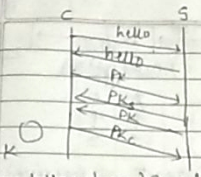
7/19



https handshake process (Protocol)

Based on the data exchanged in this protocol, a key is calculated. This key is used to encrypt all the data that is exchanged.

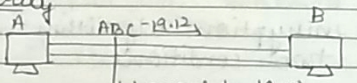
E_K [data]

This key is calculated each time the page is loaded (FS is pr

Authentication - Credentials are correct
Authorization - Resource can be accessed b not by a particular clien

Single sign on - Use multiple services b Signing in just once
Ex- Use all google servic only by signing in on

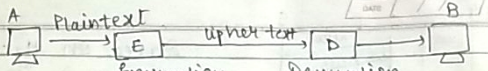
Security



Traffic monitoring attack

Types: i) Passive attack - Data is only monitored, it is not modified

ii) Active attack - Data is modified al



Encryption. Decryption

A C ... A C ...
↓ ↓ ↑ ↑
1 3 1 3

In the end, Sent plaintext = received plaintext

Ceaser cipher (first encryption).

A $\xrightarrow{+3}$ D X → C
B → E
C → F (c+3) % 26

Confidentiality - when data is sent from one end to another, the data should remain intact without anyone tampering it

Authentication - The data received should be must have been sent by the intended sender, i.e the received data is genuine

Any encryption algorithm must fulfill these two conditions.

Play fair cipher (Substitution cipher)
When same key is used to encrypt and decrypt, it is called symmetric key.
Play fair cipher is a symmetric key algorithm.

Ex: Key = MONARCHY
Plain Text = HELLO DDU

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

I.] Divide P.T into groups of two (chunks)
Replace with wild card character if the chunk contains the same char.
HELLO DDU
⇒ HELXLODDU
⇒ HE LX LO DX DU

II.] MR (same row)
Replace with immediate next char.
⇒ DM

NW (same column):
Replace with immediate next char. (columnwise)
⇒ YN

HS (diagonal)
visit the row from H to match S & visit the row from S to match H's
H Y B
P Q S
⇒ BP

YP (not diagonal)
⇒ HS

// IJ ⇒ I×J×

⇒ Computational security – can be broken after a certain amount of time.

8/7/19 Hill cipher (substitution ciphers)
Plain text = "paymoneymoney"

$$\text{key} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}_{3\times 3}$$

Divide P.T. based on dimension of matrix
paymoneymoney

No. alphabets are: a → 0, b → 1, c → 2, ..., z → 25

pay:
$$\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \times \begin{bmatrix} 15 \\ 0 \\ 24 \end{bmatrix} \begin{matrix} p \\ a \\ y \end{matrix}$$

$$= \begin{bmatrix} (17\times 15)+(17\times 0)+(5\times 24) \\ (21\times 15)+(18\times 0)+(21\times 24) \\ (2\times 15)+(2\times 0)+(19\times 24) \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 375 \\ 819 \\ 486 \end{bmatrix} \bmod 26 = \begin{bmatrix} 11 \\ 13 \\ 18 \end{bmatrix} \begin{matrix} L \\ N \\ S \end{matrix}$$

∴ p → l a → n y → s

PAGE NO.
DATE: / /

mon: $\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \times \begin{bmatrix} 12 \\ 14 \\ 17 \end{bmatrix}$

$= \begin{bmatrix} 527 \\ 861 \\ 375 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 7 \\ 3 \\ 11 \end{bmatrix}$ h d l

emo: $\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \times \begin{bmatrix} 4 \\ 12 \\ 14 \end{bmatrix}$

$= \begin{bmatrix} 342 \\ 594 \\ 298 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 2 \\ 11 \\ 6 \end{bmatrix}$ ~~B~~ C l g

ney: $\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \times \begin{bmatrix} 13 \\ \\ \end{bmatrix}$

categorize: (cryptography)

i) Substitution cipher
Ex. A B C D E
P Q Z T U

D I T
depends on the T cipher

ii) Transposition cipher
The char. is not changed or replaced. Instead its position is changed.

D I T
Sent msg. I T D
key 2 3 1

Rail-fence cipher (Transpositional)

PT: meet me after toga party

depth (given): 2

1 1 1 1 ...

2 2 2 2

(1) ⇒ m e m a t r o a a t

(2) e t e f e t g p r

Encrypted:

memat roaatetefetgpry

Decryption:

$\frac{\text{length of message}}{\text{depth}} = \frac{20}{2} = 10$

(If odd no. of chars. then add wild card char. at the end)

For depth 3:

1			2			3			2			1			2			3			2			1		

m m t d a x

e t e f e t g p r y

e a r a t

⇒ mmtdaxetefetgpryearat

Transpositional cipher
PT: Attackposeduntiltwoam
key: 4 3 1 2 5 6 7

4	3	1	2	5	6	7
a	t	t	a	c	k	p
o	s	t	p	o	n	e
d	u	n	t	i	l	t
w	o	a	m	x	y	z

Read: 1 vertical 1 vertical

⇒ ttnaaptmtsuoaodwcoixknlypetz

Decryption: Length of message / highest no. in key = 28 / 7 = 4

∴ Split in groups of 4.

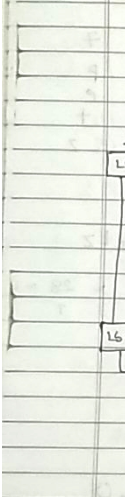
Steganography
- conceal the existing message

i) character marking
ii) Invisible ink
iii) Pin puncture
iv) Typewriter correction ribbon

S-DES Encryption (Simplified) [DES - Data Encryption Standard]

P10 = 3 5 2 7 4 10 1 9 8 6
P8 = 6 3 7 4 8 5 10 9
Key = 1010000010

Two parts : i) Key generation
ii) Original S-DES



1 2 3 4 5 6 7 8 9 10
1 0 1 0 0 0 0 0 1 0

(P10) 8 5 2 7 4 10 1 9 8 6
1 0 0 0 0 0 1 1 0 0

1 0 0 0 0 0 1 1 0 0
0 0 0 0 1 1 1 0 0 0
1 2 3 4 5 6 7 8 9 10

(P8) 6 3 7 4 8 5 10 9
1 0 1 0 0 1 0 0 -K1

1 2 3 4 5 6 7 8 9 10
0 0 1 0 0 0 0 1 1 1

6 3 7 4 8 5 10 9
0 1 0 0 0 0 1 1 -K2

∴ K1 = 10100100
K2 = 01000011

P I : 1111 0 0 1 1
Initial Permute) IP : 2 6 3 1 4 8 5 7
Expand & Permute) EP : 4 1 2 3 2 3 4 1)
P4 : 2 4 3 1

S_0 =

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

$S_1 =$

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

→ After IP : PT = 1 1 1 1 0 0 1 1 (1 2 3 4 5 6 7 8)

IP = 2 6 3 1 4 8 5 7

1 0 1 1 1 1 0 1

L R

R : 1 1 0 1 (1 2 3 4)

E/P : 4 1 2 3 2 3 4 1

XOR ⊕ 1 1 1 0 1 0 1 1

K1 : 1 0 1 0 0 1 0 0

0 1 0 0 1 1 0 1

O/P : 0100 1111 (0 1 2 3, 0 1 2 3)

(0,3) : $(00)_2 = (0)_{10}$ [ROW] | (1,3) : $(11)_2 = (3)_{10}$

(1,2) : $(10)_2 = (2)_{10}$ [column] | (1,2) : $(11)_2 = (8)_{10}$

S_0-Box : $(3)_{10} = (11)_2$ | S_1-Box : $(3)_{10} = (11$

(1 2 3 4)

1111 → P4 : 2431 → 1111

XOR ⊕ (L) 1011

0100

O/P : 1101 0100 (1st iteration)

(R)

Now, P.T becomes 1101 0100 (1 2 3 4 5 6 7 8)

IP = 2 6 3 1 4 8 5 7

1 1 0 1 | 0 0 0

L R

R : 1000 (1 2 3 4)

E/P : 4 1 2 3 2 3 4 1

$$\begin{array}{r} 01000001 \\ \oplus\ 01000011 \quad (K2) \\ \hline 00000010 \end{array}$$

O/P: 0000 0010

$(0,3) = (00)_2 = (0)_{10}$ $\quad (0,3) = (00)_2 = (0)_{10}$

$(1,2) = (00)_2 = (0)_{10}$ $\quad (1,2) = (01)_2 = (1)_{10}$

$S_0\ (01)_{10} = (01)_2$ $\quad S_1\ (1)_{10} = (01)_2$

0101

P4: 2 4 9 1

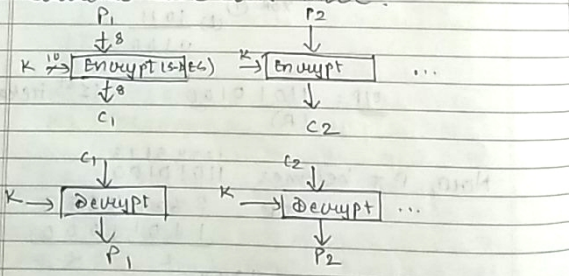
$$\begin{array}{r} 1100 \\ \oplus\ 1101 \\ \hline 0001 \end{array}$$

O/P: 10000001

5/7/19

Block cipher modes of operation

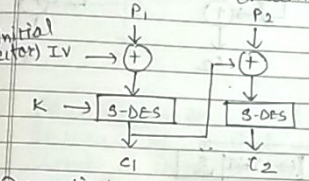
1) Electronic code book mode.



Like a dictionary. Ex - A will always be replaced by T)

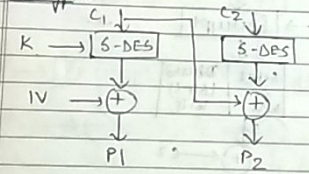
Since, the S-box and key values are not generated every time text is to be encrypted, crypt analysts can easily guess the original text based on the frequency of the letters.

2) Cipher Block Chaining



Due to this chaining the encoded character is dependent on its previous encrypted char. and does not remain fixed

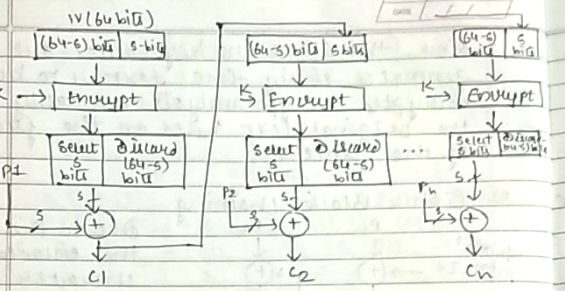
Decryption:



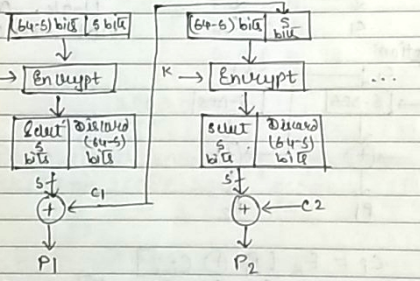
$$C_i = E_K [P_i \oplus C_{i-1}]$$
$$D_K[C_i] = D_K [E_K [P_i \oplus C_{i-1}]]$$
$$D_K[C_i] = P_i \oplus C_{i-1}$$
$$D_K[C_i] \oplus C_{i-1} = P_i \oplus C_{i-1} \oplus C_{i-1}$$
$$= P_i \oplus 0$$
$$= P_i$$

3) S-bit output feedback mode

IV is loaded in a 64-bit register and then the encryption is begun. 's' depends on the length of plain text.

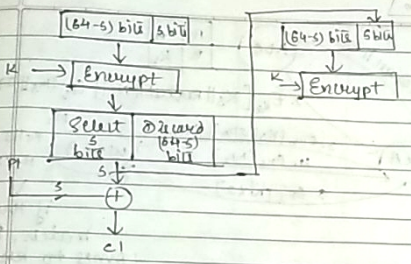


Decryption:

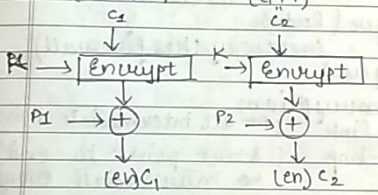


⇒ In s-bit cipher feedback mode, Parallel execution possible as the generated output (CI) is not being used anywhere in the further steps.

Advantage of using s-bit cipher feedback mode over s-bit output feedback mode?



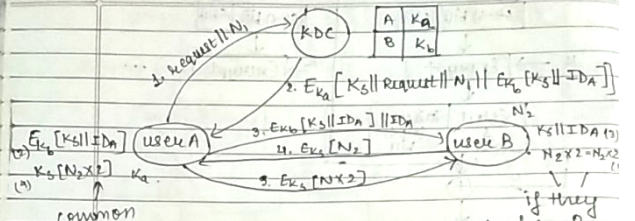
⇒ Counter mode.
Instead of initial vector (IV), we will send a counter value to the other party (counter)



- Easy to implement
- Parallel execution possible
- Compatible with both H/W & S/W

Secret Key Distribution Scenario
N_1 - Unique request identifier

⇒ K_s is not sent to B initially (by KDC)



common func.

if they match, B comes to know that A also has the same K_s

17/7/19 Placement of encryption function

i) Server ii) client

iii) Network layer (Router)

Gateway (Has firewall)

(every layer)

Types of encryption:

i) Link-to-link (At all intermediate points)

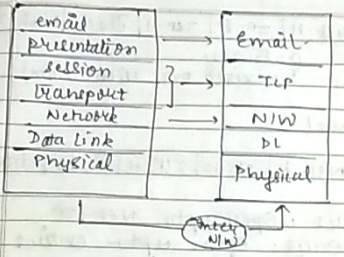
ii) Hop-to-hop (start point to end) no intermediate encrypti

Link-to-link when used distributing keys becomes a tedious job

Hop-to-hop can lead to IP spoofing or port spoofing.

22/7/19 Relationship between protocol level and encryption

Link-H	Net-H	IP-H	TCP-H	Data	Link-T



(a) Application level. Encrypted

Link-H	Net-H	IP-H	TCP-H	~~Data~~	Link-T

Valid if it passes through router, links gateway & device.

b) TCP level.

Link-H	Net-H	IP-H	~~TCP-H Data~~	Link-T

This configuration can be understood by (valid when passed through) routers links, end devices.

Gateway requires the port no. on which to forward the request. Thus it needs the TCP-H. Gateway should have key k to decrypt the TCP-H. If it is a intermediate gateway, it needs to decrypt the data too.

| Link-H | Net-H | IP-H | TCP-H | Data | Link-T |

gateway (exists on client side)

c) Link level

| Link-H | ~~Net-H~~ | ~~IP-H~~ | ~~TCP-H~~ | ~~Data~~ | Link-T |

At routers : Open upto Net / IP
At gateways: Open ~~upto~~ entire packet

23/7/19 Random number generation

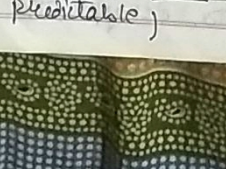
Randomness:
1) Uniform distribution [freq. of every char should be nearly equal]
2) Independence [NO repitition]
3) Unpredictability

i) Pseudorandom number generation (PRNG)

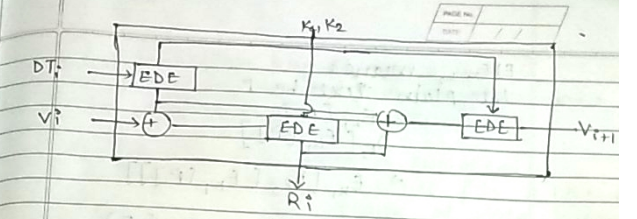
$X_{n+1} = (aX_n + c) \bmod m$

$a = 7, c = 0, m = 32, X_0 = 1$

ii) Crypto graphical PRNG's
eg:- encryption



(Still predictable)



ANSI X 9.17 PRNG [Provides complete eqn for generating pseudorandom nos.]

$R_i = EDE_{K_1,K_2}[V_i \oplus EDE_{K_1,K_2}[DT_i]]$

$V_{i+1} = EDE_{K_1,K_2}[R_i \oplus EDE_{K_1,K_2}[DT_i]]$

↑ Date time of a system.

PRNG:

$x_1 = (ax_0 + c) \bmod m$
$= (7(1) + 0) \bmod 32 = 7$

$x_2 = (ax_1 + c) \bmod m$
$= (7(7) + 0) \bmod 32 = 17$

$x_3 = (7(17) + 0) \bmod 32 = 23$

$x_4 = (7(23) + 0) \bmod 32 = 0$

$x_5 = 7$

$x_6 = 17$

Thus, this eqn can generate atmost 4 distinct pseudorandom numbers.

When we increase the value of m, the no. of distinct pseudorandom nos also increases.

EDE_{K_1,K_2} means:

Let plain text be P

$\therefore E_{K_1}[P]$

$D_{K_2}[E_{K_1}[P]]$

$\Rightarrow E_{K_1}[D_{K_2}[E_{K_1}[P]]]$

Types of attack (on security)

1) Passive attack
   - Release of message content
   - Traffic analysis

2) Active attack
   - Masquerade (hiding the real identity)
   - Replay (occurs in case of single sign-on)
   - Modification of message
   - Denial of service

use someone's ticket to avail other services as the other can behalf of person

24/7/19

Cryptography system characterized as follows:

1) Type of operations
   - Substitution
   - Transformation

2) Number of keys
   - Private / Secret / Single key algo (Both the ends use the same k

→ HTTP w.r.t SSL & TSL

- Public/Two key algo.
(One key is used for encryption and a different for decryption)

a) The way plain text is processed.
   i) Batch process (wait for a certain chunk of data before starting to process it)
   ii) Raw bits (Processing continues as bits start coming) (ex- RC4 algo., RC5 algo.)

Types of attack on encrypted message
i) Cipher text only
Intruder only has access to the algo and the cipher text.
Every protocol has a certain set of defined algorithms.

ii) Known plain text
Intruder has access to:
Algo., cipher text, part of plain t (PT → cipher te

iii) Choosen cipher text
Intruder has access to:
Algo., cipher text, (cipher → P.T)
Some samples of cipher text an its corresponding plain text is kn

iv) Choosen plain text.

v) Choosen text (everything is know

Caesar cipher

ET: PHHW PH

To get the plain text, we follow brute-force approach.

1: DlGlV OG
2: NFFU NF
3: MEET ME
4: LDDS LD.

// stop where we get natural lang. text

Mono alphabetic cipher

a	b	c	d	e	...	t	...	z
k	p	q	z	t		l		c

$26!$ possibilities of keys.