TRG

DATE
PAGE No.

E-commerce & E-security

1. computer security
2. Network security
3. Internet security

Authentication Network-Security - william Stawling.

2/7/19 Introduction

Ch-1

Application
presentation
Session
} Application

TCP ← Transport
IPSec ← N/w
Transport
Network

NO security { Datalink
physical
} Host-to-network

OSI Security Arch TCP/IP

o) Security Attacks

Active - Attacker will try to modify the data

Passive - Attacker won't modify the data

X800 ITU-T

* Services provided by X800

1) Authentication

connection oriented transfer → 1) peer entity - used with logical connection

2) data origin auth - source of the data must be authenticated

↑

connectionless transfer

2) Access control :-

only Authenticated users are allowed to access the data.

3) Data confidentiality :- protection of transmitted data from passive attacks.

4) Data Integrity :- Data should not be modified during the transition.

DATE
PAGE No.

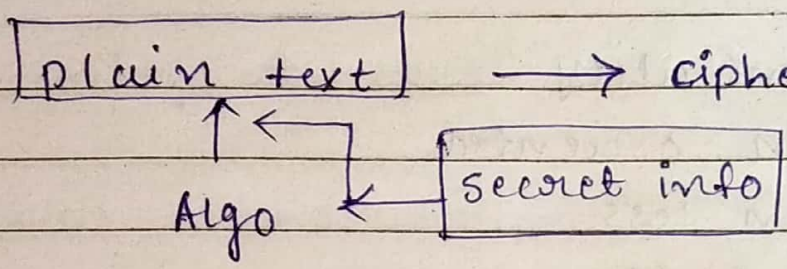
- Date confidentiality
  - → connection oriented
  - → connection less
  - → Selected field
  - → traffic confidentiality

* Date Integrity
  - → connection oriented
  - → connection less
  - → selected field.

5] Non Repudiation
provide protection from denial of one of the entity in communication.

* Security Mechanism done in OSI
  - Encryption / Decryption → presentation layer, Application layer in TCP/IP
  - Digital signature
  - traffic padding
  - Strict routing control - Only specific IPs can take the packet and pass to another IPS. Untrusted IPs are not allowed to pass the packet.

Cryptography



cryptology

crypt analysis

exploits the algo

Brute force

(1) Type of operation used to transform the data

Substitution
- substitute one data inplace of other.
- One character replace inplace of other.

Transposition
- Changing the order of the information (permutation)

2) no of key used.

(I) Symmetric key - one key is used for encryption & same key is used for decryption.

problem - key distribution.

(II) Asymmetric key - more than one key is used for enc/decry. one key used for encryption and another is for decryption.

public key & private key

(3) way in which plain text processed.

substitution → Symmetric key - 1 key

ceaser cipher key - {0 - 26} 26 keys
alphabets

(Ascii + 3) %. 26

plain text Hello this is my puss xyz
key : 3 ↓↓↓↓
khoor

$C = [(Ascii + 3) \%. 26]$

$P = [(C - key) \%. 26$

Monoalphabetic substitution cipher

Keyword → tiger 26! possibilities.

A	B	C	D	E	F	...	Z
t	i	g	e	r	a	b	c	d	f	g	h	j	...

Monoalphabatic transpo cipher

26! possibilities.

keyword : tiger

t	i	g	e	r	a
b	c	d	f	h	j
k	l	m	n	o	p
q	s	u	v	w	x
y	z				

A	B	C	D	E	F	G	...	Z
t	b	k	q	y	i	c	l	s	z	...

* playfair cipher

2 letter at a time.

Keyword.

5 x 5 matrix i&j is considered together

t	i|j	g	r	r
a	b	c	d	f
h	k	l	m	n
o	p	q	s	u
v	w	x	y	z

Rules: 1) remove all spaces & punctuation marks
2) build pair of character
3) pairing of repeatable character is not possible
hello how are you.
he lx lo ho wa re yo ux
↑
filler

4) If i & j comes together then i paired will filler and j paired with next character

If the pair of a message falls in the same row then it will replace with next character of the same row. If it is last character then it replace with the first character of that row (circular)

If the pair of a message falls in the same column it will replace with the character below ~~th~~ of that column & if it is last then it will replace with the 1st char of that column.

diagonal row of 1st char & col^{n} of 2nd intersection is replaced with 1st character and it's diag element with 2nd char
gd
ee

keyword - monarchy

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

ddu nadiad.
dx du na di ad
bz cz ar bk rb

i j i j x

ix jx ix jx xy

↑

2nd filler

2nd filler is used only when the filler character is present in the message

otherwise in whole message filler chareeter is same.

5|7 Hill cipher (polygraphic substitution technique)

encrypt multiple chareeter at ee time. based on linear Algebra.

A = 0

B = 1

C = 3

⋮

Z = 25

key

$$M = \begin{bmatrix} & \\ & \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix} \text{ mod } 26.$$

$$M \cdot M^{-1} = I$$

to find out plain text from cipher text

$(M^{-1} \cdot C) \bmod 26 = P$

$$\text{key} = \begin{bmatrix} 2 & 4 & 5 \\ 9 & 2 & 1 \\ 3 & 17 & 7 \end{bmatrix} \begin{bmatrix} 0 \\ 19 \\ 19 \end{bmatrix} = \begin{bmatrix} 171 \\ 57 \\ 456 \end{bmatrix} \begin{bmatrix} 4 & 5 \\ 2 & \\ 17 & 7 \end{bmatrix}$$

$3 \times 3 \quad 3 \times 1$

PT = attack

CT = pfogoa

$$\begin{bmatrix} 15 \\ 5 \\ 14 \end{bmatrix} \quad \begin{bmatrix} PFO \end{bmatrix}$$

$$\begin{bmatrix} 2 & 4 & 5 \\ 9 & 2 & 1 \\ 3 & 17 & 7 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 10 \end{bmatrix} = \begin{bmatrix} 58 \\ 14 \\ 104 \end{bmatrix} \cdot 1.26 \quad \begin{bmatrix} 6 \\ 14 \\ 0 \end{bmatrix} \text{ goa}$$

$PT = (\text{Pfogoa} \times M^{-1}) \bmod 26$

* vigenere cipher. (moalphabetic)

keyword = bank = 4

Msg = attack at four.

bankba nk bank

	a	b	c	d	...	z
a	A	B	C	D	...	Z
b	B	C	D	E	...	A
c	C	D	E	F	...	B
d	D	E	F	G	...	C
!	E	F	G	H	...	D
!	!					
z	Z	A				

mapping msg with rows & key with columns

Msg attack at four
bankba nk bank
↓
BT

* One time pad.

key length must be equal to the message length. but pattern inside a key shouldn't be repeated.

considere spaces.

- Very difficult to generate random key. for long msg.
- not feasible to transfer entire file.

Transposition tech :-

Railfence cipher
depth = 2 (rows)
distribute dats (diagonal form)

codes are interesting. ddu nedidd

P.T 1 c d s r
2 o e d e

P.T d u a i d
d n d a

C.T cdsroeda

C.T duaiddnda

columnar transposition cipher

key = 3 2 1 4 5
P.T n e t w o
r k s e c
u r i t y

tsickrnruwetocy

tsiekrnrnuwetocy

15/5 = 3 char in each column starting with the column having number 1.

3	2	1	4	5
n	e	t	w	o
r	k	s	e	c
u	r	i	t	y.

If key is alphabet then

Key = [A P P L E
       1 4 5 3 2
         5 or 4

Eg Keyword :- L A Y E R
P.T : welcome to network security.

LAYER
3 1 5 2 4
w e l c o
m e t o r
e t w o r
k s e c u
r i t y z

eetsicoocywmekronrzltwet

3 1 5 2 4
e e t s i
c o o c y
w m e k r
o r r z
l t w e t

eomntsckyecewolizrztocrw

3 1 5 2 4
e e t s i
c o o c y
w m e k r
o r r z
l t w e t

DES

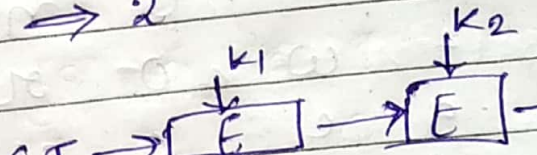
9/7

Substitution + transposition

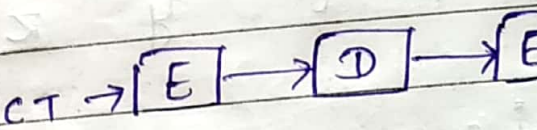
Std : 64 bit block of P.T. → 64 bit | 64 | 64.

56 bit key ⟹ 2^{56}.

Double DES



Tripple DES

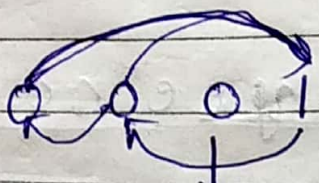


Advance encryption standard (AES)

* Simplified DES.

	block length	key length.
Std	64 bit	56 bit
S-DES	8 bit	10 bit

Permutation.



0 1 0 0

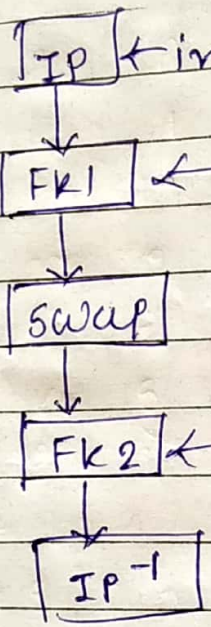
2 4 3 1

3rd bit → 3rd

4th → 2th

1st → 4st

2nd → 1.



Key generation ⟹ 10 bit key

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

P_{10}	3	5	2	7	4	10	1	9	8	6
	1	0	0	0	0	1	0	1	1	1

Shift 1 bit to left

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

← For K2 apply 2 times left shift.

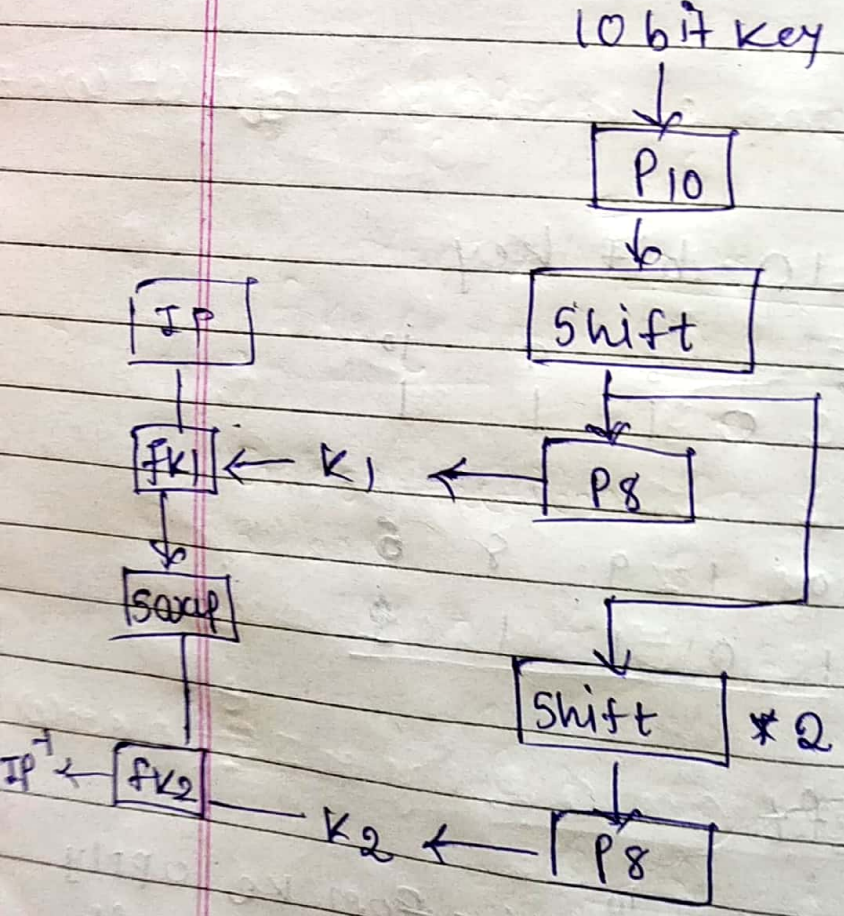
P_8	6	3	7	4	8	5	10	9
K_1 =	0	0	1	0	1	1	1	1

shift 2 times on shifted data.

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

P8: 6 3 7 4 8 5 10 9

K2 = 1 1 1 0 1 0 1 0



\# key = 1 1 0 0 0 1 1 1 1 0

(1 2 3 4 5 6 7 8 9 10)

3 5 2 7 4 10 1 9 8 6

0 0 1 1 0 0 1 1 1 1

(1 2 3 4 5 6 7 8 9 10)

0 1 1 0 0 1 1 1 1 0 ←

P8 : 6 3 7 4 8 5 10 9

K_1 = 1 1 1 0 1 0 0 1

2 times shift

(1 2 3 4 5 6 7 8 9 10)

1 0 0 0 1 1 1 0 1 1

P8 : 6 3 7 4 8 5 10 9

K_2 = 1 0 1 0 0 1 1 1

\# P.T = 8 bit = (1 2 3 4 5 6 7 8) 1 0 1 0 0 1 0 1

P8 = 2 6 3 1 4 8 5 7

0 1 1 1 0 1 0 0

IP :

1	2	3	4	5	6	7	8
2	6	3	1	4	8	5	7

IP^{-1} :

1	2	3	4	5	6	7	8
4	1	3	5	7	2	8	6

f_{k1} $\quad k_1 = 00101111$

$f_k(L, R) = (L \oplus f(R, k_1)), R$

$f_{k_1}(0111, 0100) = (0111 \oplus f(0100, k_1)), R$

(i) Expansion Permutation on $R = 0100$ (positions 1 2 3 4)

E/P = 4 1 2 3 2 3 4 1

$\oplus$ 0 0 1 0 1 0 0 0

k_1 0 0 1 0 1 1 1 1

0 0 0 0 0 1 1 1

S_0 S_1

(ii) ← Substitution

& S-box. S_0 & S_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

1st & 4th gives row number

2nd & 3rd " column number

row col^n

00 00 - 1 → 01

01 11 → 3 → 11

(iii) S-box Substitution

CT = 01 11

1 2 3 4

(iv) P_4 = 2 4 3 2

1 1 1 0

(v) L ⊕ R

0111 ⊕ 1110

1001

⇒ 1001 ⊕ 0100

IP

fk1

1001 0100

swap

0100 1001

fk_2

10/7 1. IP

2. complex function $fk(L, R) = [L \oplus P_{k_1}(R, K_1)], R$

i) EP on R_4 bits 4 bit → 8 bit

ii) EP ⊕ K1

8 bit 8 bit

iii) S-box substitution S_0 S_1

1st 4 bit next 4 bit

iv) P_4 Permutation of (iii)'s result

v) L ⊕ (iv)

L modified ⊕ R

3) swap

4) complex function with K_2

1001 0100

after swap

0100 1001

$K_2 = 1110\ 1010$

$f_{K_2}(0100, 1001) = (0100 \oplus f(1010, K_1)), R$

$R = \overset{1}{1}\overset{2}{0}\overset{3}{0}\overset{4}{1}$

E/P = 4 1 2 3 2 3 4 1

1 1 0 0 0 0 1 1

⊕ 1 1 1 0 1 0 1 0

0 0 1 0 1 0 0 1

S_0 S_1

S_0 00 01 0 row 1 col^n 00

S_1 3rd row 0th col^n 10

CT = 0010

DATE
PAGE No.

P4 = 2 4 3 2
0 0 1 0

L ⊕ 0010
0000 ⊕ 0010
f_{k_2} = 0010, 1001

IP^{-1} 4 1 3 5 7 2 8 6
0 0 1 1 0 1 1 0

---

1 2 3 4 5 6 7 8
PT = 0010 1000
k_1 = 1110 1001
k_2 = 1010 0111
P8 = 2 6 3 1 4 8 5 7
EP = 4 1 2 3 2 3 4 1
P4 = 2 4 3 1
IP^{-1} = 4 1 3 5 7 2 8 6

1) IP on PT
0010 0010

2) f_{k_1} = [L ⊕ P_{k_1}(R, k_1)], R

[0010 ⊕ P_{k_1}(0010, k_1)], 0010

(i) E/P on R 0010

4 1 2 3 2 3 4 1

0 0 0 1 0 1 0 0

(ii) ⊕ 1 1 1 0 1 0 0 1

1 1 1 1 1 1 0 1

S0 S1

(iii) 3rd row 2nd col^n 3rd row 2nd col^n

10 00

(iv) ~~fk1~~ F_4 on 1000

2 4 3 1

0 0 0 1

v) L ⊕ 0001

0010 ⊕ 0001

0011

fk_1 = 0011 0010

3) swap

~~1 2 3 4 5 6 7 8~~

0010 0011

L R

4) ~~0 1 0 0 1 0 1~~

4) $fk_2 = [L \oplus Pk_2(R, K_2)], R$

$= [0010 \oplus Pk_2(0011, K_2)], 0011$

E/P on R

4	1	2	3	2	3	4	1
1	0	0	1	0	1	1	0

$\oplus$ 1 0 1 0 0 1 1 1

0 0 1 1 1 0 0 0 1

S0 S1

1 2 1 C 1 2 0 C

0 0 1 0

0010

P4 on 1010

2	4	3	1
0	1	1	1

$L \oplus$ 0011

0010 $\oplus$ 0011

0001

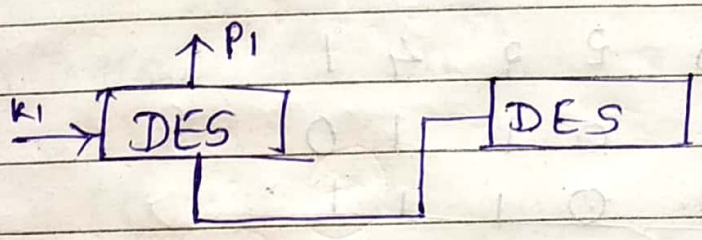
$fk_2 = 0001\ 0011$

$IP^{-1} = 10001010$

Block cipher modes :-

→ Algorithm which operates on block data cipher.

→ DES



1. Electronic code block
2. cipher block chaining
3. cipher feedback
4. output feedback
5. counter

64 → 2^{64} distinct block

56 → 2^{56} distinct keys

4 bit block = 2^4

0001

$K_1 \rightarrow CT_1$

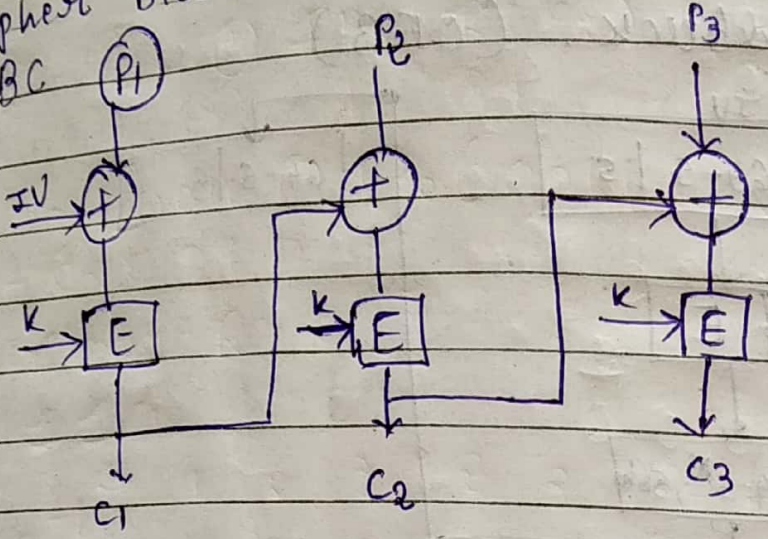
$K_2 \rightarrow CT_2$

$K_3 \rightarrow CT_3$

$K_n \rightarrow CT_n$

15/1/24

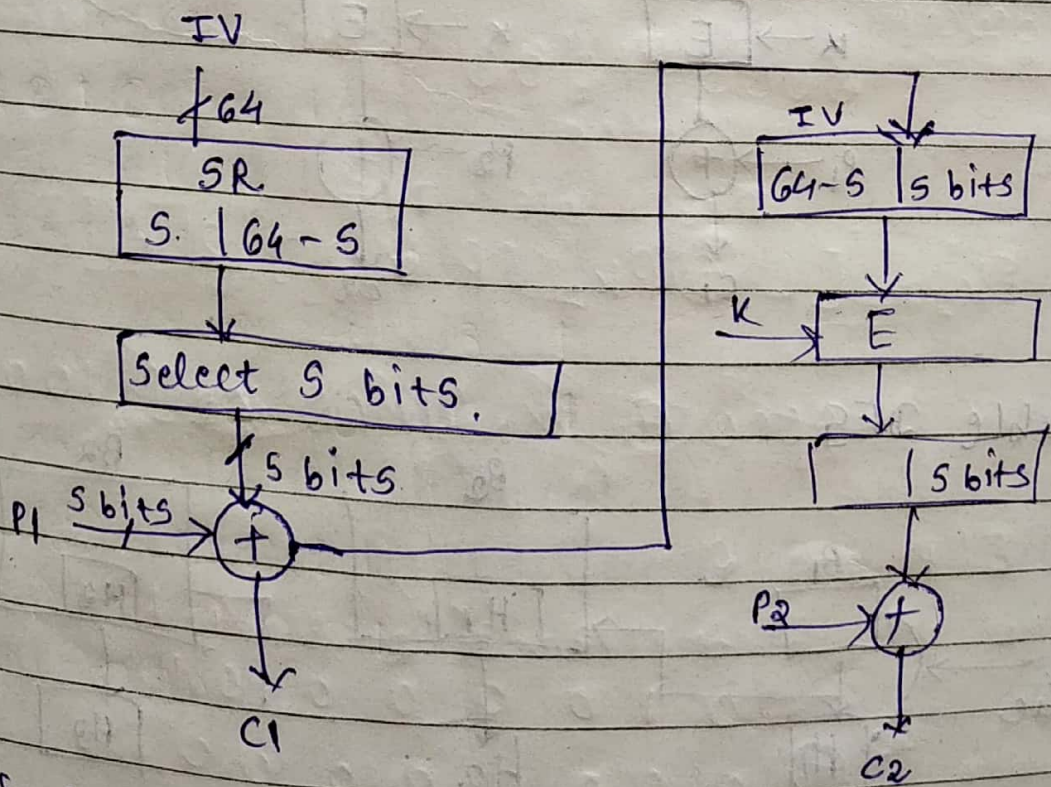
2) cipher block chaining.



IV - initialization vector.

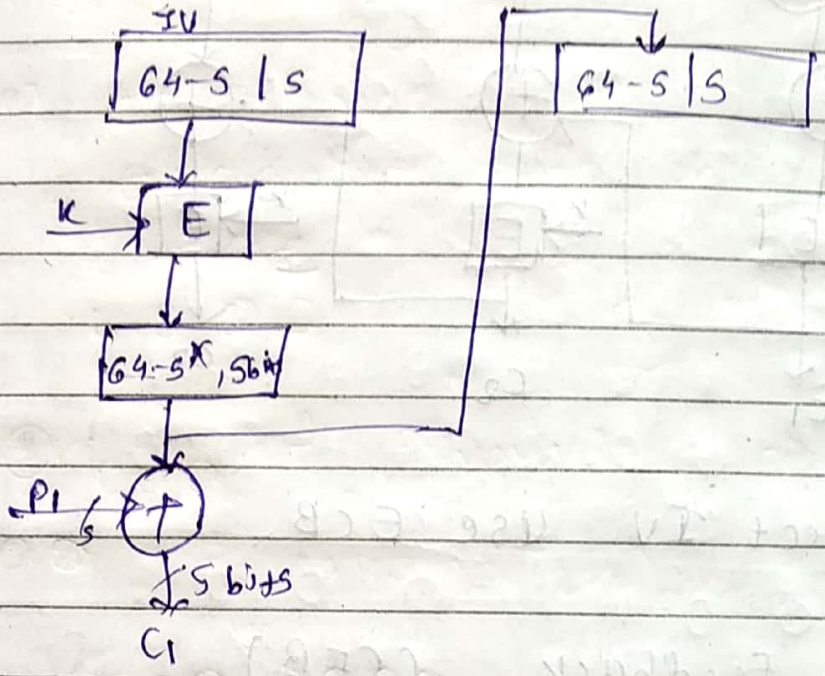
To protect IV use ECB.

3) cipher feedback. (CFB)
converting block cipher into stream cipher.

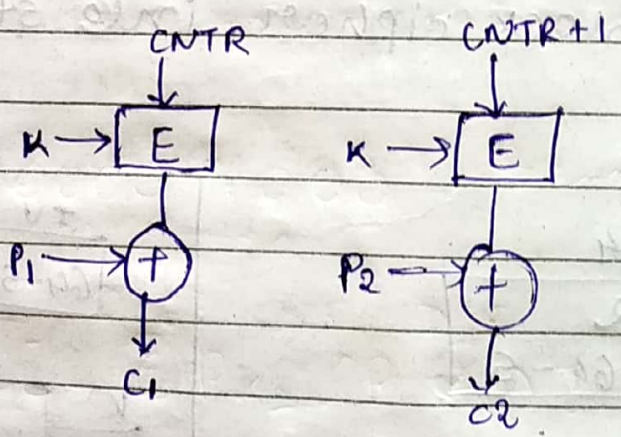


cons: If error is in C_1 then it is propogated in next level.

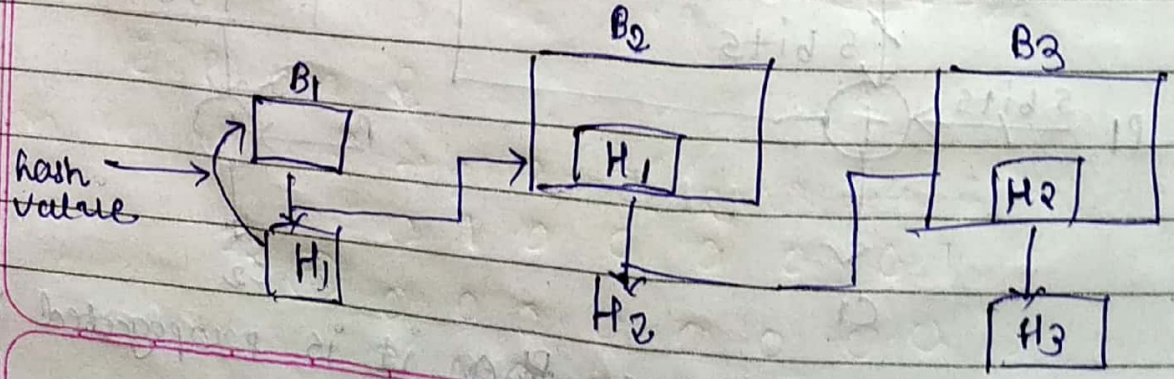
4) Output feedback (OFB)



5) CNTR



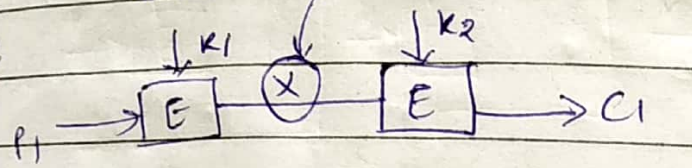
* Double DES



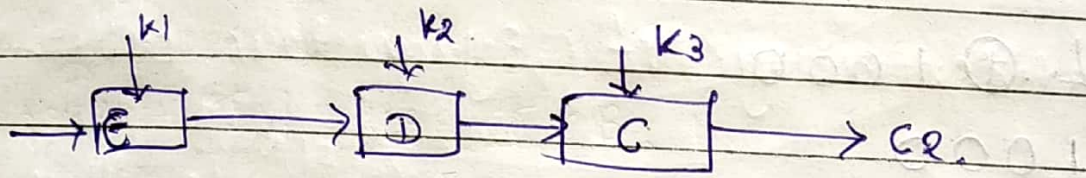
DES is weak bcoz it uses only 2^{56} keys. To strengthen the performance of DES uses double DES.

DES meet in middle attack.

Double DES



Tripple DES



P.T = 0000 0000
key = 0000000000
E.P = 4 1 2 3 2 3 4 1
K_1 = 00000000 = K2
IP = 2 6 3 1 4 8 5 7
IP^{-1} = 4 1 3 5 7 2 8 6

IP on PT = 0000 0000
f_{k_1} = [L ⊕ P_{k_1}(R, K_1)], R
0000 ⊕ P_{k_1}(0000, K_1)], 0000

EP on R

0 0 0 0 0 0 0 0
⊕ 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0.

S_0 S_1

row col row col

0 0 0 0

0 1 0 0

0100

2 4 3 1

1000

L ⊕ 1000

1000

$fk_1 = 10000000$

Swap

0000 1000

$fk_2 = [L \oplus P_{K_2}(R, K_2)], R$

$0000 \oplus P_{K_2}(1000, K_2), 1000$

E/P on R

4 1 2 3 2 3 4 1

0 1 0 0 0 0 0 1

K_2 ⊕ 0 0 0 0 0 0 0 0

0 1 0 0 0 0 0 1

S0

row 2 col

11

S1

row 0 col

10

1110

2 4 3 1

1 0 1 1

L ⊕ 1001

1011

1 2 3 4 5 6 7 8

f_{K2} = 1011 1000

IP^{-1} 4 1 3 5 7 2 8 6

1 1 1 0 0 0 0

AES

Advance encryption standard.

1. Sub bytes. (byte substitution - S boxes)
2. Shift rows.
3. mix column.
4. Add round key.

After shifting, in neco matrix.

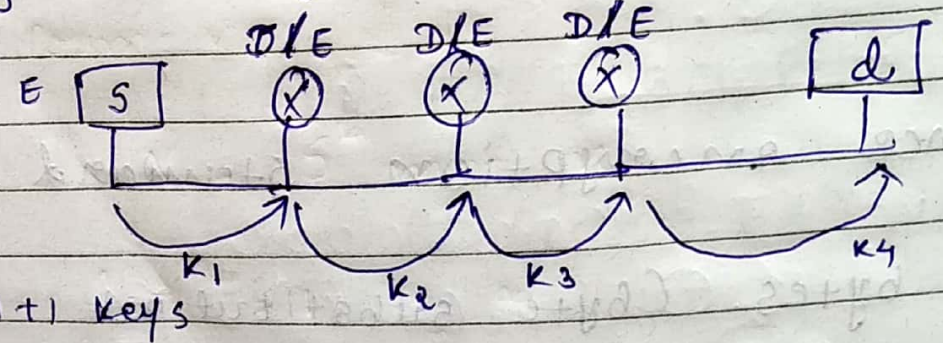
1st row — same
2nd — 1 Byte left shift (circular)
3rd - 2 " "
4th - 3 " "

* Confidentiality at Symmetric cipher :-

* placement of encryption algorithm

Link to link encryption. (implemented on network layer)

each link data will be decrypted and again encrypted



n+1 keys

n to n encryption (implemented at Application layer)

data only decrypted at receiver not at intermediate node.

2) should be able to identify the possible security attacks.

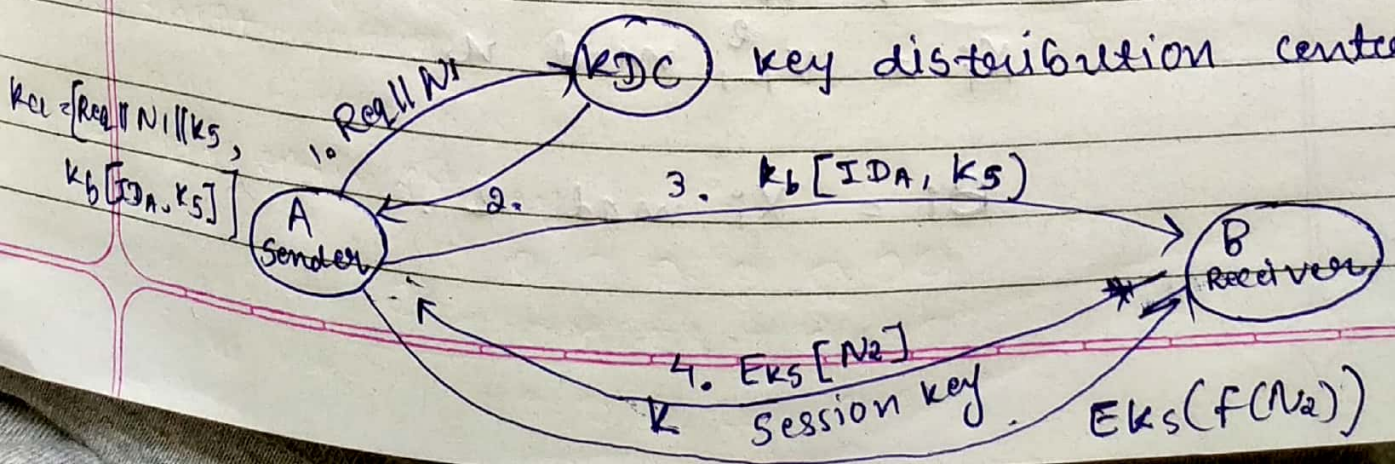
17/12 Charecteristics of adv symm algo

- DES
- AES

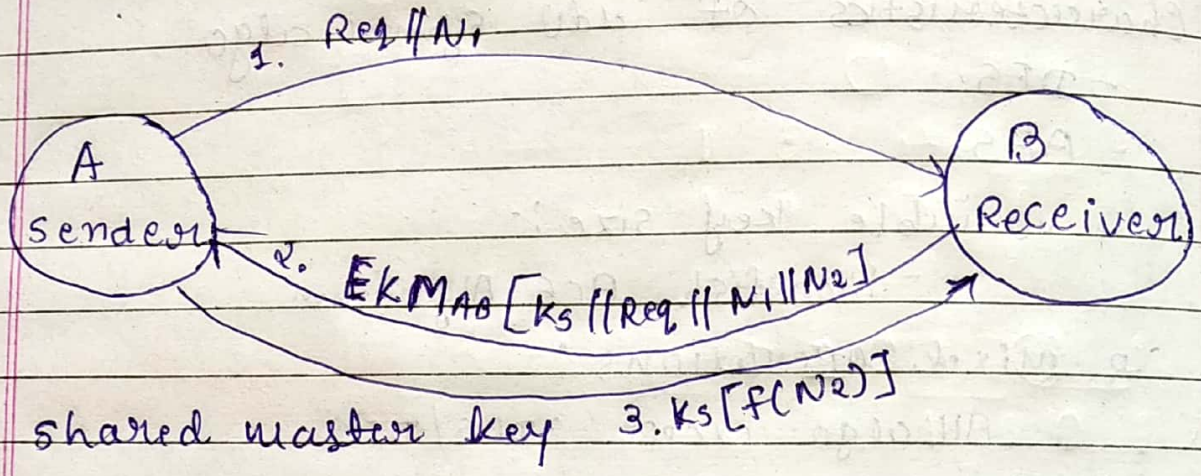
1. Variable key size :-
   - Blockfish, RC5 Algorithm
2. Mixed operations :-
   All algo except 3DES / DES
3. Data dependent rounds :-
4. key dependent s-boxes.
5. Variable plaintext / ciphertext block
6. Variable rounds.
7. Operation on both halves of data.

Centralized key distribution.

Central entity which will distribute the key.



decentralized



shared master key

23/4 Blum blum ~~Shub~~ generator :-
Cryptographically secure pseudo random bit generator
Binary string.
1) P Q
2) $n = p * q$
3) Prime no

$$X_0 = S^2 \bmod n.$$

for $i = 1$ to ∞

$$X_i = X_{i-1}^2 \bmod n.$$

$$B_i = X_i \bmod 2$$

consider 2 prime nos. p = 7 q = 11, s = 19

$n = 77$

$x_0 = (19)^2 \% 77$

$x_0 = 53$

$x_1 = (53)^2 \% 77 = 37$ 100101 5

$x_2 = (37)^2 \% 77 = 60$ 111100 4

$x_3 = (60)^2 \% 77 = 58$ 111010 2

$\log_2(\log_2(n)) = 2.64 \approx 3$

4 bit no

101 100010 x

11 1