated by receiver
   - if matched, authentic.

Notes

or IDEA, 3DES

② CONFIDENTIALITY -

RSA algo
- creates msg and a 128 bits session key
- CAST 128 encryption algo and session key.
- session key encrypted by recievers public key
- decrypted by recievers private key
- using session key message decrypted.

③ Confidentiality and authentication - Combine both

④ COMPRESSION -

Reduce the size of message. done after generation of digital signature but before encryption.

⑤ E-MAIL COMPATIBILITY

eg if confidentiality needed ; message and digital signature both encrypted, Thus resulting block consists of stream of 8-bit octets. PGP provides service of converting raw 8 bits binary stream to ASCII using radix-64.

⑥ SEGMENTATION and REASSEMBLY

Notes Cannot send large messages through email. PGP automatically subdivides. It is done before sending an e-mail when all process completed.

Generic transmission

File
↓
is authentication required → Yes → generate digital sig.
↓ NO
Compression
↓
is confidentiality required → Yes → encryption
↓ No
convert using radix 64

Generic reception

convert from radix 64
↓
is confidentiality req. → Yes → Decryption
↓ No
Decompression
↓
is authentication required → Yes → generate DS and compare with DS recieved.
NO ↓

S/MIME

Uses symmetric encryption algorithms, public key cryptography, message digest algorithms, certificates for authentication and message integrity.

Symmetric algo - RC2 and Triple-DES.

RSA - key generation

SHA-1 or MD5 - message digest.

Secrecy:

(a) A random key called session generated.

Notes

Firewall.

Firewall prevents unauthorised access to and from the ~~system~~ network. Tool used to protect the network from attackers. Can be software, hardware or combination. First line of defence. Allows only authenticated packets to come and go.

Generally installed b/w network and internet also installed in an Intranet to protect one internal network such as one LAN from other LAN.

Functions -

1) Blocks unauthorised traffic
2) forwards incoming traffic to more reliable internal computer systems.
3) hides internal networks, vulnerable
4) hides information about internal network
5) provides strong user authentication
6) serve as a platform for IPsec.

• Service control, direction control, user control, behaviour control.

SUNDAY 05

→ all traffic denied except that which is specifically authorised.

Notes

→ all traffic allowed except which is specifically denied.

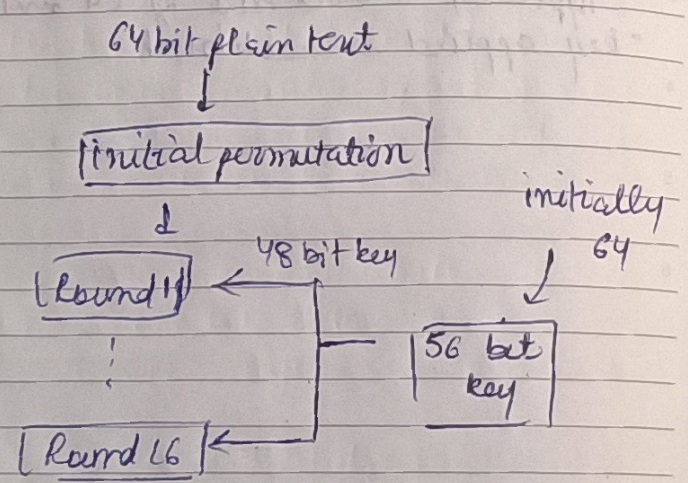
08 2015 APRIL WEDNESDAY WEEK 15 DAY 098-267

DES

i) block cipher • symmetric cipher
(same key for en and decrypt)
• 64 bit plain text.
• 16 rounds - fiestel round.

Steps:
1) initial permutation
2) 16 fiestel rounds
3) swapping / left right swap
4) final permutation / inverse initial

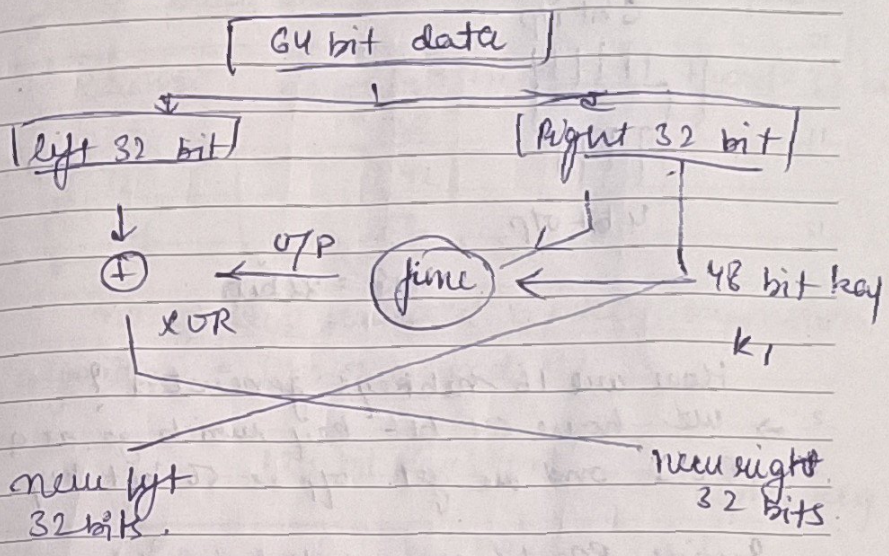
Basic structure:



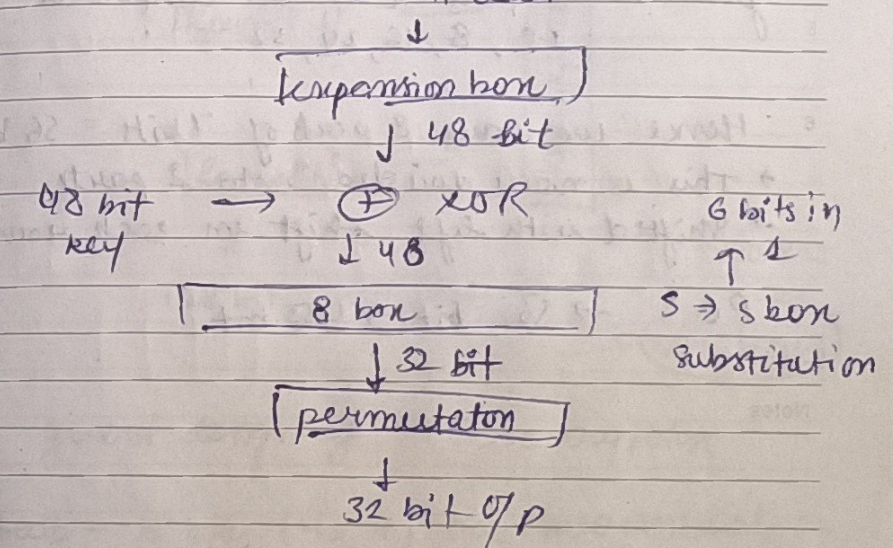
Notes

09 APRIL 2015 THURSDAY WEEK 15 DAY 099-266

Fiestel round -



function:



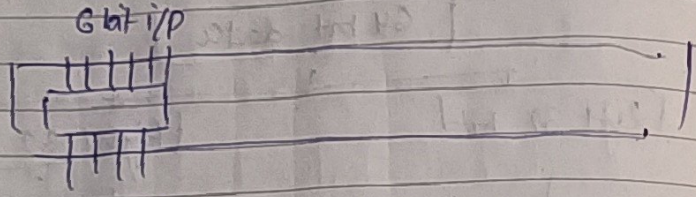
Notes

10 2015 APRIL FRIDAY WEEK 15 DAY 100-265

APRIL 2015

Wk	M	T	W	T	F	S	S
14			1	2	3	4	5
15	6	7	8	9	10	11	12
16	13	14	15	16	17	18	19
17	20	21	22	23	24	25	26
18	27	28	29	30			

S-boxes



4*8 = 32 bits

How are 16 subkeys generated?

→ we have 64 bit key which go as a i/p to PC 1 and we get o/p as 56 bit key

Inside PC-1 (permuted choice - 1)

- 64 bit key divided into 8 parts of 8 bit each
- from each part last bit discarded.

i.e, 8, 16, 24, 32 ---

Hence we have 8 parts of 7 bits = 56 bits.

→ This is now divided into 2 parts.

→ Shifted with left shift in each round.

PC 2 → 56 bit → 48 bit.

Notes

MAY 2015

Wk	M	T	W	T	F	S	S
18					1	2	3
19	4	5	6	7	8	9	10
20	11	12	13	14	15	16	17
21	18	19	20	21	22	23	24
22	25	26	27	28	29	30	31

APRIL 2015 SATURDAY WEEK 15 DAY 101-264 11

AES

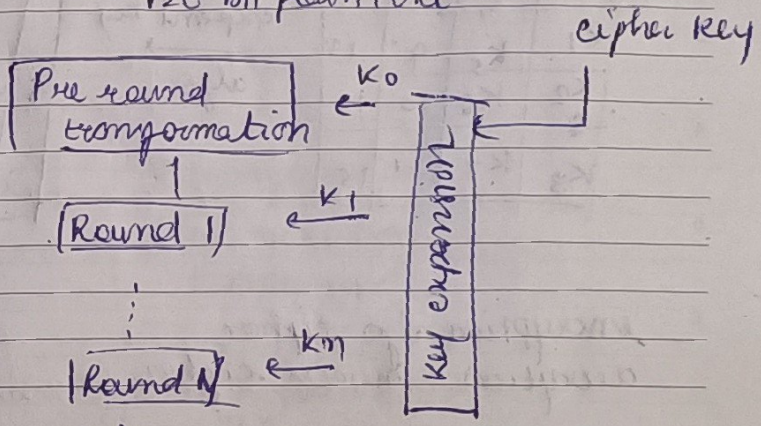
- symmetric key block cipher
- fixed block size 128 bits i.e 16 bytes

4 words

Rounds	no of bits in key
10	128
12	192
14	256

1 word = 32 bits

no. of keys generated by key expansion algorithm = (no. of rounds + 1)



128 bit cipher text

→ N+1 keys

SUNDAY 12

Notes

general design of AES encryption

State - 16 bytes (4 × 4) store intermediate result.

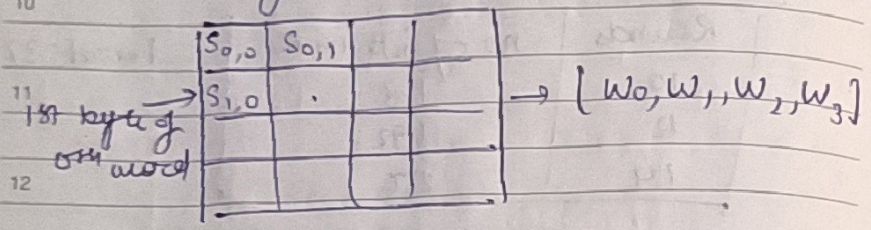
13 2015 APRIL
MONDAY
WEEK 16 DAY 103-262

APRIL 2015

Wk	M	T	W	T	F	S	S
14			1	2	3	4	5
15	6	7	8	9	10	11	12
16	13	14	15	16	17	18	19
17	20	21	22	23	24	25	26
18	27	28	29	30			

~~Plain text~~

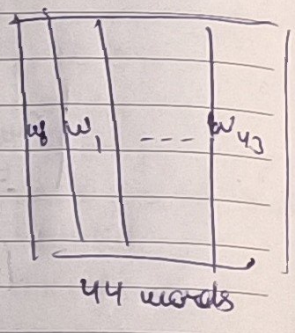
State array (4×4) = 16 byte



Key → 128 bit ie 4 words

W_0	W_1	W_2	W_3
K_0	K_4	K8	12
K_1	K_5	9	13
K_2	K_6	10	14
K_3	K_7	11	15

expand key algo →



44 words

encryption algo - cipher
decryption - inverse cipher

round keys applied in reverse order.
much stronger than DES.

Notes

APRIL 2015
TUESDAY
WEEK 16 DAY 104-261
14

128 bit key → expand key

Plain text (128 bit)

only XOR oper^n — Add round key (W_0-3)

↓ sub bytes

Substitute bytes

↓

Shift rows

↓

mix columns

↓

add round keys ← W_{4-7}

↓

R_{10} Transformation (No mix column transformation)

Structure of each round →

4×4

↓

Sub bytes

↓

4×4 State

↓

Shift rows

↓ State 4×4

mix column

↓ 4×4

add round key

Notes

15 2015 APRIL WEDNESDAY WEEK 16 DAY 105-260

APRIL 2015

Wk	M	T	W	T	F	S	S
14			1	2	3	4	5
15	6	7	8	9	10	11	12
16	13	14	15	16	17	18	19
17	20	21	22	23	24	25	26
18	27	28	29	30			

Transformations

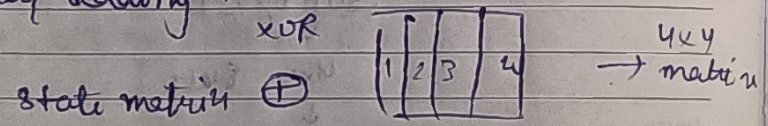
1) Subritution - substitution done for each byte using s-box...

Subbytes - we interpret the byte as 2 hexadecimal digit.
1st HX → Row 2nd → column
of substitution table.

2) Permutation - Right the bytes,
- Shifting done to the left
- depends on row of state matrix.

3) Mixing - Take each word (column i.e 4 bytes or 4×1 matrix. and multiply it with const matrix
O/p is stored in 4×1 matrix of 4 bytes and stored in state matrix.

4) Key adding.



Notes

16 APRIL 2015 THURSDAY WEEK 16 DAY 106-259

MAY 2015

Wk	M	T	W	T	F	S	S
18					1	2	3
19	4	5	6	7	8	9	10
20	11	12	13	14	15	16	17
21	18	19	20	21	22	23	24
22	25	26	27	28	29	30	31

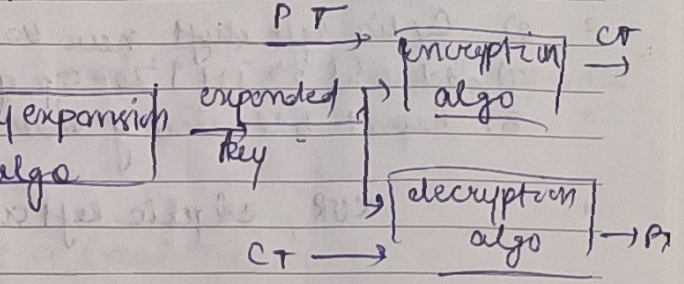
RC5

- Block cipher, symmetric text
- address 2 word blocks at a time

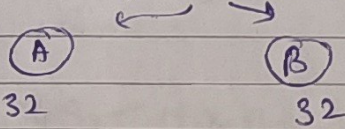
3 parameters

w = word size (16, 32, 64 bits) } based on plain text
r = no. of rounds (0-255)
b = key size in bits (0-255)

3 components - key expansion, encryption, decryption.



Key expansion
complete set of operations to produce k subkeys



subkeys generated S[0] and S[1].
2 subkeys are added to A and B
↓
C and D

Notes

Rounds
- Bitwise XOR
- left circular shift
- addn to next subkey for both C and D.

17 2015 APRIL
FRIDAY
WEEK 16 DAY 107-258

APRIL 2015

Wk	M	T	W	T	F	S	S
14			1	2	3	4	5
15	6	7	8	9	10	11	12
16	13	14	15	16	17	18	19
17	20	21	22	23	24	25	26
18	27	28	29	30			

Encryption:

1) One time initialisation S[0] ← A
S[1] ← B

2) XOR A and B

3) Cyclic left shift of A by B bits.

4) add S[2*i] to op of previous step = A
↓
round

5) XOR B with new value of A ⇒ B

6) Cyclic left shift new val B by A bits

7) add S[2*i+1] to op of previous step ⇒ B

8) repeat till end of rounds.

XOR, cyclic left shift, add of subkeys

Notes

MAY 2015

Wk	M	T	W	T	F	S	S
18					1	2	3
19	4	5	6	7	8	9	10
20	11	12	13	14	15	16	17
21	18	19	20	21	22	23	24
22	25	26	27	28	29	30	31

APRIL 2015
SATURDAY
WEEK 16 DAY 108-257
18

Chinese Remainder Theorem

There always exist an "x" (integer) that satisfies the given congruence

$x \equiv rem[0] \pmod{num[0]}$
$x \equiv rem[1] \pmod{num[1]}$

and num[0], num[1] ... must be relatively prime.

eg.
$x \equiv 1 \bmod 5$ → 5 and 7 coprime
$x \equiv 3 \bmod 7$

Explanation.

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

(i) m_1, m_2, m_3 should be relatively prime.

SUNDAY 19

(ii) $x = (M_1 X_1 a_1 + M_2 X_2 a_2 \cdots M_n X_n a_n) \bmod M$

$M = m_1 \times m_2 * m_3 \cdots m_n$

$M_i = \frac{M}{m_i}$

Notes

To calculate X_i → multiplicative inverse of M_i

$M_i X_i \equiv 1 \bmod m_i$

eg $M_1 X_1 = 1 \bmod m_1$

Diffie-Hellman Key exchange algo

- not an encryption algo.
- exchange secret keys between 2 users
- asymmetric encryption used to exchange the secret key. → public and private key

Algorithm

(i) consider prime number 'q'
(ii) select α such that it must be primitive root of q $(\alpha < q)$.

$a \bmod q$
$a^2 \bmod q$
$a^{q-1} \bmod q$ ← Primitive root

gives $\{1, 2, 3, 4 \ldots q-1\}$

Notes

let $q = 7$, $\alpha = 5$

α and q → global public elements.

X → private Y → public.

(3) assume X_A (private key and $X_A < q$ of A)

calculate $Y_A = \alpha^{X_A} \bmod q$
(Y_A: public key.)

let $X_A = 3$, $Y_A = 5^3 \bmod 7$
$Y_A = 6$.

(4) assume X_B (private key) $X_B < q$
$Y_B = \alpha^{X_B} \bmod q$
$= 5^4 \bmod 7 = 2$

(5) calculate secret keys.

$K_1 = (Y_B)^{X_A} \bmod q$ $K_2 = Y_A^{X_B} \bmod q$
(Y_B, Y_A: public keys.)

$K_1 = K_2$

$K_1 = 2^3 \bmod 7 = 1$ $K_2 = 6^4 \bmod 7 = 1$

22 2015 APRIL WEDNESDAY WEEK 17 DAY 112-253

Rivest Shair Adleman

RSA algorithm

- asymmetric cryptographic algo.
- if public key of user A used for encryption, we have to use private key of same for decryption
- RSA scheme is a block cipher in which plain text and ciphr text are integers btw 0 and n-1 for some values n.

Algorithm.

1 Key generation

(i) Select two large prime no - p and q.

(ii) Calculate $p * q = n$

(iii) Calculate $\phi(n) = (p-1) * (q-1)$ // euler's totient func^n.

(iv) choose value of e

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

(v) Calculate

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

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

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

(vi) public key = $\{e, n\}$ → encryption

(vii) private key = $\{d, n\}$ → decryption

Notes

23 APRIL 2015 THURSDAY WEEK 17 DAY 113-252

c → ciphertext

2) Encryption

Plaintext = $M < n$

$C = M^e \bmod n$

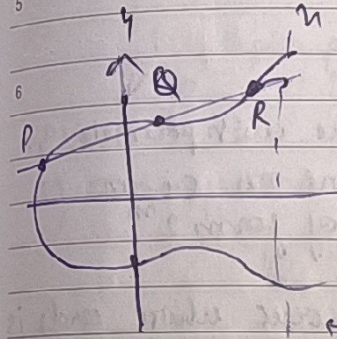
3) Decryption

$M = C^d \bmod n$

Elliptic Curve Cryptography

- asymmetric / public key cryptosystem.
- provides equal security with smaller key size.
- makes use of elliptic curves.
- elliptic functions defined by some mathematical functions eg cubic.

$y^2 = x^3 + ax + b$



- symmetric about x-axis
- if we draw a line, intersect max 3 points.

← limiting it

Notes

Trapdoor function - easy to compute in one dir^n but difficult in opp dir^n (finding its inverse) without special info called trapdoor

Algorithm.

- Let $E_q(a,b)$ be the elliptic curve.
  Consider the equation $Q = kP$

where Q, P = points on curve $k < n$

it is easy to find Q given k and P but difficult to find k from P and Q. this is called discrete logarithmic problem for elliptic curves
→ trapdoor function.

ECC Algo.

1 Key exchange

global public elements.

$E_q(a,b)$ - elliptic curve with parameters a, b and q → prime no. or an integer of form 2^m.

G : point on the curve whose order is large value of n.

Notes

2) User A key generation
select private key n_A $\quad n_A < n$
public key => $P_A = n \times G$

similarly for B, $P_B = n_B \times G$ $\quad n_B < n$

calculation of secret key by A

$K = n_A \times P_B$

Calculation of secret key by B

$K = n_B \times P_A$

3) encryption.
- set message be M
- encode this into a point on elliptic curve
  P_m
  → encrypted

choose random the integer K.

cipher point →
$C_m = \{kG, P_m + kP_B\}$

4) Decryption.

$key * n_B$

$P_m + kP_B - (kG * n_B)$

$P_B = n_B G$

=> P_m → original point.

27 2015 APRIL
MONDAY
WEEK 18 DAY 117-248

APRIL 2015

Wk	M	T	W	T	F	S	S
14			1	2	3	4	5
15	6	7	8	9	10	11	12
16	13	14	15	16	17	18	19
17	20	21	22	23	24	25	26
18	27	28	29	30			

Authentication

(i) Message encryption (cipher text)

(ii) MAC (message authentication code).
we have some authentication function and we apply them on plaintext along with key which produces a fixed length code called MAC.

$C(M, K)$ = fixed length code

(iii) Hash functions

$H(M)$ = fixed length code (Hash code) 'h'
(M: msg)

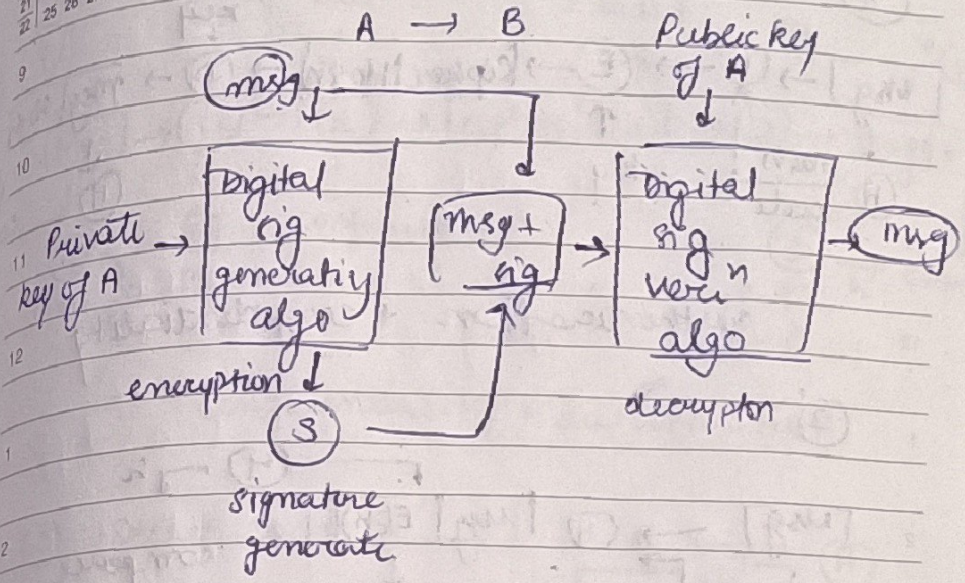
independent of key → message digest.

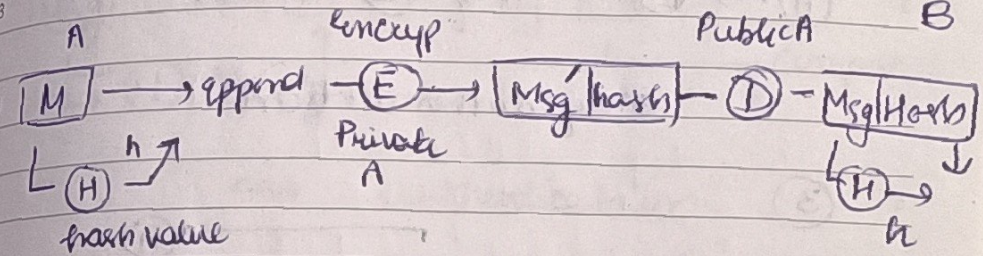
Digital signature

- e commerce, online transaction etc.
- asymmetric key cryptography.
- used for msg authentication and non repudiation and msg integrity.
- not used for confidentiality.

Notes

28 TUESDAY
WEEK 18 DAY 118-247





Hash functions / Compression fun^n

- similar to MAC, doesn't use a key
- Takes in variable size msg and produce fixed output.
  ↓
  called hash code / value / or message digest.
- only I/P is msg

$H(M)$ → fixed length of code 'h'

Notes

29

2015 APRIL

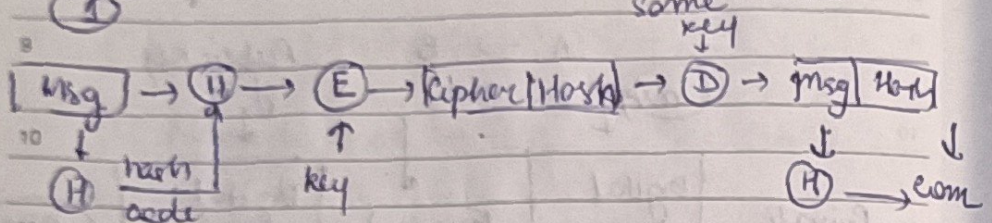
WEDNESDAY

WEEK 18 DAY 119-246

APRIL 2015

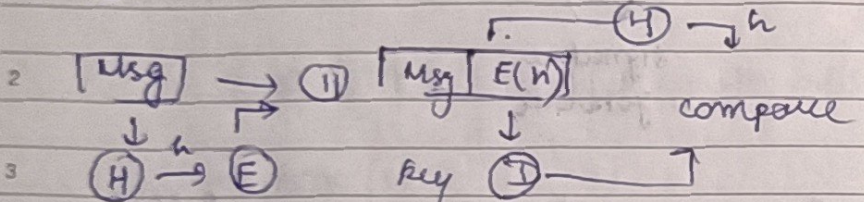
Wk	M	T	W	T	F	S	S
14			1	2	3	4	5
15	6	7	8	9	10	11	12
16	13	14	15	16	17	18	19
17	20	21	22	23	24	25	26
18	27	28	29	30			

(1)



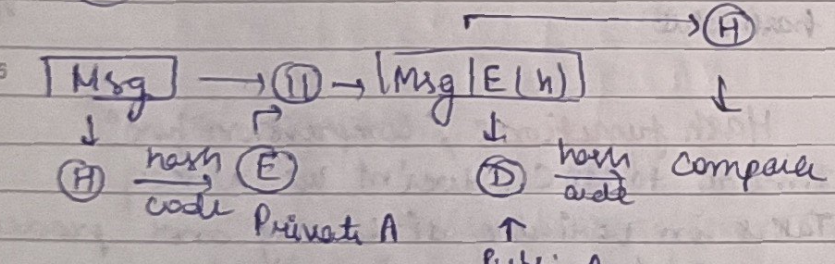
authentication + confidentiality.

(2).



- only authentication.

(3)



only authentication.

Notes

30

APRIL 2015

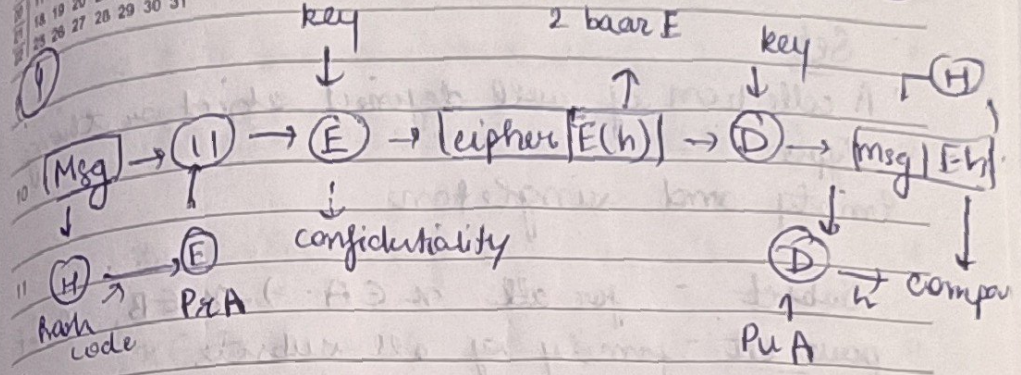
THURSDAY

WEEK 18 DAY 120-245

MAY

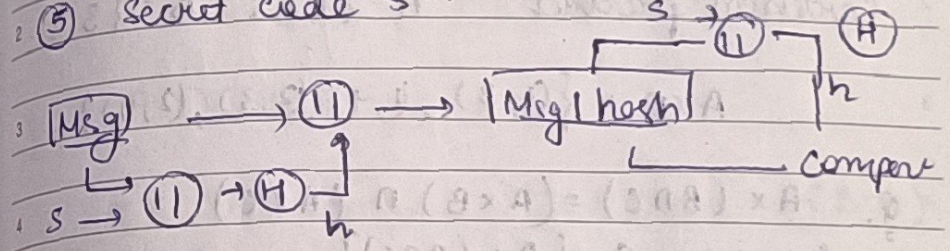
Wk	M	T	W	T	F	S	S
18					1	2	3
19	4	5	6	7	8	9	10
20	11	12	13	14	15	16	17
21	18	19	20	21	22	23	24
22	25	26	27	28	29	30	31

(4)



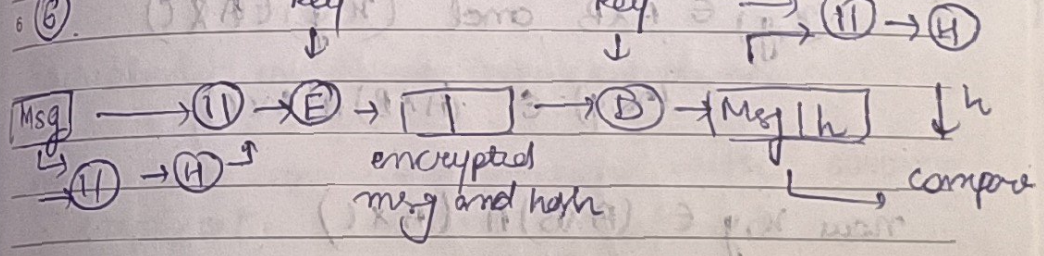
confidentiality + authentication.

(5) Secret code 's'.



~~No~~ authentication.

(6).



confidentiality + authentication.

Notes