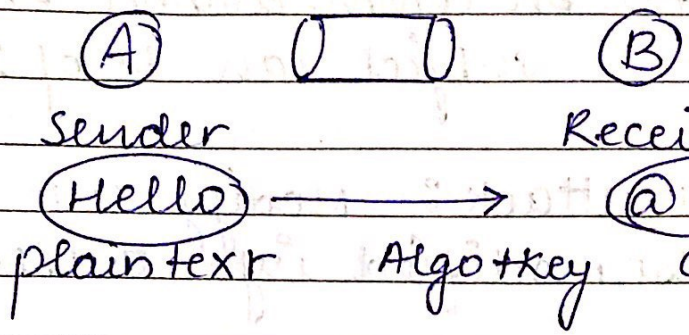
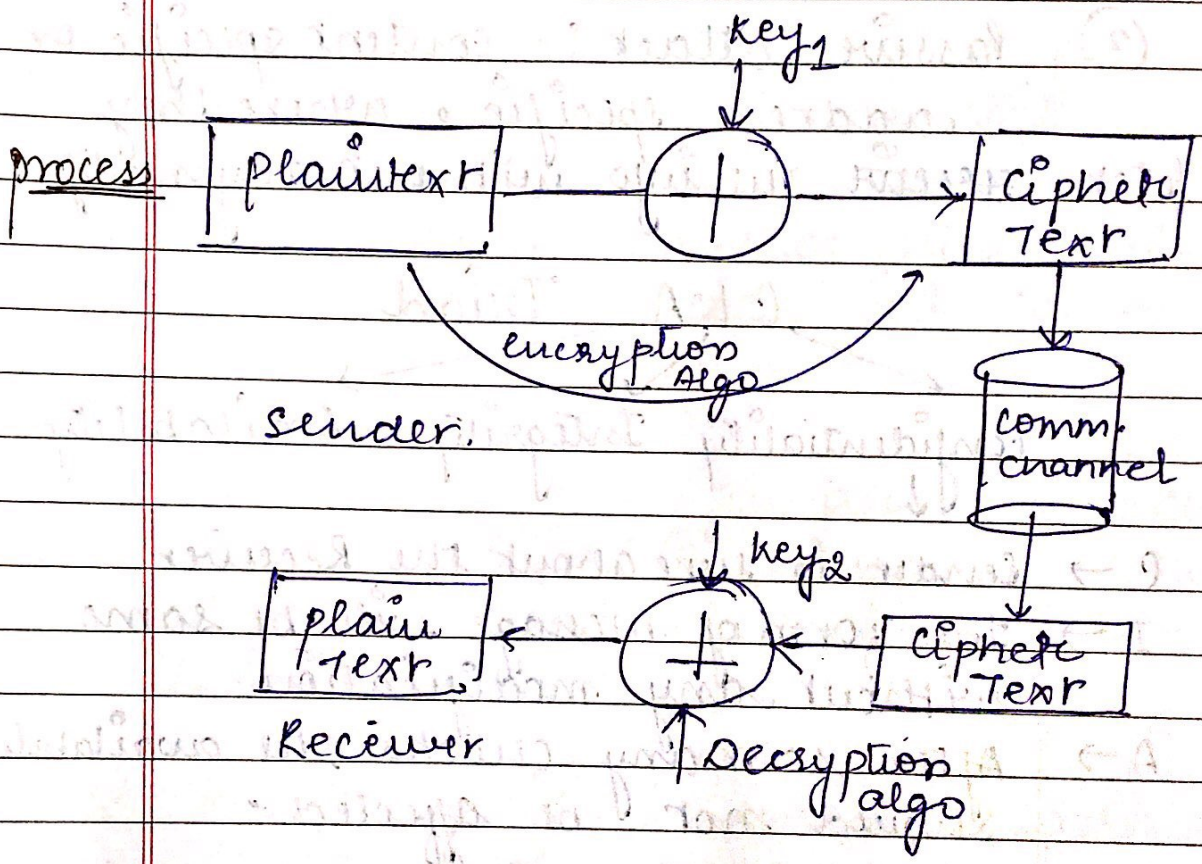
30/July/18

(secret writing) ← Greek

CRYPTOGRAPHY





if Key1 = Key2 Symmetric key crypto.

Key1 ≠ Key2 Asymmetric key crypto

Stagnography :- add text in a medium & then send.

Scanned with CamScanner

Attack on comms. channel or on subject can be of 2 types

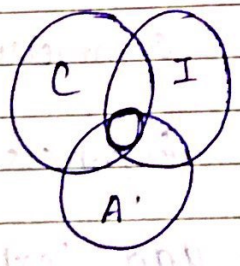
① Activ attack :- modify info & send false modified info to receiver.

② Passive attack :- content specific or address specific. where they fetch ~~receiver~~ the info without any modifica

CIA Triad

confidentiality ↓ Integrity Availability

C → Sender is sure about the Receiver
I → The form of message will be same without any modification.
A → After so many checks the availabilty should not be affected.



There must be a proper balance b/w all these three terms.

Security & Time complexity.

CIA is achieved by :-
① Authentication
② Authorization

① where the credentials of a user are checked & verified is known as Authentication. (fingerprint, face Recognition, retina etc).

② After Login → Authorization tells about the access limitation & permissions for particular use.

Confidentiality attacks :-
① Reception :- when the attack is content specific. Eg Ⓐ & Ⓑ company. A↑ B↓ B fetches detail of employee of A & "incr" its prod.

② Address specific :- check the address & attack the vendors address.

Integrity
→ Modification in data
→ Masquereading ~~Masoreading~~ :- attacker pretends to be a valid user
→ Replaying :- one msg many times.
→ Repudition :- either sender or receiver denys for the msg

Scanned with CamScanner

Availability

① Denial of service attack (DOS) :- many request at a time so that even valid user can't use that.

Components of encryption Decryption

① Plaintext
② CipherText
③ Encryption algorithm
④ Decryption algorithm
⑤ Key

Symmetric key cryptography

Substitution algo / Cipher	Transposition Algo / Cipher
① secure	① less secure
② Key required	② no key required
③ Substitution takes place	③ Re-shuffling takes place

Note :- Before cryptography earlier we use compression

Compression :- Merging 2 or more data together & separate using keys. less efficient.

Algorithm

Caesar Cipher.

Consider Reference No. for coding

A = 0
B = 1
C = 2
⋮
Z = 25

(PlainText) PT = BCD

(CipherText) CT = (PT + 3) mod 26.

$CT_1(B) = (1+3) \bmod 26$
$= 4$
$= (E.)$

$CT_2(C) = 5\ (F)$

$CT_3(D) = 6\ (G)$

Encrypted (CT) = EFG.

for decryption use $PT_1 = (CT_1 - 3) \bmod 26$.

Easy but not secure. & works only for Alphabets.

So we use Generalized ceasar cipher.

$CT = (PT + K) \bmod 26$

↓

vary (0 - 25) which is known only to comm. party

Book :- → William Stalleys ✓ prefered
→ Forozen

Scanned with CamScanner

NOTE { Stream cipher :- when one alphabet are encrypted one by one
Block cipher :- one or more alph. can be encrypted.

31st July '18.

Playfair Cipher.

Here we will use stream ~~Block~~ cipher.

PT = COMPUTER } encrypt this PT using key into encry form.
Key = CRYPTO

Make pairs of 2 CO MP UT ER.

Assumption

① There may be odd no. of alphabets. Then we will add a filler letter X
Eg RUCHI(X)-filler.

② for same alphabet, add filler letter in b/w & make pairs.
Eg BALLOON
X X
BA LX LO ON

③ Make a box of 5X5

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

ROW
COLUMN

26 alphabet but 25 block so put I/J together.

Assumption about I/J is that they will rarely/never occur together in a text.

3 cases for paired alphabets.

① when they are in same ROW:-
Eg ① BD.
So CT for BD will be just next alphabet for each so,
BD = DE.

② AE
CT = A → B so, CT(AE) = BO
Circular shift E → O

② for same column :-
Eg BN.
Move downwards, (immediate below element)
B → H N → W (BN) → HW

③ Different Row different column.
Eg AQ.
→ for first alphabet :- Move in the row for the first alphabet
for second alphabet :- Move in the column for the second Alphabet find the strike point.
A → D AQ (CT) = DM
Q → M

Scanned with CamScanner

find CT for COMPUTER

CT= OFQRZCAT.

Limitation

① X can be a alphabet & a filler too
② Use only for alphabets
③ I/J lie on the same position.

Que PT= DIT UNIVERSITYX

KEY = BCDQR

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

BLUOIKWADUMOZY

6th Aug '18

AFFINE CIPHER

Plain Text (PT) = AFFINE CIPHER

$C = (AP + B) \bmod 26$

C ↓ CT

A & B are Keys.

Let A=5 B=8.

A → Multiplicative key

B → Additive key.

If we put A=1 then, it will a case of Caesar Cipher.

#Condition :- A & 26 (mod value) both should be coprime.

for plain Text from CipherText

$P = A^{-1}(C-B) \bmod 26.$

Note. Both works only for Alphabets.

A - 0	J - 9	S - 18
B - 1	K - 10	T - 19
C - 2	L - 11	U - 20
D - 3	M - 12	V - 21
E - 4	N - 13	W - 22
F - 5	O - 14	X - 23
G - 6	P - 15	Y - 24
H - 7	Q - 16	Z - 25
I - 8	R - 17	

Scanned with CamScanner

	A	F	F	I	N	E	C	I	P	H	E	R
for	0	5	5	8	13	4	2	8	15	7	4	17

Given A = 5 , B = 8.

for A = 0×5+8 = 8
F = 5×5+8 = 33
I = 8×5+8 = 48
N = 13×5+8 = ~~48~~ 73
E = 4×5+8 = ~~28~~ 28
C = 2×5+8 = ~~28~~ 18
P = 15×5+8 = 83

H = 7×5+5 = 43
R = 17×5+5 = 93

	A	F	F	I	N	E	C	I	P	H	E	R
	8	33	33	48	~~73~~	28	18	48	83	43	28	93
mod 26	8	7	7	22	21	2	18	22	5	17	2	15
	I	H	H	W	V	C	S	W	F	R	C	P

for Inverse

$$P = A^{-1}(C-B) \bmod 26$$

use $AA^{-1} = 1 \bmod 26$

means A multiplied with some value (A^{-1}) which gives rem 1 when modulo by 26.

for Inverse

$5A^{-1} = 1 \bmod 26$

use Hit & Trial find no. which gave 1 remainder on (mod 26)

27 → 5×?
53 → 5×?
79 → 5×?
105 → 5×21

$A^{-1} = 21$

EULER TOTIENT FUNCTION (ϕ)

$\phi(P) = (P-1)$

↓ ϕ funct^n of a prime no. $P = (P-1)$

Note:- (1) If you want to find ϕ for a non-prime no. then you have to break that value into prime no.

Let $\phi(6) = \phi(3) \times \phi(2)$
$(3-1) \times (2-1)$
$2 \times 1 \Rightarrow 2$

Euler totient tells that their are such number of coprime no below that number.

Eg for eg $\phi(6) = 2$ (Euler Totient)
1 ↔ 5

Eg $\phi(8) = \phi(2) \times \phi(2) \times \phi(2)$
not correct because all $\phi(-)$ prime values must be different

Scanned with CamScanner

So, we can write.

$\phi(2^3) = (2)^3 - (2)^2$

$\Rightarrow 8 - 4 = 4$

Conditions

① $\phi(p) = p-1$

② $\phi(p) = \phi(m) \times \phi(n)$ (m & n = prime)

$\Rightarrow (m-1) \times (n-1)$

③ $\phi(p^n) = p^n - p^{n-1}$

Eg $\phi(120)$ → $2\times2\times2\times3\times5$

$= \phi(2^3) \times \phi(3) \times \phi(5)$

$4 \times 2 \times 4$

$\Rightarrow 32$ Ans

Generalize formula for A^{-1}

$AA^{-1} = 1 \bmod 26$

↓

can be written as :-

$\Rightarrow \boxed{5^{-1} \bmod (26)}$

$\Rightarrow \boxed{5^{\phi(26)-1} \bmod 26}$

$\Rightarrow 5^{12-1} \bmod 26$

$\Rightarrow 5^{11} \bmod 26$

Another approach

$5 \bmod 26 = 5$

$5^2 \bmod 26 = 25$

$5^4 \bmod 26 = (5^2 \bmod 26 \cdot 5^2 \bmod 26) \bmod 26$

$\Rightarrow 625 \bmod 26$

$\Rightarrow 1$

$5^{11} \bmod 26 = ((5^4 \bmod 26)(5^4 \bmod 26)(5^2 \bmod 26)(5 \bmod 26)) \bmod 26$

$\Rightarrow (1 \cdot 1 \cdot 25 \cdot 5) \bmod 26$

$\Rightarrow (125) \bmod 26$

$\Rightarrow 21$

Here with Euler totient also

$\boxed{A^{-1} = 21}$

now Decryption using A^{-1}.

for I $P = 21(8-8) = 0 = A$

for H $P = 21(87-8) = -21$

$-21 \bmod 26 \Rightarrow 26 - 21 \bmod 26$

$26 - 21 \Rightarrow 5$

$\boxed{-A \bmod m = m - A \bmod m}$ f

for W : $P = 21(22-8) \bmod 26 \Rightarrow 21(14) \bmod 26$

$294 \bmod 26$

$\Rightarrow 8$ (I)

for C : $21(2-8) \bmod 26$

$21(-6) \bmod 26$

$-126 \bmod 26 \Rightarrow 26 - 126 \bmod 26$

Scanned with CamScanner

$26 - 22 \Rightarrow 4 \Rightarrow$ (E)

9/Aug '18

Ques $CT = VWZMSCXX$

$K = \begin{matrix} 9 & 2 \\ A & B \end{matrix}$

Sol^n $P = A^{-1}(C-B) \bmod 26$

$9^{-1}(C-2) \bmod 26$

$9^{-1} \bmod 26$

$9^{\phi(26)-1} \Rightarrow 9^{12-1} \bmod 26 = 9^{11} \bmod 26$

$9 \bmod 26 = 9$

$9^2 \bmod 26 = 3$

$9^4 \bmod 26 = 9$

$9^8 \bmod 26 = 3$

$9^{11} \bmod 26$

$(9^8 \bmod 26 \cdot 9^2 \bmod 26 \cdot 9 \bmod 26) \bmod 26$

$(3 \cdot 3 \cdot 9) \bmod 26$

$81 \bmod 26$

$\Rightarrow 3$

for V $P = 3(21-2) \bmod 26$

$\Rightarrow 57 \bmod 26 \Rightarrow 5^{th} = F$

for W $P = 3(22-2) \bmod 26$

$\Rightarrow (3 \times 20) \bmod 26$

$\Rightarrow 8^{th} = I$

for Z $P = 3(25-2) \bmod 26$

$\Rightarrow (23 \times 3) \bmod 26$

$\Rightarrow 17 \Rightarrow R$

Similarly for all.

FIREWALL

HILL CIPHER

PT, K condition with key is that it will be in the form of square matrix. NXN

No. of blocks of plaintext is NX1

similarly cipher text is also NX1

$CT = KP \bmod 26$

Ex $(NXN)(NX1) = (NX1)$

$$\begin{bmatrix} C_1 \\ C_2 \\ C_3 \end{bmatrix} = \begin{bmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \\ P_3 \end{bmatrix} \bmod 26.$$

Qu $K = \begin{bmatrix} 2 & 3 \\ 7 & 8 \end{bmatrix}$

PT = NO ANSWER

PT_1 PT_2 PT_3 PT_4

Block cipher coz we are dividing into blocks

2 X 2 $\Rightarrow$ 2 Blocks of 2

Scanned with CamScanner

polyAlphabetic :- for a single alphabet cipher is always different

MonoAlphabetic :- for a alphabet cipher is always same

$$C_T = \begin{bmatrix} 2 & 3 \\ 7 & 8 \end{bmatrix} \begin{bmatrix} 13 \\ 14 \end{bmatrix} \bmod 26$$

$$\Rightarrow \begin{bmatrix} 2\times13 + 3\times14 \\ 7\times13 + 8\times14 \end{bmatrix} \bmod 26$$

$$\Rightarrow \begin{bmatrix} 26 + 42 \\ 91 + 112 \end{bmatrix} \bmod 26$$

$$\Rightarrow \begin{bmatrix} 68 \\ 203 \end{bmatrix} \bmod 26$$

$$\Rightarrow \begin{bmatrix} 16 \\ 21 \end{bmatrix} \Rightarrow \begin{bmatrix} Q \\ V \end{bmatrix}$$

for AN $C_T = \begin{bmatrix} 2 & 3 \\ 7 & 8 \end{bmatrix} \begin{bmatrix} 0 \\ 13 \end{bmatrix} \bmod 26$

$$\Rightarrow \begin{bmatrix} 2\times0 + 3\times13 \\ 7\times0 + 8\times13 \end{bmatrix} \bmod 26$$

$$\Rightarrow \begin{bmatrix} 39 \\ 104 \end{bmatrix} \bmod 26$$

$$\Rightarrow \begin{bmatrix} 13 \\ 0 \end{bmatrix} \Rightarrow \begin{matrix} N \\ A \end{matrix}$$

for SU $\begin{bmatrix} 2 & 3 \\ 7 & 8 \end{bmatrix} \begin{bmatrix} 18 \\ 22 \end{bmatrix} \bmod 26$

$$\begin{bmatrix} 2\times18 + 3\times22 \\ 7\times18 + 8\times22 \end{bmatrix} \bmod 26$$

$$\Rightarrow \begin{bmatrix} 36 + 66 \\ 126 + 176 \end{bmatrix} \bmod 26$$

$$\begin{bmatrix} 102 \\ 302 \end{bmatrix} \bmod 26$$

$$\begin{bmatrix} 24 \\ 16 \end{bmatrix} \Rightarrow \begin{bmatrix} Y \\ P \end{bmatrix}$$

for ER $\begin{bmatrix} 2 & 3 \\ 7 & 8 \end{bmatrix} \begin{bmatrix} 4 \\ 17 \end{bmatrix} \bmod 26$

$$\begin{bmatrix} 2\times4 + 3\times17 \\ 7\times4 + 8\times17 \end{bmatrix} \bmod 26$$

$$\begin{bmatrix} 8 + 51 \\ 28 + 136 \end{bmatrix} \bmod 26$$

$$\begin{bmatrix} 59 \\ 164 \end{bmatrix} \bmod 26$$

$$\begin{bmatrix} 7 \\ 8 \end{bmatrix} \Rightarrow \begin{matrix} H \\ I \end{matrix}$$

PT → NO ANSWER

CT → QV NAYQHI

From cipher text to plain text

Que $P = K^{-1}[C] \bmod 26$

$$P = \begin{bmatrix} 2 & 3 \\ 6 & 7 \end{bmatrix}^{-1} \begin{bmatrix} Q \\ V \end{bmatrix} \bmod 26$$

find Inverse of the Matrix. $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

$$A = \frac{Adj\,A}{mod\,A} \qquad \boxed{A^{-1} = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}}$$

$$\begin{bmatrix} 2 & 3 \\ 6 & 7 \end{bmatrix} = \frac{1}{14-18}\begin{bmatrix} 7 & -3 \\ -6 & 2 \end{bmatrix}$$

$$\left\{\frac{1}{-4}\right\} \times \begin{bmatrix} 7 & -3 \\ -6 & 2 \end{bmatrix} \bmod 26$$

Scanned with CamScanner

Note:- No value should be negative.
& no value to be greater than 26.

13 Aug '18

Ques Calculate Hill Cipher.

$$K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}_{3\times3}$$

PT = PAY MORE MONEY.

$$CT_1 = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} P \\ A \\ Y \end{bmatrix}$$

$$\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} 15 \\ 0 \\ 24 \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} 255+0+120 \\ 315+0+504 \\ 30+0+456 \end{bmatrix} \Rightarrow \begin{bmatrix} 375 \\ 819 \\ 486 \end{bmatrix} \text{ mod } 26$$

486
468
18

$$\begin{bmatrix} 11 \\ 13 \\ 18 \end{bmatrix} \Rightarrow \begin{bmatrix} L \\ N \\ S \end{bmatrix}$$

$$CT_4 = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} M \\ E \\ Y \end{bmatrix} \Rightarrow \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} 13 \\ 4 \\ 24 \end{bmatrix}$$

$$\begin{bmatrix} 17\times13 + 17\times4 + 5\times24 \\ 21\times13 + 18\times4 + 21\times24 \\ 2\times13 + 2\times4 + 19\times24 \end{bmatrix}$$

$$\begin{bmatrix} 221+68+120 \\ 273+72+504 \\ 26+8+456 \end{bmatrix} \begin{bmatrix} 51+68+120 \\ 63+72+504 \\ 26+8+456 \end{bmatrix} \Rightarrow \begin{bmatrix} 239 \\ 639 \\ 490 \end{bmatrix} \text{ mod } 26$$

$$\begin{bmatrix} 409 \\ 849 \\ 490 \end{bmatrix} \text{ mod } 26 \begin{bmatrix} 5 \\ 15 \\ 22 \end{bmatrix} \Rightarrow \begin{bmatrix} 19 \\ 17 \\ 22 \end{bmatrix} = \begin{bmatrix} T \\ R \\ W \end{bmatrix}$$

$$CT_2 = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} 12 \\ 14 \\ 17 \end{bmatrix} = \begin{bmatrix} \quad \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} H \\ P \\ L \end{bmatrix}$$

$$CT_3 = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} 4 \\ 12 \\ 14 \end{bmatrix} = \begin{bmatrix} \quad \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} E \\ W \\ M \end{bmatrix}$$

$$K^{-1} = \frac{1}{|K|} \times \text{adj } K$$

$$|K| = 17[(18\times19 - 21\times2) - 17(21\times19 - 21\times2) + 5(21\times2 - 18\times2)$$

$$17(342-42) - 17(399-42) + 5(42-36)$$

Scanned with CamScanner

$$\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

$$17(300) - 17(357) + 5(6)$$
$$5100 - 6069 + 30$$
$$-939$$

Cofactor Matrix

$$K^c = \begin{bmatrix} + & - & + \\ - & + & - \\ + & - & + \end{bmatrix} \begin{bmatrix} (18\times19-21\times2) & (21\times19-21\times2) & (21\times2-10\times2) \\ \downarrow & & \end{bmatrix}$$

$$K^c = \begin{bmatrix} (18\times19-21\times2) & (21\times19-21\times2) & (21\times2-10\times2) \\ (17\times19-5\times2) & (17\times19-5\times2) & (17\times2-17\times2) \\ (17\times21-5\times18) & (17\times21-5\times21) & (17\times18-17\times21) \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} 300 & -357 & 6 \\ -313 & 313 & 0 \\ 267 & -252 & -51 \end{bmatrix}$$

Transpose

$$adj(K) = (K^c)^T = \begin{bmatrix} 300 & -313 & 267 \\ -357 & 313 & -252 \\ 6 & 0 & -51 \end{bmatrix}$$

$$K^{-1} = \frac{-1}{939} \begin{bmatrix} 300 & -313 & 267 \\ -357 & 313 & -252 \\ 6 & 0 & -51 \end{bmatrix}$$

$$K^{-1} = \frac{-1}{3} \begin{bmatrix} & & \\ & & \\ & & \end{bmatrix}$$

$$K^{-1} = 3^{-1} \bmod 26 \begin{bmatrix} & & \\ & & \\ & & \end{bmatrix} = -9 \begin{bmatrix} & & \\ & & \\ & & \end{bmatrix}$$

Note: negative, fractional & values greater than 26 are not allowed, take mod 26 until the value is ded to

VIGENERE CIPHER

PT = X Y Z A W X Y P W M
Key = D I T U D I T U D I

$$CT = (PT + K) \bmod 26$$
$$\rightarrow CT_1 = (X + D) \bmod 26 = (23 + 3) \bmod 26$$
$$\Rightarrow 0 = A$$

$$PT_1 = (CT_1 - K_1) \bmod 26$$

Note:- This is a polyalphabetic cipher i.e. 2 cipher values for one Alphabet.

VIGENERE SQUARE

Key \ PT →	A	B	C	D	E	-	-	-	-	-	Z
B											
C											
D											
⋮											
Z											

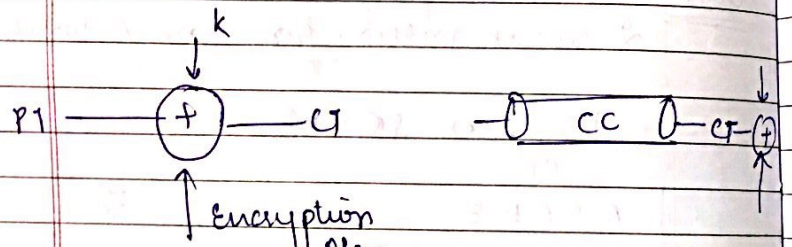
Scanned with CamScanner

→ $CT_2 = (4+I) \bmod 26$
⇒ $(24+8) \bmod 26$
⇒ $32 \bmod 26$
⇒ 6 ⇒ (G)

→ $CT_3 = (X+7) \bmod 26 = (S)$
$CT_4 = (A+U) \bmod 26 = (U)$
$CT_5 = (W+D) \bmod 26 = (Z)$
$CT_6 = (X+I) \bmod 26 = (F)$
$CT_7 = (4+7) \bmod 26 = (R)$
$CT_8 = (P+U) \bmod 26 = (J)$
$CT_9 = (W+D) \bmod 26 = (Z)$
$CT_{10} = (M+I) \bmod 26 = (U)$

VERNAM CIPHER

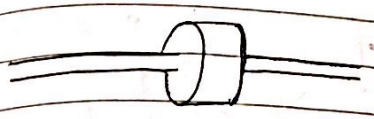
PT, K, CT Random key Generator ⇒



16/Aug'18

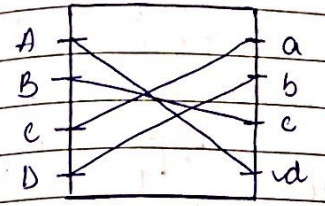
polyalphabetic

ROTOR CIPHER or ENIGMA M/C CIPHER



can move round

6 wires cannot move

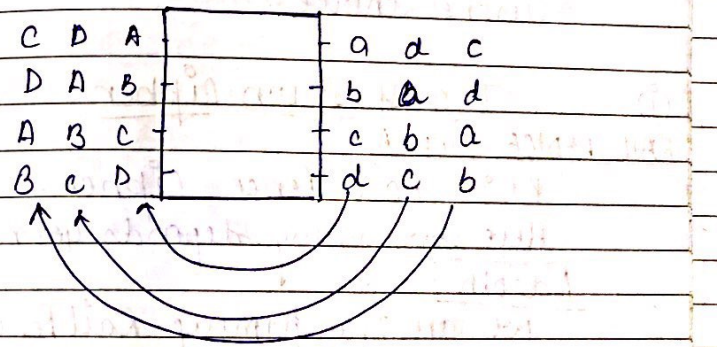


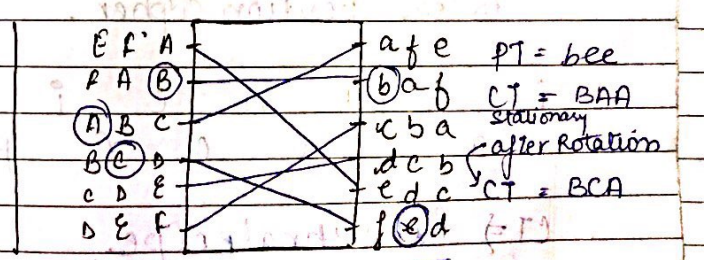
vABC = CDB.

simple connection.

How to generate key?

Assumption :- Rotor moves only one place at a time.



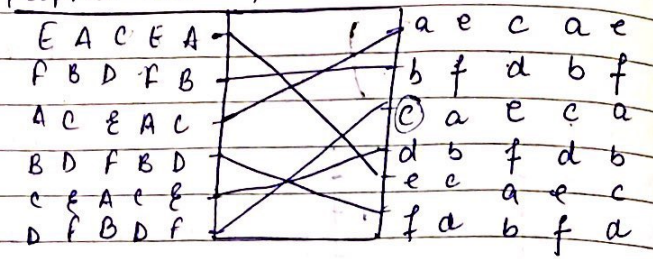


Scanned with CamScanner

PT = FEDCA

Plain Text

Cipher text



Left Right

On Rotation CT ⇒ ccdae (PT → CT)

2 times

Left Right

for CT → PT

DADFD

Note:- Here Rotation depends upon the user's choice.

(i) Transposition Cipher

RAIL FENCE CIPHER

PT:- Rail fence cipher.

Here everything depends upon the depth

we are transforming Rail fence Cipher to transposition cipher.

R i f n e i h n
a l e c C p e

CT ⇒ RifneihralecCpe

Transp.

(RFC) (CC)

(WK) (without key)

All are STREAM CIPHER

(ii) • Columnar Cipher (key not given)

Here no. of column are provided

↓ ↓ ↓ ↓ Here we read column wise I II III & so on

T R A N

S P O S

I T I O

N C I P

H E R Z filler

⇒ CT ⇒ TSINHRPTCEA OIIRNSOPZ

• (with key)

Column no is not given but key is given.

entries always b/w (1 - 9)

prev. example

PT:- TRANSPOSITION CIPHER

key given (1324)

4 values so divide the text into 4 column

1	3	2	4
T	R	A	N
S	P	O	S
I	T	I	O
N	C	I	P
H	E	R	Z

CT:- TSINHAOIIRRPTCENSOPZ

1 2 3 4

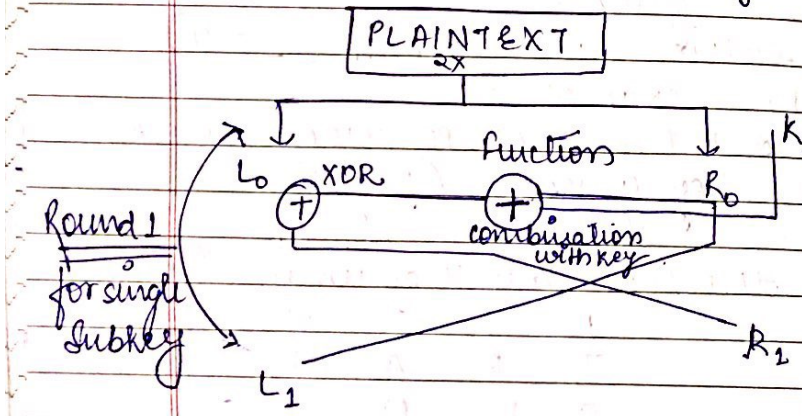
(Modern block cipher) - all used ↓ N/w

FIESTAL NETWORK (STRUCTURE).

The way you did encryption will be exactly same i.e used for decryption

same: PT ↓ CT — same: for PT → CT we use K ⇒ $K_1 K_2 K_3 K_4$
so for CT → PT we use K ⇒ $K_4 K_3 K_2 K_1$

key is divided into subkeys.
subkeys used for encryption is reversed & used for decryption.



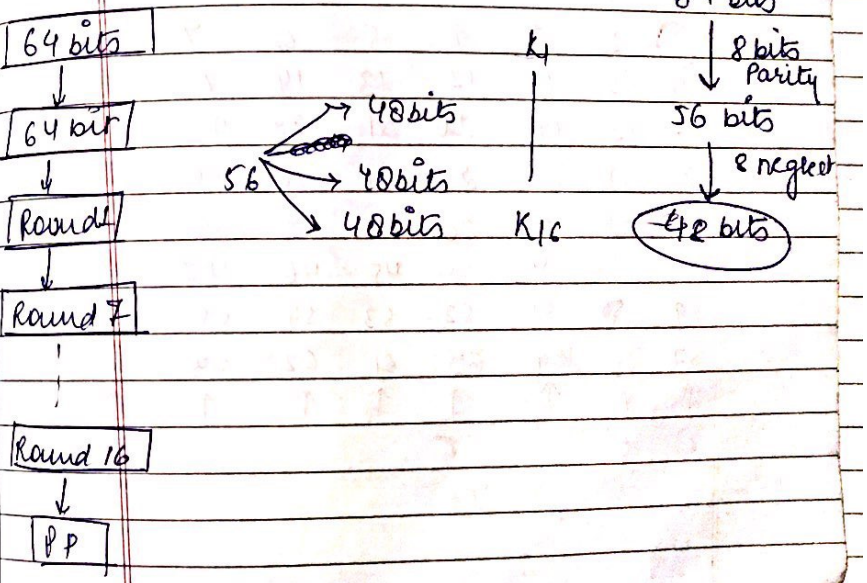
Generalise form

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus_{XOR} f(R_{i-1}, K_i)$$

elements / components
1. Block size ↑ complexity ↑ security ↑
2. n ↑ strong security ↑
3. Round key ↑ security ↑
4. No. of Rounds
5. Selection of Plain Text
6. Selection of Random key generator
7. sub key

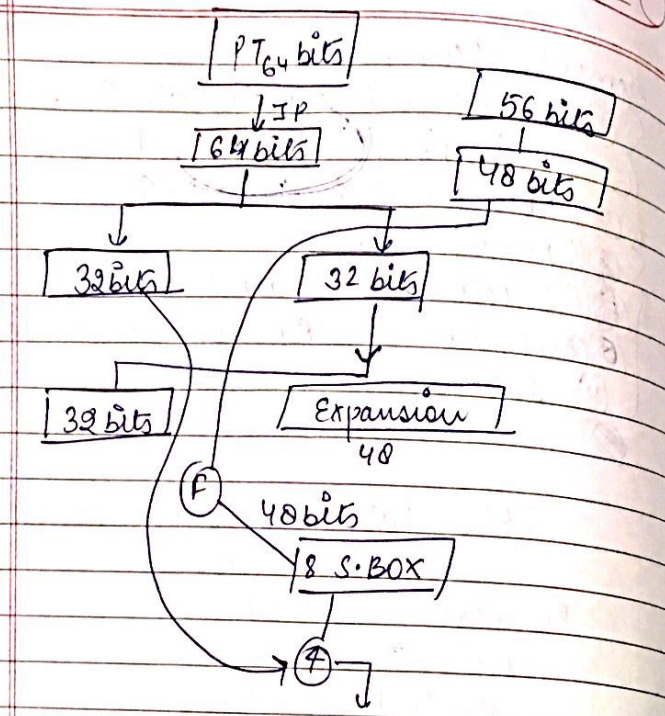
DES (Data Encryption standard)

Plaintext → 64 bits
Key → 64 bits
Cipher Text → 64 bits
No. of Rounds → 16



Scanned with CamScanner

Scanned with CamScanner



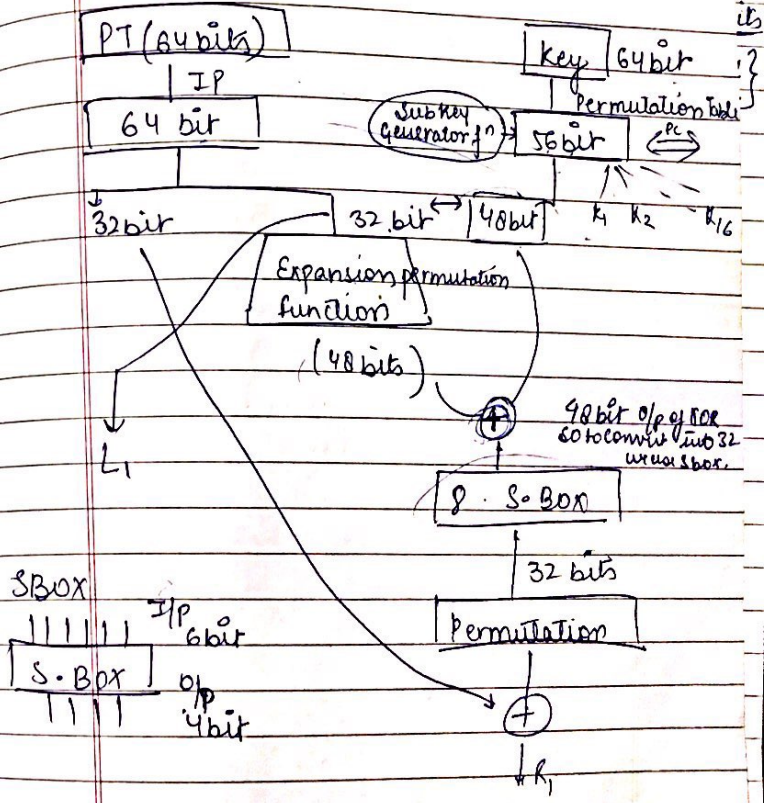
PT → 1,0

Plaintext

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64
↑	↑	↑	↑	↑	↑	↑	↑
0	E	0	E				

⇒ IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	30	30	22	14	6
64	56	48	40	32	24	16	8
57	-	-	-	-	17	9	1
59					19	11	3
61					21	13	5
63					23	15	7



Qw Explain DES structure

Qw SBOX - i/p given state o/p and its role

Qw Write PI initial permutation

Qw 64 bits - 48 bit conversion

21st Aug'18

DES (Block cipher algorithm)

i/p: 64 bits → 56 bits = K+

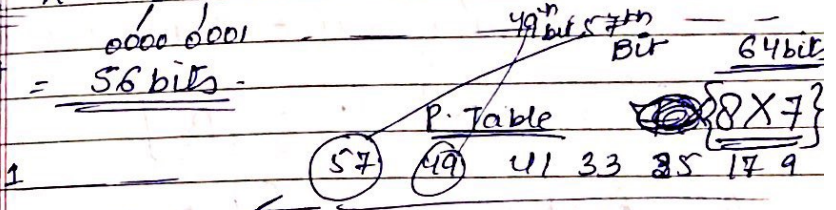
generally every 8th bit is discarded we need to arrange bits according to the permutation table.

64 bits K = 0 1 2 3 4 5 6 7 8 9 A B C D E F

0000 0001 ...

K+ = 56 bits.

0 1 ...



56 bits

K_1 K_2 - - - K_{16}

$K_1 - K_{16}$

1, 2, 9, 16 — 1 Bit. Shift

K+ = 56 bits

C_0 28 bits D_0 28 bits

C_0 = 1010 1 - - - - 1010

D_0 = 1011 1 1 - - - 0010

C_1 = 0101 0 - - - - 0101 } K_1

C_2 = 0111 1 - - - - 00101 } K_2

:

K_{16}

Like PI we have another PI for 56 → 48

Summary

① Key → 64 bits
② PTable → 8×7 table
& acc to table arrange position.
③ K^+ : 56 bits
C_0 28 bits, D_0 28 bits.
④ Left circular shift
for {1,2,9,16} → 1 bit L.C. shift.
for rest of all → 2 bit L.C. shift.
⑤ $K_1 \Rightarrow C_1 D_1$ | $K_2 = C_2 D_2$ ----
⑥ Another table will be there to convert 56 bit ⟶ 48 bits.
for all numbers b/w $K_1 \rightarrow K_{16}$
So all will be converted into
$K_1^+ \longrightarrow K_{16}^+$ (48 bits)

after making these sub keys they will be XOR with expanded Data and X will be created.

X = 10.1010.0 10111- ---- 10

48 bits

6 bit 6 bit . . . 8 S boxes will be formed

which will take 6 bit as I/p & give 4 bit as O/p.

now suppose we have a S box bit-
010101

0000 0001 0010 - - - 1010 1011 - - 1111

00
01
10
11

(X) (X1)

take the first & last bit out of the key 010101 S_1

01 go to 01 Row

Here at (X) position we find a 4 bit no. that no. will be a O/p for 6 bit

$S_2 \Rightarrow$ 010111

01 (X1) O/p

Note { This complete is just 1 Round like this 16 Rounds will takes place }

for even a lil change in PT, alot of change occurs in CT.
Known as
AVLANCHE Effect

Scanned with CamScanner

classmate
Date
Page

IP

0 1	0000 0001
2 3	0010 0011
4 5	0100 0101
6 7	0110 0111
8 9	1000 1001
A B	1110 1111
C D	1000 1001
E F	1110 1111
	E O E O E O E O

PT

1 0 1 0 1 1 0 0	odd
0 0 0 0 0 0 0 0	
1 0 1 0 1 1 0 0	
1 1 1 1 1 1 1 1	
1 1 1 1 0 0 0 0	even
1 0 1 0 1 0 1 0	
1 1 1 1 0 0 0 0	
1 0 1 0 1 0 1 0	

11x0
0 / 1

classmate
Date
Page

27/08/18

AES

Double DES — K1, K2 EKL [EK, (P)]

Triple DES — K1, K2 → EKD [DK_L {EK (P)}]

Ser of Residue	DES	AES
Block size	64	128
No. of Round	16	10, 12, 14
Key size	64	128, 192, 2
Total sub key	16	No of Rou 1

$Z_n \{0, 1, 2 \cdots n-1\}$

$Z_3 = \{0, 1, 2\}$

a and b are said to be additive inverse if $a+b = 0 \bmod n$

multiplicative inverse if

$a \times b = 1 \bmod n$

Qu $ZT = \{0, 1, 2, 3, 4, 5, 6\}$

Scanned with CamScanner

$n = 10$

$Z_n = \{0,1,2,3,4,5,6,7,8,9\}$ classmate — can be only one of these values

Extended Euclidean Algorithm to find multiplicative inverse

b under Z_n

3 Z_{10}

q	r_1	r_2	r	t_1	t_2	t
3	10	3	1	0	1	-3
3	3	1	0	1	-3	10
	1	0		-3	10	

$-3 \bmod 10$ (Z ki associated value)

$0 = 10 - 3 \bmod 10$

$= 10 - 3$

$= 7$

Algo

```
r1 ← n
r2 ← b
t1 ← 0
t2 ← 1
while (r2 > 0)
{
  q ← r1/r2
  r ← r1 - q r2
  t ← t1 - q t2
  r1 ← r2
  r2 ← r
  t1 ← t2
  t2 ← t
}
```

Qw b under Z_n

23 Z_{100} — 23 in $Z_{100} \Rightarrow 23^{-1} \bmod 100$

q	r_1	r_2	r	t_1	t_2	t
4	100	23	8	0	1	-4
2	23	8	7	1	-4	9
1	8	7	1	-4	9	-13
7	7	1	0	9	-13	100

$r = 100 - 92 = 8$

$q = (1$

1 0

$-13 \equiv 100$

$-13 \bmod 100$

$Z_n \rightarrow$ additive inverse $(a+b) = 0 \bmod n$ → find all pairs of a & b → {3,7}, {2,8}, {5,5}, {4,1} ... soon

multiplicative inverse $(a*b) = 1 \bmod n$ ⇒ {3×7}

$-13 \bmod 100 = 87$

Qw 23 under Z_{100}

⇒ $23^{-1} \bmod 100$

⇒ $23^{\phi(100)-1} \bmod 100$

⇒ $\phi(100)$

$\phi(2 \times 2 \times 5 \times 5)$

$\phi(2^2) \times \phi(5^2)$

$2^2 - 2^1 \times 5^2 - 5^1$

2×20

40

$23^{39} \bmod 100$

$23 \bmod 100 = 23$

$23^2 \bmod 100 = (23 \times 23) \bmod 100$

$= 529 \bmod 100$

$= 29$

$23^4 \bmod 100 = 29 \times 29 \bmod 100$

$= 841 \bmod 100$

$= 41$

$23^8 \bmod 100 = (41 \times 41) \bmod 100$

$= 81$

$23^{16} \bmod 100 = (81 \times 81) \bmod 100$

$= 61$

Scanned with CamScanner

$(23^{16} \cdot 23^{16} \cdot 23^{4} \cdot 23^{2} \cdot 23)$

$\{ 1356^{170} \bmod 171 \rightarrow (1) \}$ ←

Extended Euclidean Algorithm

Multiplicative Inverse of 11 in @26

q	r_1	r_2	r	t_1	t_2	t
2	26	11	4	0	1	-2
2	11	4	3	1	-2	5
1	4	3	1	-2	5	-7
3	3	1	0	5	-7	26
		0		-7	26	

→ $-7 \bmod 26$

→ $26 - 7 \bmod 26$

→ $26 - 7 = 19$

Fermat's Theorem

If p is a prime no. & a is the +ve integer, condition a is not divisible through p. (i.e p is not divisible by a)

$$\boxed{a^{p-1} = 1 \bmod p}$$

$$a^{p-1} = 1 \bmod p$$

or

$$a^{p-2} \cdot a^{-1} \bmod p$$

$$\boxed{a^{p} \cdot a \bmod p} \rightarrow a^{p} \bmod p = a \bmod p$$

Scanned with CamScanner

Q $6^{10} \bmod 11$

$6^{11-1} \bmod 11 = 1 \bmod 11 = 1$

Q $3^{12} \bmod 11$

$(3 \bmod 11 \cdot 3^{11} \bmod 11) \bmod 11$

$(3 \bmod 11 \cdot 3 \bmod 11 \cdot 3^{10} \bmod 11) \bmod 11$

$\Rightarrow 9$

Q $5^{15} \bmod \bmod 13$

$(5 \bmod 13 \cdot 5^{14} \bmod 13) \bmod 13$

$(5 \bmod 13 \cdot 5 \bmod 13 \cdot 5^{13} \bmod 13) \bmod 13$

$(5^2 \bmod 13 \; 5^{13} \bmod 13) \bmod 13$

8.

Q $456^{17} \bmod 17$

$(456 \bmod 17 \; 456^{16} \bmod 17) \bmod 17$

14.

Q $7^{16} \bmod 17$

$7^{17-1} \bmod 17 = 1 \bmod 17$

$= 1.$

Euler's Theorem

If n and a are positive integer then according to Euler theorem

$$a^{\phi(n)} = 1 \bmod n$$

$$a^{\phi(n)+1} = a \bmod n \quad (*a)$$

$$a^{\phi(n)-1} = a^{-1} \bmod n \quad (*a^{-1})$$

Q $6^{24} \bmod 35$

Note Fermat theorem is not applicable because 35 is not a prime number

$\phi(35) = \phi(7) \times \phi(5)$

$(7-1) \times (5-1)$

$6 \times 4 = 24$

$6^{\phi(35)} \bmod 35 = 1 \bmod 35 = 1$

Q $20^{62} \bmod 77$

$\phi(77) = \phi(11) * \phi(7)$

$(11-1) * (7-1)$

$10 * 6 = 60$

$20^{60} \bmod 77 \cdot 20^2 \bmod 77$

$20^{\phi(77)} \bmod 77 \cdot 20^2 \bmod 77$

$400 \bmod 77 = 15$ ans

Q' $7^{222} \bmod 10$

$\phi(10) = \phi(5) \times \phi(2) \Rightarrow 4 \times 1 \Rightarrow 4$

$7^4 \bmod 10 = 1$

$(7^4 \bmod 10)^{55} \cdot 7^2 \bmod 10 \bmod 10$

$(49 \bmod 10) \bmod 10$

$= 9$ Ans

Scanned with CamScanner

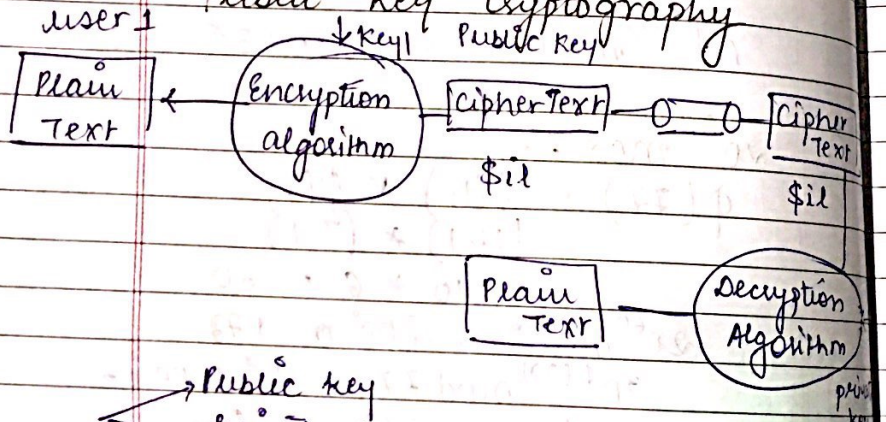
Assignment

Q1 What are different security services, security mechanism to counter various types of cryptographic attacks

Q2 Categories different types of model of operations of block ciphers.

Q3 Different b/w (i) Cryptography & Steganography
(ii) Confusion & diffusion
(iii) Stream & block cipher

Public key Cryptography



Public key
Private key

- authentication
- authorization
- confidentiality
- Integrity

Chinese Remainder Theorem

$x = x \equiv a_1 \bmod m_1 \quad —①$
$x \equiv a_2 \bmod m_2 \quad —②$
$x \equiv a_3 \bmod m_3 \quad —③$

$M = m_1 \times m_2 \times m_3$

$M_1 = \frac{M}{m_1}, \quad M_2 = \frac{M}{m_2}, \quad M_3 = \frac{M}{m_3}$

$M_1^{-1}, \quad M_2^{-1}, \quad M_3^{-1}$

$x = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1} + a_3 \times M_3 \times M_3^{-1}) \bmod M$

Qu $x = 2 \bmod 3$
$x = 3 \bmod 5$
$x = 2 \bmod 7$

3&5, 5&7, 7&5 → coprime. Hence we can solve using CRT

$M = 3 \times 5 \times 7 = 105$

$M_1 = \frac{105}{3} = 35$

$M_2 = \frac{105}{5} = 21$

$M_3 = \frac{105}{7} = 15$

$M_1^{-1} = 35^{-1} \bmod 3$
$= 35^{\phi(3)-1} \bmod 3$
$= 35^{1} \bmod 3$
$= 2$

Scanned with CamScanner

$M_1^{-1} = 21^{-1} \bmod 5$

$= 21^{\phi(5)-1} \bmod 5$

$= 21^3 \bmod 5$

$= 1$

$M_3^{-1} = 15^{-1} \bmod 7$

$= 15^{\phi(7)-1} \bmod 7$

$= 15^5 \bmod 7$

$= 759375 \bmod 7$

$=$

$x = (2 \times 35 \times 2 + 3 \times 1 \times 21 + 2 \times 15 \times 1) \bmod 105$

$\Rightarrow (140 + 63 + 30) \bmod 105$

$\Rightarrow 233 \bmod 105$

$\Rightarrow 23$

Qu GCD (12345, 11111)

GCD (1275, 50)

GCD (1237, 1947)

GCD (1275, 50) GCD (a, b) = GCD (b, a mod b)

(50, 25) GCD (b, 0) = b

25, 50 mod 25

(25) 0 GCD (1275, 50)

GCD (50, 25)

GCD (25, 0) = 25

Sender private Authentication

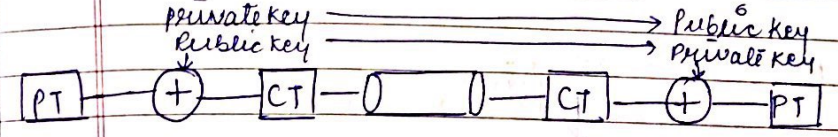
Sender public confidentiality

Public key cryptography

Key → Private

Key → Public

Chinese Reminder Theorem



→ If sender user private key then receiver have a corresponding public key for that which ensures Authentication. (user/sender confirmed)

→ If sender uses public key then receiver uses private key corresponding to that which ensures confidentiality.

CRTheorem

Qu $X = 4 \bmod 7$

$X = 5 \bmod 11$

$X = 7 \bmod 13$

$X = 12 \bmod 17$

use

$X_1 = a_1 \bmod m_1$

$X_2 = a_2 \bmod m_2$

$M = m_1 \times m_2$

$M_1 = \frac{M}{m_1}$, $M_2 = \frac{M}{m_2}$ find M_1^{-1} M_2^{-1}

Scanned with CamScanner

Sol:- $M = 7 \times 11 \times 13 \times 17 = 17017$

$M_1 = \frac{17017}{7} \Rightarrow 2431$ $\quad M_2 = \frac{17017}{11} = 1547$

$M_3 = \frac{17017}{13} = 1309$ $\quad M_4 = \frac{17017}{17} = 1001$

M_1^{-1} $\quad 2431^{-1} \bmod 7$

$(2431)^{\phi(7)-1} \bmod 7$

$7\overline{)2431}$ (347, 21, 33, 28, 51, 49, 2)

$(2431)^5 \bmod 7$

$\Rightarrow (2)^5 \bmod 7 \Rightarrow 32 \bmod 7$

$\Rightarrow 4.$

M_2^{-1} $\quad (1547)^{-1} \bmod 11$

$(1547)^9 \bmod 11$

$\Rightarrow 8$

M_3^{-1} $\quad 3$ Similarly

M_4^{-1} $\quad 4.$

find $\left[(a_1 \times M_1 \times M_1^{-1} + a_2 M_2 M_2^{-1}) \bmod M\right]$

$x = (4 \times 2431 \times 4 + 5 \times 1547 \times 8 + 7 \times 1309 \times 3 + 12 \times 1001 \times 4) \bmod 17017$

$\Rightarrow$ [redacted] $\quad 6143$

for verification

$x = 4 \bmod 7$ put $x = 15152$

$7\overline{)15152}$ (2165, 14, 11, 7, 45, 42, 32, 28, 4) Rem should be 4.

(4) verified

chinese Remainder applied only when mod value are coprime like here in Ques 7, 11, 13, 17 are coprime

RSA Algorithm (provide confidentiality)

Public key cryptography algorithm.

prime No:- p & q (distinct prime No.)

find a value (n) = multiple of p & q

($n = p \times q$) part of any public or private key

find $\phi(n) = (p-1)(q-1)$

To cal. public key (e).

GCD $(e, \phi(n)) = 1$

Scanned with CamScanner

To calculate Private key corr to that publickey

$d \cdot e = 1 \bmod \phi(n)$

Eg: p = 7, q = 11, (M)

$n = 77$

$\phi(n) = 60$

public key (can be any no. which is coprime to 60)

either 7, 11, 13, 17 - - (any no. Smaller than 60)

suppose we take 7

private $e = 7$

$d \cdot 7 = 1 \bmod 60$

∴

Cipher Text

$C = M^e \bmod n$ encrypted value

for verification

stability M &

(M) = $C^d \bmod n$

↳ must be similar.

Qu: p = 11 q = 13 M = 5

$n = 11 \times 13 \Rightarrow 143$

$\phi(n) = 10 \times 12 \Rightarrow 120$

public key GCD$(e, \phi(120)) = 1$

Let $e = 7$

private $d \cdot e = 1 \bmod 120$

$d \cdot 7 = 1 \bmod 120$

$d = 7^{-1} \bmod 120$

$7^{\phi(120)-1} \bmod 120$

$7^{31} \bmod 120$

$\Rightarrow 7 \bmod 120 = 7$

$7^2 \bmod 120 = 49$

$7^4 \bmod 120 \Rightarrow$

$(7^2 \bmod 120 \, 7^2 \bmod 120) \bmod 120$

$\Rightarrow (49 \times 49) \bmod 120$

$\Rightarrow 2401 \bmod 120$

$\Rightarrow 1$ continues.

$7^{-1} \bmod 120 \Rightarrow 103$ final

$d = 103$

$C = 5^7 \bmod 143 \Rightarrow 47$

120 → 60 2 → 30 2 → 15 × 2 → 5 5 × 2 → 3 × 5 × 2 × 2 × 2

$2^4 \times 3 \times 5 = 2^3$

120 / 2 = 2400

Scanned with CamScanner

CA → certificating Authority.

RSA algorithm
for 2 different parties:

	A	B
large prime no. →	p_A, q_A	p_B, q_B
	$n_A = p_A \times q_A$	$n_B = p_B \times q_B$
Euler totient	$\phi(n_A) = (p_A-1)(q_A-1)$	$\phi(n_B) = (p_B-1)(q_B-1)$
public key	(e_A)	(e_B)
	$1 < e_A < \phi(n_A)$	$1 < e_B < \phi(n_B)$
	CA	
private key	(d_A)	(d_B)
	$e_A \cdot d_A = 1 \bmod \phi(n_A)$	$e_B \cdot d_B = 1 \bmod \phi(n_B)$

public key of all are stored in CA.
If A want to contact B then it will ask for B's public key from CA (Certificate Authority)

A ⟷ B
sender Receiver

A → CA → B
e_B

$C = M^{e_B} \bmod n$ encrypted

$M = C^{d_B} \bmod n$ decrypted

Note: Sender take public key from CA & encrypt msg using that key then private key is used by rcvr receiver to decrypt the same msg.

Ques $p = 7 \quad q = 11 \quad m = 5$

$n = 77$

$\phi(n) = (7-1)(11-1) = 60$

$1 < e < \phi(n)$

$GCD(e, \phi(n)) = 1$

Suppose $e = 13$ public key.

$13 \cdot d = 1 \bmod \phi(n)$

$d = 13^{-1} \bmod 60$

$d = 13^{\phi(60)-1} \bmod 60$

use

q	r_1	r_2	r	t_1	t_2	t
4	60	13	8	0	1	-4
1	13	8	5	1	-4	5
1	8	5	3	-4	5	-9
1	5	3	2	5	-9	14
1	3	2	1	-9	14	-23
2	2	1	0	14	-23	60
	1	0			-23	60

$-23 \bmod 60$

$\Rightarrow 60 - 23 \bmod 60$

$\Rightarrow 60 - 23 = 37$

Scanned with CamScanner

private id = 37 same by euler totient also

message send to be = 5

cipher text = $M^e \bmod n$

$\Rightarrow 5^{13} \bmod 77$

$(5^2 \bmod 77)\ 5^{12} \bmod 77) \bmod 77$

48.

$(48 \cdot 48 \cdot 48 \cdot 48 \cdot 5) \bmod 77$

$(26 \cdot 5 \cdot 2080) \bmod 77$

26 C.T.

decryption

$M = C^d \bmod 77$

$26^{37} \bmod 77$

$(26^3 \bmod 77)$

$20^{11} \bmod 77$

$(20^5 \bmod 74)$

$(34 \cdot 20) \bmod 77$

$680 \bmod 77$

74

$(74 \times 26) \bmod 77$

76

$26^{37} \bmod 77$

$26 \bmod 77$

$\Rightarrow 26$

$(60)^{18} 26 \bmod 77$

$(58)^9 \cdot 26 \bmod 77$

$(53)^4 \cdot 58 \cdot 26 \bmod 77$

$(37)^2 \cdot 58 \cdot 26 \bmod 77$

$60 \cdot 45 \bmod 77$

$2700 \bmod 7$

$\Rightarrow 5$

Assgm

Ques find cipher text for "HELLO"

Scanned with CamScanner

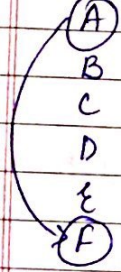
10/Sept/18.

Key Management

In this keys are known to authenticated parties only

Public key distribution
↳ shared secret key distribution

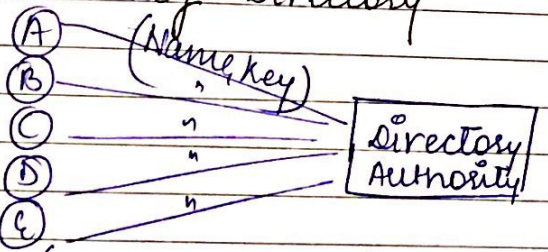
(i) Public announcement (broadcasting)
A have public key of all



A sends msg to F using public key of C so that F knows that msg comes from C (Authentication)

Drawback:- Public key visible to all.

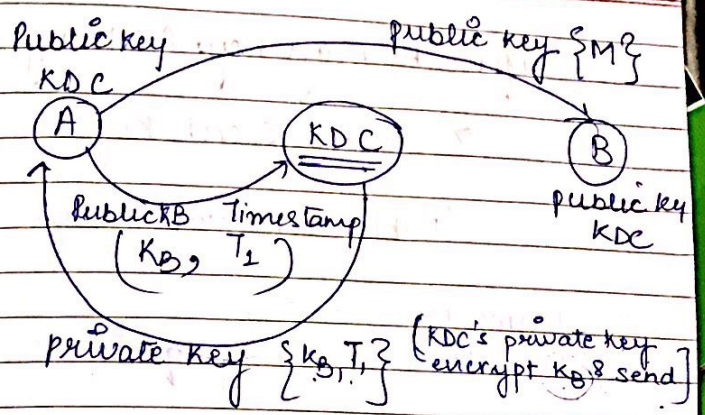
(ii) Public key directory



(Name, key) pair is available

Drawback:- same as above.

(iii) Key Distribution Centre



This private key will be decrypted by public key i.e. available to all. Then A got the public key of B so it will send a msg. that msg will be decrypted by B using its private key. (This same process is done for B as well to check the authentication).

(iv) Key certification

If this comm^n occurs b/w 2 parties again & again then KDC provide certificate to both i.e used for authentication & KDC is not disturbed again & again

→ When 2 parties don't want any third party to interfere so they create a shared key (public + private combination)

Scanned with CamScanner

Diffie Hellman key Exchange Algo.

↓

shared secret key

(Public + Private) key

→ Prime No ⟶ q

→ primitive root of q is α

→ Psirutive Root

Eg p prime no. α is its primitive root

$^{7}p \longrightarrow {}^{3}\alpha$

$\alpha^x \bmod p$

$x = 1$ to $p-1$

$\Rightarrow 1, 2, 3, 4, 5, 6.$

$\alpha^1 \bmod p$	$3^1 \bmod 7$	$= 3$
	$3^2 \bmod 7$	$= 2$
	$3^3 \bmod 7$	$= 6$
$\alpha^6 \bmod p$	$3^4 \bmod 7$	$= 4$
	$3^5 \bmod 7$	$= 5$
	$3^6 \bmod 7$	$= 1$

{ PR is a generator fn which generate distinct number. }

Both know
① Prime no.
② PR.
③ Private key.

	A	B	condition
private key	X_A	X_B	$\{X_A, X_B < q$
public key	$Y_A = (\alpha)^{X_A} \bmod q$	$Y_B = (\alpha)^{X_B} \bmod q$	

Exchange of keys.

Generate a shared key

$K_{shared} = (Y_B)^{X_A} \bmod q$ $\quad$ $K_{shared} = (Y_A)^{X_B} \bmod q$

Both the keys are equal
comm° will be authenticated

$K = (Y_B)^{X_A} \bmod q$

$K = (\alpha^{X_B})^{X_A} \bmod q$

$K = (\alpha^{X_A})^{X_B} \bmod q$

$K = (\alpha^{X_A} \bmod q)^{X_B} \bmod q$

$K = (Y_A)^{X_B} \bmod q$

If shared secret key then $K_B = K_A$ always#

13/sep/'18

Types of Questions :

prime $q = 23$ $\quad \alpha = 9$ (Primitive root)

$X_A = 4$ $\quad X_B = 3$

Q1 check whether α is a Generator or not
Q2 Calculate Public key for A & B
Q3 Calculate shared secret key for the user

Scanned with CamScanner

Ans 1 $9^1 \bmod 23$ ——
$9^2 \bmod 23$ ——
⋮ ——
$9^{22} \bmod 23$ ——
} all values must be different then gener.

Ans 2 $X_A = 4 \quad X_B = 3$

$Y_A = (\alpha)^{X_A} \bmod q$
$= (9)^4 \bmod 23$
$\Rightarrow 6$

$Y_B = (\alpha)^{X_B} \bmod q$
$\Rightarrow (9)^3 \bmod 23$
$\Rightarrow 16$

Ans 3 Shared secret key.

$K_A = (Y_B)^{X_A} \bmod q$
$\Rightarrow (16)^4 \bmod 23$
$(16)^2 \bmod 23 = 3$
$(16)^4 \bmod 23 \Rightarrow 3^2 \Rightarrow 9$

$K_B = (Y_A)^{X_B} \bmod q$
$\Rightarrow (6)^3 \bmod 23$
$\Rightarrow 9$

Both must be equal

Ans.

$Y_A = 40 \quad Y_B = 248$
$K = 160$

Q $q = 353 \quad , \alpha = 3$
$X_A = 97 \quad X_B = 233$
find shared secret key.

$Y_A = (3)^{97} \bmod 353$
$\Rightarrow (3^5 \bmod 353)^{19} \cdot 3 \bmod 353$
$= (243)^{19} \bmod 353 \cdot 3 \bmod 353$
$= (243^{19}) 3 \bmod 353$
$\Rightarrow 3 \cdot (243^{19}) \bmod 353$

$\Rightarrow 3^{97} \bmod 353$
$\Rightarrow (9)^{48} 3 \bmod 353$
$\Rightarrow (29)^{24} 3 \bmod 353$
$\Rightarrow (135)^{12} 3 \bmod 353$
$\Rightarrow (260)^6 3 \bmod 353$
$\Rightarrow (177)^3 3 \bmod 353$
$\Rightarrow (265)\,177\; 3 \bmod 353$
$\Rightarrow 140715 \bmod 353$
$Y_A \Rightarrow 40$

$Y_B = (3)^{233} \bmod 353$
$\Rightarrow (243)^{38} 3^5 \bmod 353$
$\Rightarrow (265)^9 \cdot (243)^2 \cdot 3^5 \bmod 353$
$\Rightarrow (331)^4 \cdot 265 \cdot 243^2 \cdot 3^5 \bmod 353$
$\Rightarrow (131)^2 \cdot 265 \cdot 243^2 \cdot 3^5 \bmod 353$
$\Rightarrow 217 \cdot 243^2 \cdot 149 \bmod 353$
$\Rightarrow 217 \cdot 102 \bmod 353$
$\Rightarrow 248$

Scanned with CamScanner

Elgamel cryptosystem

A (sender) | B (recipient)

B (recipient) → p → e_1 (primitive roots of p) → choose a private key d, $1 \le d < p-2$ → $e_2 = e_1^d \bmod p$

public key (e_1, e_2, p)

Message = M

Random no = r {same as cond as d} $1 < r < p-2$

$C_1 = e_1^r \bmod p$

$C_2 = (M \times e_2^r) \bmod p$.

$(C_1 C_2)$

Decrypted Text

$D = [C_2 (C_1^d)^{-1}] \bmod p$

$= M$ always

Qu p = 11 e1 = 2

primitive check

$2^1 \bmod 11 = 2$
$2^2 \bmod 11 = 4$
$2^3 \bmod 11 = 8$
$2^4 \bmod 11 = 5$
$2^5 \bmod 11 = 10$
$2^6 \bmod 11 = 9$
$2^7 \bmod 11 = 7$
$2^8 \bmod 11 = 3$
$2^9 \bmod 11 = 6$
$2^{10} \bmod 11 = 1$

all values are distinct so 2 is a primitive root of 11

Recipient end

Select a private key b/w 1 to 9
d = 3.

$e_2 = e_1^d \bmod p$
$= 2^3 \bmod 11$
$= 8$

public key for B to A (e_1, e_2, p)
$(2, 8, 11)$.

sender side

M = 7
r = 4 Suppose

$C_1 = 2^4 \bmod 11$
$= 5$

$C_2 = (7 \times 8^4) \bmod 11$
$= 8^2 \bmod 11$
$= 9.$
$= 81 \bmod 11$
4
$= 7 \times 4 \bmod 11$
$28 \bmod 11 = 6$

$(C_1 C_2) = (5, 6)$

Receiver end

$D = [C_2 (C_1^d)^{-1}] \bmod 11$

$= 6 (5^3)^{-1} \bmod 11$

$= 0 \bmod 11$

Scanned with CamScanner

$$\# \left[(c_1^d)^{-1} \bmod p = c_1^{p-1-d} \bmod p \right]$$

$5^{11-1-3} \bmod 11$

$\Rightarrow 5^7 \bmod 11$

$= 5^2 \bmod 11$

$= (5)^3 \, 5 \bmod 11$

$9 \cdot 3 \cdot 5 \bmod 11$

$\Rightarrow 3$

$e_2 \; 3 \bmod 1$

$6 \times 3 \bmod 11$

$\Rightarrow (7) = (M)$

Que $p = 107 \quad e_1 = 2 \quad M = 66$

let $d = 5 \qquad 1 < d < 105$

$e_2 = e_1^d \bmod p$

$\Rightarrow 2^5 \bmod 107$

$\Rightarrow 32$

$M = 66$

$r = 4$ suppose

$C_1 = e_1^r \bmod p$

$= 2^4 \bmod 107$

$\Rightarrow 16$

$C_2 = (M \times e_2^r) \bmod p$

$\Rightarrow (66 \times (32)^4) \bmod 107$

$\Rightarrow 1024 \bmod 107$

$(61)^2 \bmod 107$

$3721 \bmod 107$

$(66 \times 83) \bmod 107$

(11)

$(C_1, C_2) = (16, 11)$

$D = [C_2 (C_1^d)^{-1} \bmod p.$

$16^{107-1-5}$

$16^{101} \bmod 107$

$(42)^{50} \cdot 16 \bmod 107$

$(52)^{25} \, 16 \bmod 107$

$(29)^{12} \, 52 \cdot 16 \bmod 107$

$(92)^6 \, 52 \cdot 16 \bmod 107$

$(11)^3 \, 52 \cdot 16 \bmod 107$

$(11)^2 \, 11 \cdot 52 \cdot 16 \bmod 107$

$14 \cdot 11 \cdot 52 \cdot 16 \bmod 107$

$\Rightarrow$

$\Rightarrow 11 \cdot 49 \bmod 107$

$\Rightarrow 66$

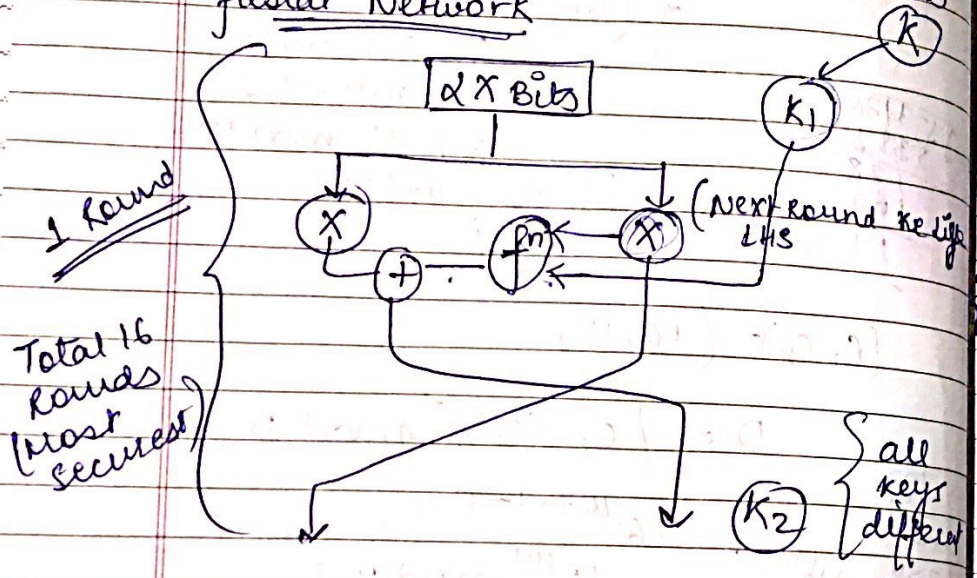
check.

Scanned with CamScanner

Revision

⊕ XHS bits = K_1 bits

Feistal Network



Qu Explain Feistal structure
Qu Key components
Qu significance of no.of rounds & fn.
Qu on which algorithm you can use this.

Note:- for Decryption we reverse the keys-

DES Question

Qu Explain structure.
Q Key specif.
Q To calc initial Perm
Q Role of S-Box
Q I/p to o/p from S Box
Q Generation of sub key from.

Key generation

56 bits

28 bits | 28 bits

use IC.S. in {1,2,9,16}

& for rest 2 bit CS- {3,4,5,6...}

L_1 = 10101 — — 1010
R_1 = 01010 — — 0101

Round 1
L_1^+ = 01010 — — 10101...
R_1^+ = 10101 — — 01010
$K_1 = L_1^+ + R_1^+$

Then

Round 2
L_2^+ = 10101 — — 101010
R_2^+ = 01010 — — 010101
$K_2 = L_2^+ + R_2^+$

; and so on for 16 rounds

for converting 64 → 56 (T_1 table) (different Table)
converting 56 → 64 (T_2 table)

Scanned with CamScanner

Sessional Paper

(1) Public key - Assymetric
Private key → Symmetric.

(2) $456^{17} \bmod (17)$ - prime
[$a^p \bmod p$]
So, $456 \bmod 17 \Rightarrow 14$ Ans

(3) for symmetric no of keys.
${}^{n}C_2$ or $\frac{n(n-1)}{2}$
for asymmetric no of keys
$2n$

(4) Relative prime
$\phi(6) = 2$ this value shows that there are 2 no. less than 6 which are coprime
(1, 5)

(5) $A^{-1} \bmod n$ ⇒ possible only when A & n are coprime
So in last Question Decryption key was not possible.

15/Oct'18

Message Authentication :-

Attacks on comm^n channel
- ↳ Traffic Analysis
- ↳ Masquereading
- ↳ Repudition
- ↳ Content Modification (attack is on Integrity)
- ↳ Source repudition.

destruction, Repudition

To check Message Authentication.
Sender is a valid user. (by checking that it is using private key of send).

Message Authen
- Message encryption using private key
  - use:- Digital signature
- MAC
  - Message Authentication code
  - code
  - One More Firm MDC
    - {Modification detection code}
    - ↓ provide Integrity.
- Hash Algo. (Variable length to fixed length)
  - Hash

Scanned with CamScanner

provide ability to
① verify author, date & time of signature.
② authenticate message content.
③ be verified by third parties to resolve disputes.

Digital signature (looked for msg authentication)

Reverse the initial crypto process
sender → private key } Authentication
receiver → public key } security

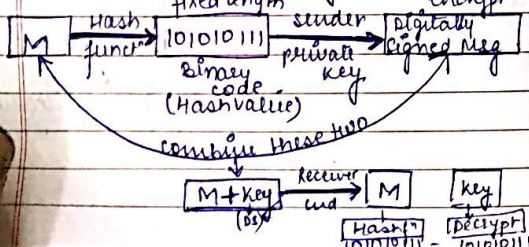
initial crypto process
sender → public key } confidentiality
receiver → private key

This is followed and called as digital signature

- Direct
- Arbitrated.

How to generate & use digital sign
① Generation
② Apply
③ Verification.

user have a msg [M]



Assumption :-
① Same Hash values.
② same methods must be used for encryption as well as decryption.

Direct Digital signature :-
Direct comm" b/w communication parties.
Elgamel & RSA both are applied in digital signature algo.

Eg $p = 17$ $q = 19$ $e = 7$ $M = 24$

$n = 17 \times 19$

$\phi(n) = 18 \times 16$.

private key ⇒ $d \cdot e = 1 \bmod \phi(n)$.

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

$\Rightarrow 7^{-1} \bmod (288)$

$\Rightarrow 7^{\phi(288)-1} \bmod (288)$

$\Rightarrow$

$\phi(2^5 \times 3)$

$\Rightarrow \phi(2^5) \times \phi(3^2)$

$\Rightarrow (2^6) - (2^5) =$

Ans $\Rightarrow$ 96.

2	288
2	144
2	72
2	36
2	18
3	9
3	3
	1

$2^5 \times 3^2$

64
32

$\Rightarrow 7^{95} \bmod 288$

$(49)^{35} \cdot 7 \bmod 288$

$(97)^7 \cdot 49 \cdot 7 \bmod 288$

$(193)^3 \cdot 97 \cdot 49 \cdot 7 \bmod 288$

$(97) \cdot 193 \cdot 97 \cdot 49 \cdot 7 \bmod 288$

private key ⇒ 151

Scanned with CamScanner

$7^{95} \bmod 288$.

$(49)^{17} \cdot 7 \bmod 288$

$(97)^{23} \cdot 49 \cdot 7 \bmod 288$

$(193)^{11} \cdot 97 \cdot 49 \cdot 7$

$(97)^{5} \cdot 193 \cdot 97 \cdot 49 \cdot 7$

$(193)^{2} \cdot 97 \cdot 193 \cdot 97 \cdot 49 \cdot 7$

$97 \cdot 97 \cdot 193 \cdot 97 \cdot 49 \cdot 7$

247

Q. $p = 7 \quad q = 13 \quad e = 5 \quad M = 35$

$n = 7 \times 13 = 91$

$\phi(n) \Rightarrow 6 \times 12$

$\Rightarrow 72$

$d \cdot e = 1 \bmod \phi(n)$

$d = 5^{-1} \bmod 72$

$d = 5^{\phi(72)-1} \bmod 72$

$\boxed{d = 29}$ — private key.

Sender $\Rightarrow 35^{(29)} \bmod 91$

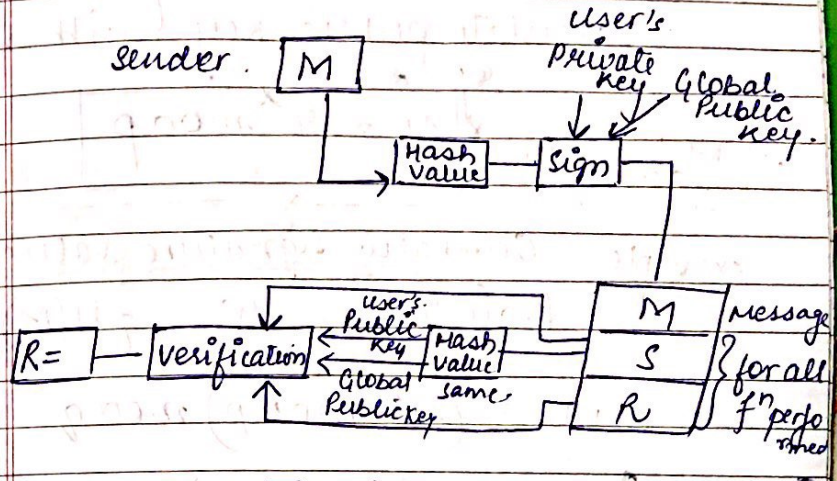
$\Rightarrow$

In Normal RSA we use public key but for DS RSA we use private key.

20978486O

16/10/18.

Digital signature Standard (DSS)



If after verification R = value after verified then we can say it is verified.

Algorithm

① Design

p = prime Number

we have to choose another prime No = q. {selection criteria $(P-1) \bmod q = 0$}

q must be divisible by $(p-1)$

Random value = h $\{1 < h < p-1\}$

calculate $x = h^{(P-1)/q} \bmod p$

↓

Help in cal. Private key.

p = PN
q = multiple of p-1
1 < h < p-1
$x = h^{(p-1)/q \bmod p}$ → private key
$0 < x < q$
$y = g^{x} \bmod p$
public key

signature $w = \frac{1}{msg}$
$0 < k < q$ gcd(k, q) = 1
$a = (g^{k} \bmod p) \bmod q$
$b = k^{-1}(w + za) \bmod q$
(a, b) sign

Verification
$z = b^{-1} \bmod q$
$u_1 = wz \bmod q$
$u_2 = az \bmod q$
$(g^{u_1} \cdot y^{u_2} \bmod p) \bmod q$

p
q
h
w
x
y
x
a
b
z
u_1
u_2

Scanned with CamScanner

Suppose private key = x $\{0 < x < q\}$

calculate public key $\{$with $x\}$

$$y = r^x \bmod p.$$

Till Now key Generation ✗

Example. Generating signature value.

PlainText = w $\{H(M)\}$

$$a = (r^k \bmod p) \bmod q$$

$\{0 < k < q, \gcd(k,q) = 1\}$ $\quad b = k^{-1}(w + xa) \bmod q$

signature = (a, b) if ✗

for verification

$$\begin{cases} z = b^{-1} \bmod q \\ u_1 = wz \bmod q \\ u_2 = az \bmod q \end{cases}$$

v value = $(r^{u_1} y^{u_2} \bmod p) \bmod q$

if this value = a

Then Verified

Qu $p = 11 \quad q = 5 \quad h = 2$

$r = 2^{10/5} \bmod 11$

$\Rightarrow 2^2 \bmod 11$

$r \Rightarrow 4.$

Suppose

① $x = 3$

public key

$y = 4^3 \bmod 11$

$y = 9$

② $k = 3$ $\quad w = 54$ given.

$a = (4^3 \bmod 11) \bmod 5$

$\Rightarrow 9 \bmod 5$

$\Rightarrow 4$

$b = 3^{-1}(54 + 3 \times 4) \bmod 5$

$\Rightarrow 3^{-1}(66) \bmod 5$

$= \{3^{\phi(5)-1} \bmod 5\}$

$= \{3^3 \bmod 5\}$

$\Rightarrow (2 \times 66) \bmod 5$

$\Rightarrow 2$

54 / 12 / 6 6

33 33

27 / 03 / 81

Signature (4, 2)

Verification. $z = 2^{-1} \bmod 5$

$= 2^{\phi(5)-1} \bmod 5$

$= 2^3 \bmod 5$

$= 3$

Scanned with CamScanner

$U_1 = (54 \times 3) \bmod 5 = 2$

$U_2 = (4 \times 3) \bmod 5 = 2$

Values = $(4^2 q^2 \bmod 11) \bmod 5$

$\Rightarrow ((16 \times 81) \bmod 11) \bmod 5$

$9 \bmod 5$

$\Rightarrow 4$ = a Verified

Qu) $p = 7$, $h = 2$, $k = 2$, $H(m) = 3 = w$

$q = 3$

$r = 2^{6/3} \bmod 7$

$\Rightarrow 2^2 \bmod 7$

$\Rightarrow 4$

ϕ = given, q = multiple of $(\phi - 1)$, $\{0 < x < q\}$, $r = h$

$x = 2$

$y = 4^2 \bmod 7$

$\Rightarrow 2$

$a = (4^2 \bmod 7) \bmod 3$

$\Rightarrow 2 \bmod 3$

2

$b = 2^7 (3 + 2 \times 2) \bmod q$

$\Rightarrow 2^7 (7) \bmod 3$

$2^{\phi(3)+1} \bmod 3$

$\Rightarrow (2 \times 7) \bmod 3$

$\Rightarrow 2$

Signature $(2, 2)$

$z = 2^1 \bmod 3$

$\Rightarrow 2$

$U_1 = 3 \times 2 \bmod 3$

$U_1 = 0$

$U_2 = 2 \times 2 \bmod 3$

$\Rightarrow 1$

$(4^0 2^1 \bmod 7) \bmod 3$

$2 \bmod 3$

$\Rightarrow 2$ = a Verified.

Qu) $p = 7$ $q = 11$. find DS using RSA. also verify: $M = 10$

$p = 7$ $q = 11$

$n = 7 \times 11 = 77$

$\phi(n) = 6 \times 10 = 60$

public key $\Rightarrow 13$

private key

$n = p \times q$, $\phi(n)$, $e = GCD(e, \phi(n)) = 1$, $d \cdot e = 1 \bmod \phi(n)$, $d \rightarrow$ private key

Sig $S = M^d \bmod n$, same, $M = S^e \bmod n$

$e \cdot d = 1 \bmod \phi(n)$

$\Rightarrow d = 13^{-1} \bmod 60$

$\Rightarrow 37$.

$x \Rightarrow 37$; $y = 13$

Digital Sign

$S = M^d \bmod n$ — private key; $n = p \times q$

$10^{37} \bmod 77$

$(23)^{18}\ 10 \bmod 77$

$(67)^{9}\ 10 \bmod 77$

$(23)^{4}\ 67 \cdot 10 \bmod 77$

$(67)^{2}\ 67 \cdot 10 \bmod 77$

$23\ 67\ 10 \bmod 77$

Signature ~~Message~~ = 10

Verification

$M' = S^e \bmod n$

$M = 10^{13} \bmod 77$

$(23)^{6}\ 10 \cdot \bmod 77$

$(67)^{3}\ 10 \cdot \bmod 77$

$(23) \cdot 67 \cdot 10 \bmod 77$

$10 = M$

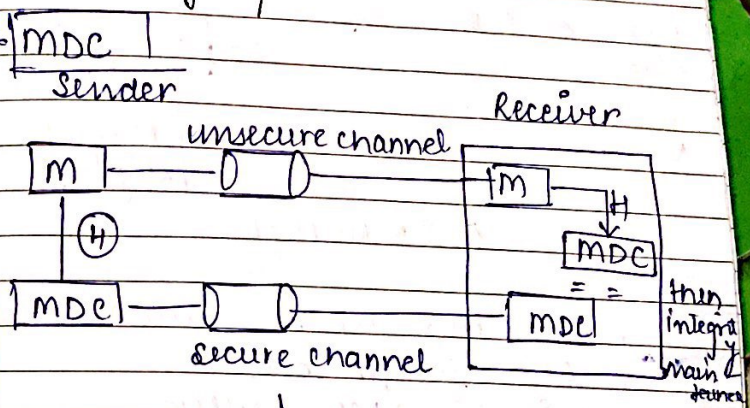
Verified

23/10/18.

Message Authentication.

⇒ MDC

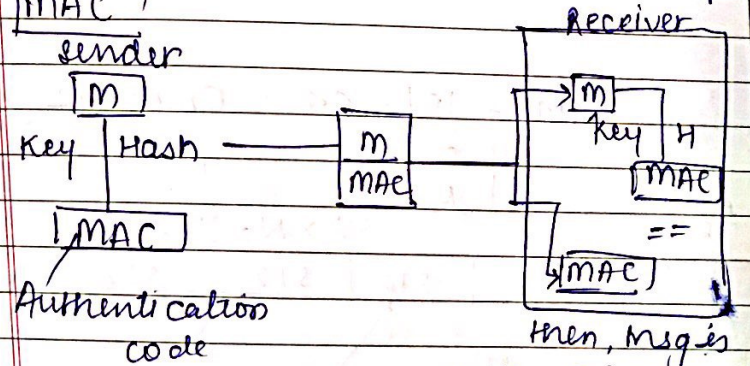
Sender



↓ use of key, will add authenticity

⇒ MAC

sender



Authentication code

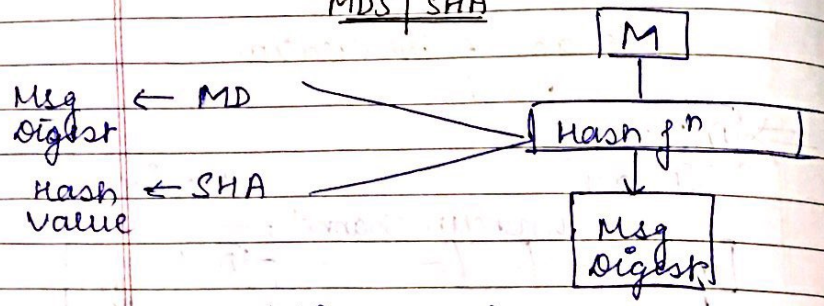
then, Msg is authentic as well as Integrity is maintained.

Asgn Q1 Difference b/w CMAC & HMAC.

Q2 Explain Compression fn

30/Oct'18

MD5 | SHA

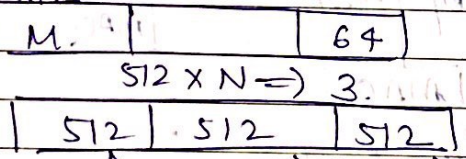


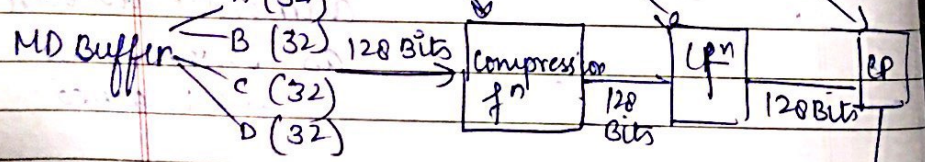
512 x Multiple

1) Add Padding bits into message
2) Add length bits
3) Initialize MD Buffer.
4) divide/separate into 512 block
5) O/p

$|M| + |P| - 64 = 0 \bmod 512$

512 / 64 / 448

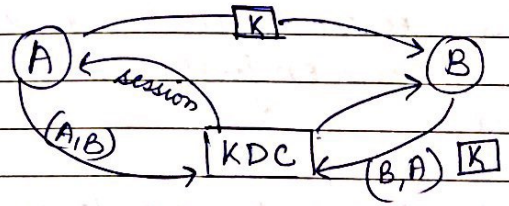




	SHA 1	SHA 224	SHA 256	SHA 512
Block size	512	512	512	512
MD	160	224	256	384
Rounds	80	64	64	80

Message Authentication

Key Distribution Center.

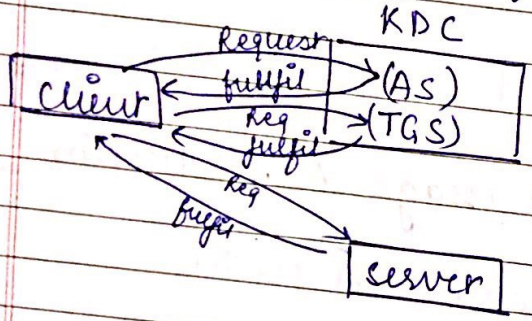


First, A will comm^n with KDC & KDC will provide with the session key & then A will pass that key to B. Then, B will comm^n with KDC & also pass the key. If both the key, one passed by KDC to A & second key from B to KDC matches then A & B will communicate.

→ Three servers will exist by KDC :-
→ Authentication server (AS) } They are with KDC
→ Ticket Grant server (TGS) }
→ server

Scanned with CamScanner

Both server are kept individual
As for client recognition &
second one for key/Token



client Request to each and & as the request keeps on fulfilling it goes forward.

Step1 client send a Request to connect with TGS to AS.

Step2 AS will send session key & Ticket to client.

Step3 Client will send to Ticker to TGS. TGS will verify that & then send a ~~real~~ encrypt ticker to client to connect with the required server.

Step4 Server will decrypt that ticker & give access to client.

Session key is time constrained.

→ Suppose time limit is 10 secs & the session takes more than 10 secs so, server will declare that invalid user.

2 Versions
→ KERBUROS 4
→ KERBUROS 5.
↓ Modification
→ client's time is increased for the session.
→ client can comm" to multiple server at a given time.

Scanned with CamScanner

1/Nov/18

Setting Padding Bits

padding Bits

Message → 449 bits → MD5 → |M| + |P| + 64 = 0 mod 512 (Block size)

Message → 2590 bits → SHA → |M| + |P| + 128 = 0 mod 1024 (Block size)

Eg Padding bits - (MD5)

449 + |P| + 64 = 0 mod 512

513 + |P| = 0 mod 512

512 - 513 mod 512

512 - 1

→ 511

449
64
63

add padding bits.

449 + 511 + 64 = 0 mod 512

1024 = 0 mod 512.

449
511
64
1024

(SHA)

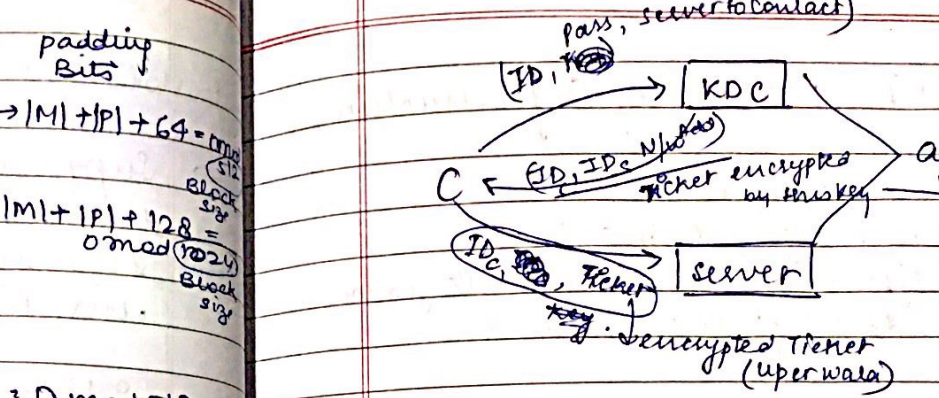
2590 + |P| + 128 = 0 mod 1024

|P| = -2718 mod 1024

1024 - 670

354.

2590
128
2718
1024
1024
2048
2718
2048
670
1024
670
354



Now server will Match the ID for authentication.

This case when KDC is a single entity.

→ If KDC considered as 2 parts AS & TGS Authenticated server gives ticket for TGS & TGS will will give ticket for main server.

Qu $q = 7$, $p = 23$, $x = 3$, $y = 6$. find symmetric shared key.

Sol^n $K = 7^3 \bmod 23$

⇒

49
23
36

All algorithm starts with the selection of a large prime no.

A ← p, g → B

x y

$K_1 = g^x \bmod p$ $K_2 = g^y \bmod p$

$g^{xy} \bmod p$

$K_{11} = (K_2)^x \bmod p$ $K_{22} = (K_1)^y \bmod p$.

Scanned with CamScanner

15/NOV'18.

PKI (Public Key Infrastructure)

Entities can be
→ Registration Authority (Registering)
→ Certificating authority (Verification is done)
→ Validating authority.

Expl^{n} :- User give credential to RA. It will give it to CA after (after verifying) that a stamp is given by CA then request is transfered back to RA.

So we can say RA act as an intermediate b/w CA & users.

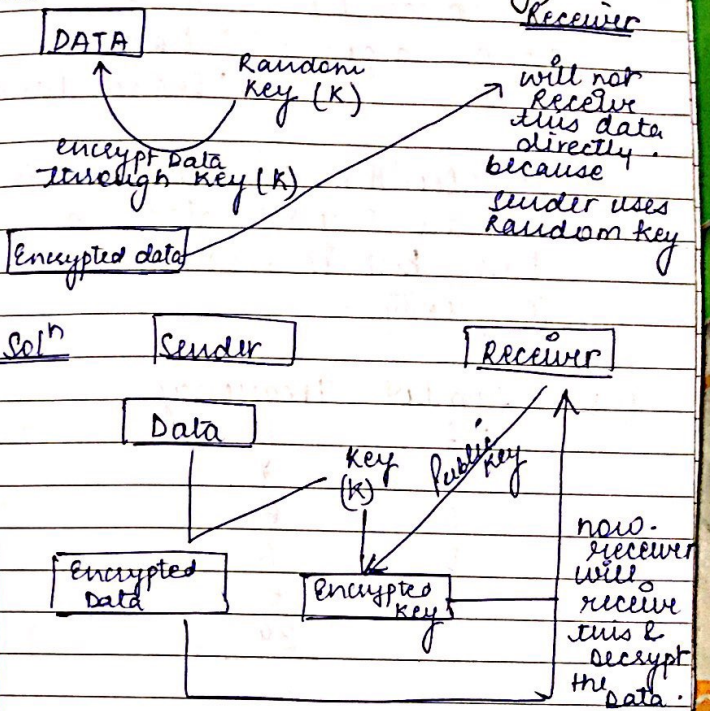
Validating authority plays important role to avoid repudition.

#. Certification standard = X.509 format

Version -
algo used -
Public key -
Validation -

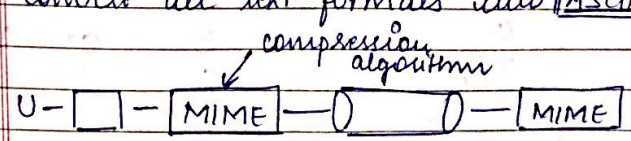
(user jisko issue hai uski)

PGP (Pretty Good Privacy)



Generally used in email transfer.
{used of S/MIME
{Secure Multipurpose Internet Mail Extention}}.

Convert all text formats into ASCII-7



Scanned with CamScanner

compression is provided by various algo:
- LZ78
- LZ77
- LZW
- Huffman
- Shanon Fanno.

→ all algorithm gives different result
→ we can run single algo multiple times but it will increase time complexity.

Qu

symbol	frequency
A	15
B	7
C	6
D	6
E	5
	39

use Huffman algo.

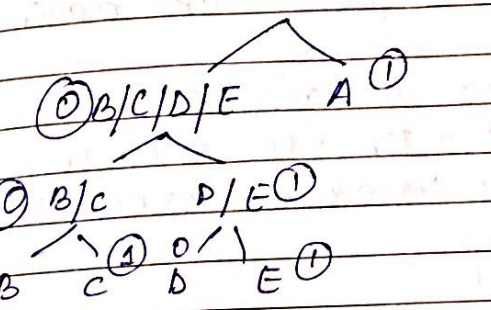
Sol" ① Arrange in Dec" order of freq"
② Combine least 2
③ again step 1.

A = 15
B = 7
C = 6
D/E = 11

⟹ A = 15, D/E = 11, B = 7, C = 6

⟹ A = 15, B/C = 13, D/E = 11

A : 15 ⇒ B/C/D/E : 24
B/C/D/E : 24 A : 15



bits	codes		freq	bits Required
1	1	A	15	15
3	000	B	7	21
3	001	C	6	18
3	010	D	6	18
3	011	E	5	15
				87

for single A we require 1 bit
" B we " 3 bit

⇒ If we use Huffman then we require 87 bits to represent all. {compressed}.

If we use traditional way then ASCII-8 will use 39 x 8 bits

Scanned with CamScanner

Note:-

⇒ Entropy is the max limit upto which any algorithm can compress a particular data.

→ no algo can give 100% result so value after compression will be the ~~max no~~. more than entropy.

19/11/18

* Differentiate b/w substitution & transposition cipher, with the help of example
* Given $p = 17$, $q = 13$, $M = 11$. Generate cipher text using RSA.

Q2. $p = 17 \quad q = 13$

$n = 17 \times 13 \Rightarrow 221$

$\phi(n) = (16)(12) \Rightarrow 192$

$1 < e < \phi(n)$

$GCD(e, \phi(n)) = 1$

Let e be 11 public key.

private key

$d \cdot e = 1 \bmod \phi(n)$

$d = 11^{-1} \bmod \phi(n)$

$\Rightarrow 11^{-1} \bmod 192$

$\Rightarrow 11^{\phi(192)-1} \bmod 192$

$\Rightarrow 11^{31} \bmod 192$

$\Rightarrow (121)^{15}\, 11 \bmod 192$

$\Rightarrow (49)^{7}\, 121 \cdot 11 \bmod 192$

$\Rightarrow (97)^{3}\, 49 \cdot 121 \cdot 11 \bmod 192$

$(1)^{2}\, 97 \cdot 49 \cdot 121 \cdot 11 \bmod 192$

$\Rightarrow 35$

2	192
2	96
2	48
2	24
2	12
2	6
3	3
	1

2^6

$\Rightarrow 2^{6-2^5}$

$64 - 32$

$\Rightarrow 32$

~~mod~~.

$C = M^e \bmod n$

$\Rightarrow 11^{11} \bmod 221$

$\Rightarrow (100)^{5}\, 11 \bmod 221$

$\Rightarrow (55)^{2}\, 100 \cdot 11 \bmod 221$

Scanned with CamScanner

$152 \cdot 100 \cdot 11 \bmod 221$

124

Verify

$M \Rightarrow C^d \bmod n$

$\Rightarrow 124^{35} \bmod 221$

$(127)^{17} 124 \bmod 221$

$(217)^9 187 \cdot 124 \bmod 221$

$16^4 \; 127 \cdot 124$

$(35)^2 \; 127 \cdot 124 \bmod 221$

$120 \cdot 127 \cdot 184 \bmod 221$

$\Rightarrow 210$

Kerberos

(i) authentication service (part of Athena at MIT)

(ii) we can experience 3 threats

(i) user may gain access to particular workstation & pretend to be another user

(ii) alter the network address so that request sent from the altered work-sta appear to come from the impersonated workstation.

(iii) User may eavesdrop on exchange and use a replay attack to gain entrance to a server or to disrupt operations.

Kerberos provide a centralized authentication server whose f^n is to authenticate users to servers & server to user.

Kerberos 4 (MILL88, STEI88)
Kerberos 5 (KOHL94)

Motivation
→ security :- individual computer is secure but when it comes about workstation security is a major issue but is not complex these days.

Scanned with CamScanner

3 Approaches to Security.

1. assure the identity of user or users using client workstation & enforce a security policy based on user ID using server
2. client authenticate them to server
3. Require the user to prove his or her identity for each service invoked.

Kerberos Repot include :-

1. Secure
2. Reliable
3. Transparent
4. Scalable.

Kerberos 4

→ use a Authentication Server (AS) that knows the password of all users & stores these in a centralized database.
→ AS shares a Unique secret key with each Server (in a secure Manner)

1) C → AS : $ID_c \| P_c \| ID_v$ (client; identifier of user on C; pass of user on C; identifier of V)
2) AS → C : Ticket
3) C → V : $ID_c \| Ticket$ (server)

$Ticket = E(K_v, [ID_c \| AD_c \| ID_v])$ (secret encry key shared b/w AS & V; N/w Addr of C)

another secure approach includes (TGS) Ticker Granting Server. {Hypothetical}

Once per user logon session

1) C → AS : $ID_c \| ID_{tgs}$
2) AS → C : $E(K_c, Ticket_{tgs})$

Once per type of service

3) C → TGS : $ID_c \| ID_v \| Ticket_{tgs}$
4) TGS → C : $Ticket_v$

Once per service session

5) C → V : $ID_c \| Ticket_v$

$Ticket_{tgs} = E(K_{tgs}, [ID_c \| AD_c \| ID_{tgs} \| TS_1 \| Lifetime_1])$
$Ticket_v = E(K_v, [ID_c \| AD_c \| ID_v \| TS_2 \| Lifetime_2])$

Difference b/w Ker 4 & Ker 5

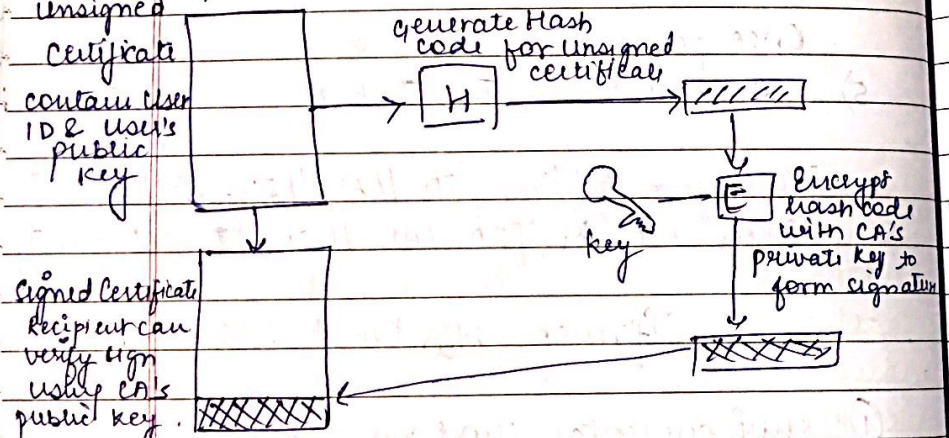
(i) environmental shortcomings :-
(ii) encry system dependence :- Version 4 use only DES, & use any of the encryption technique
(iii) Internet protocol dependence :- Version 4 req IP addressing, Version 5 use any type of length allowing any N/w address type to be used
(iv) message byte ordering :-
(v) Ticket lifetime :- Version 4 8 bit used 5 minutes so max time is 1280 min, Version 5 arbitrary

Scanned with CamScanner

(v) Authentication forward
(vi) Intersecalm authentication
(2) Technical Shortcomings.
(i) Double encryption :- In version 4, 2 encry where 1 is useful & 2 is wasteful.
(ii) PCB encryption
(iii) SessionKey
(iv) Password attack

X.509

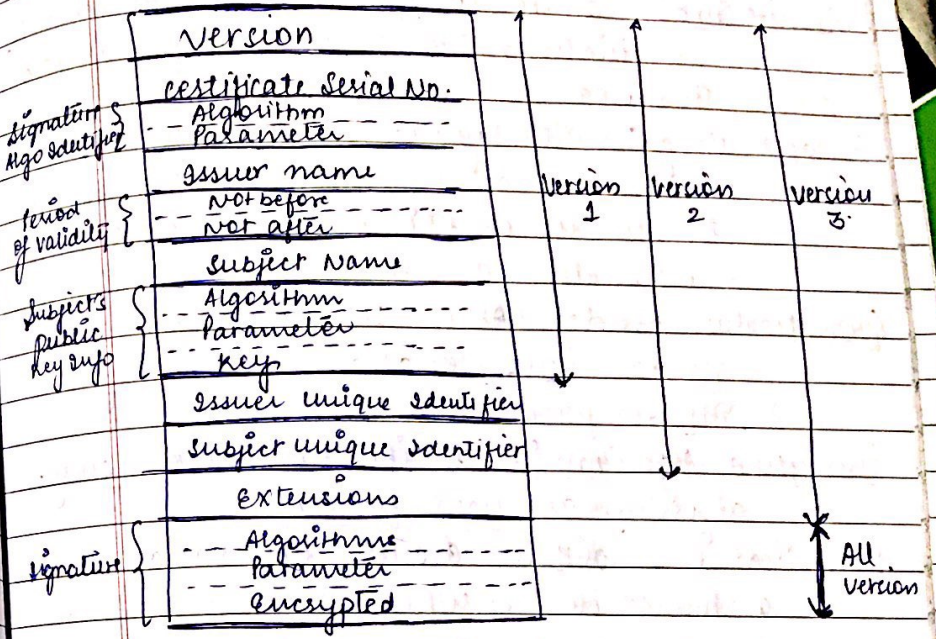
public-key certificate Use



→ part of X.500 series
→ distributed server maintaing user info DB.
→ Define framework for authentication servi
→ Defini authentication protocol

X.509 → public key cryp. is used. (RSA recomm)
→ Certificate issued by Trusted CA (Cert Author.
CA<<A>> {Certi signed by CA for A}

X.509 Certificate



IP Security Architecture

Important Docs.
① RFC 2401 :- overview of a security Architecture
② RFC 2402 :- Description of a pack authentication extension to IP4 & IPv6.
③ RFC 2406 :- Description of a pack encryption extension IP4 & IPv6.
④ RFC 2408 :- Specification of key mgmt capabilities

Scanned with CamScanner

Architecture :- general concept, security requirements, definations & mechanism defining IPsec technology.

Encapsulating Security Payload :- (ESP) covers the packet format & general issues related to the use of ESP for packet encryption & optionally authentication.

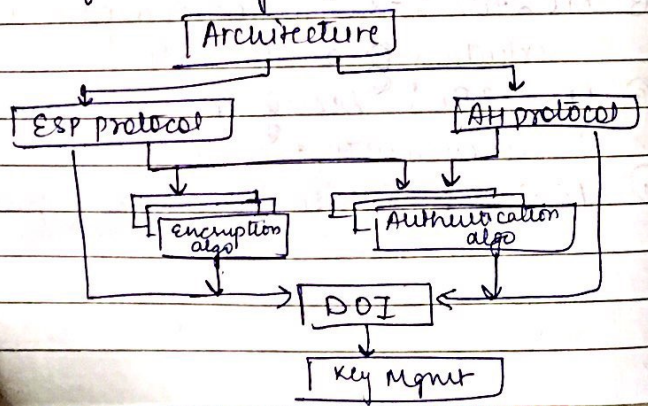
Authentication Header (AH) :- covers packet format & general issues related to the use of AH for pack authentication.

Encryption Algorithm :- describes how various encryp algorithm are used for ESP.

Authentication algorithm :- describe how various authentication algorithm are used for AH & for the authentication option of ESP.

Key Management :- docs that describes key mgmt schemes.

Domain of Interpretation (DOI) :- values needed for the other docs to relate to each other {Identifiers & key lifetime are examples}.



Authentication Header

→ It Provide support for ~~header~~ data Integrity & authentication of IP packets.

→ ensures undetected modification to a ~~transit~~ packet's content in transit is not possible

→ AH also guards against the replay attack ~~described~~

→ Authentication is based on MAC (Message Authentication Code)

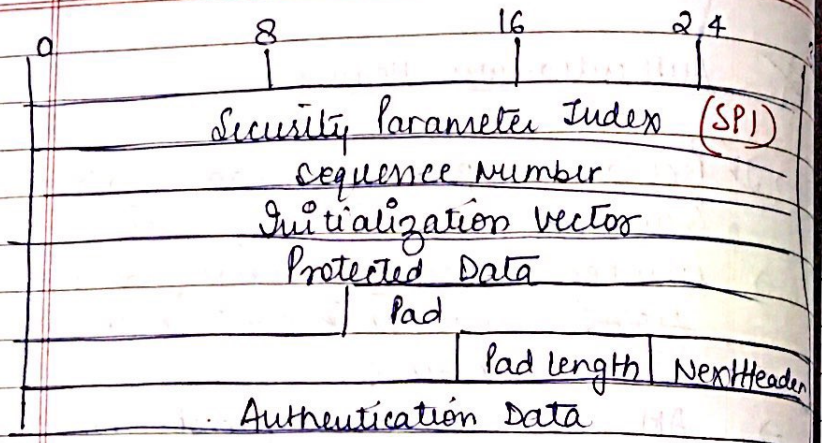
Authentication Header

Bit 0	8	16	31
NextHeader	Payload length	Reserved	
Security Parameters Index (SPI)			
Sequence Number			
Authentication Data (variable)			

Encapsulating Security Payloads

ESP is a Protocol within the IPsec for providing authentication, Integrity & Confidentiality of N/w packets data/payload in IPv4 & IPv6 N/w. ESP provide msg/payload encryption & the authentication of a payload & its ~~orgin~~ origin within the IPsec protocol Suite

Scanned with CamScanner



Combining Security Association

Individual SA can implement either AH or ESP protocol not both. But in some cases both protocols are required so for that we need multiple SAs for an same traffic flow.

Security Association Bundle refers to a sequence of SAs through which traffic must be processed to provide a desired set of IPSec services.

SA can combine in 2 ways :-

1. Transport adjacency :- applying more than one security protocol to the same IP packet, without invoking tunneling.
2. Iterated tunneling :- Refers to the appln of multiple layer of security protocol effected through IP tunneling.

Key Management

It involves the determination & distribution of secret keys.

4 keys ⇒ 2 transmit & 2 receive (for both AH & ESP)

2 Types of key mgmt

1. Manual : manually configure each system
2. Automated :- on-demand creation of keys for SAs & facilitate the use of keys in large distributed system

consist of :-

→ Oakley key determination protocol (key exchange)
(based on Diffie-Hellman algo)
→ Internet security Association & key mgmt protocol (ISAKMP)
: provide
(i) framework (ii) specific protocol support, (iii) formats etc

Secure Socket Layer & Transport Layer Security

SSL → was designed with public review & input from industry & was published as an Internet draft docs. Subsequently, when a consensus was reached to submit the protocol for

Scanned with CamScanner

Ask sir about SSL & TLS

Internet Standardisation, The TLS working group was formed within IETF to develop a common standard.

Secure Electronic Transaction (SET)

Its is an open encryption & security specification designed to protect credit card transactions on the Internet.

Secure Electronic Transaction is an examples of application of Credit Card

Intruders

It is one of the two most publicized threat to security. Generally referred to as a hacker or cracker.

3 classes of Intruder :-

Outsider ① Masquerader :- unauthorised user acces control to exploit a legitimate user's ac

Insider ② Misfeasor :- authorised user who misuse the priviledges or unauthorise user wants to access.

outsider or insider ③ Clandestine user :- Individual who seizes supervisory control of the sy

Intrusion Technique

→ aim is to gain access or incr privileges on a
→ key goal often is to acquire password sys

Intruder Range

benign → Serious

① (normal searching of data) ① (attempt to read privileged data)

② Tolerable ② Severe

Password files can be protected by intruders in 2 ways

① One-way fn :-

system: fn ← user: Password

based on user's pass.

system transform the pass, & compare that with stn fn

② Access control :- pass file limited to one or very few accounts

Viruses & Related Threats

① Malicious Programs :-

Virus :- Attaches itself to a program & propagate copies to itself to other progr^n

Worm :- prog that propagates copies of itself to other computer

Logic bomb :- Trigger action when condition occur

Trojan horse :- prog that contain unexpected additional functionality

Backdoor (Trapdoor) :- prog modification that allows unauthorized access to functionalities

Scanned with CamScanner

Exploits :- Code specific to a single or set of vulnerabilities.

Downloaders :- prog that install other item on a m/c that is under attack (sent via email)

Auto-rooter :- Malicious hacker tools used to break into new m/c remotely.

kit :- tool generating new viruses automatically

Spammer :- send large volume of unwanted email

flooder :- attack m/w computer to carry out denial of service attack.

Keylogger :- Capture keystrokes

Rootkit :- Set of hacker tool used after Root access

Zombie :- prog activated on an infected m/c that is activated to launch attack on other m/c.

Firewall Design Principles

Imp Goals for firewall are :-

1. All traffic from inside & Outside must pass through a firewall. (achieved by blocking all the access to the local n/w except the firewall)
2. Only authorised traffic, as defined by the local security policy will be allowed to pass.
3. Firewall itself is immune to penetration

Firewall provide 4 techniques to use to control access.

1. Service control :- Internet service that can be accessed, inbound or outbound. filter traffic on the basis of IP address & TCP port number.
2. Direction control :- Direction for initiation of a request.
3. User control :- Control access to a service according to which user is attempting to access it.
4. Behavior control :- Control how particular services are used.

Features of firewall

1. provide location for monitoring security-related events
2. Single choke point that keeps unauthorised user out of the protected n/w.
3. Convinient platform for several Internet f° that are not security related
4. Can serve as a platform for IPsec.

Scanned with CamScanner

Limitations of firewall

1. Cannot protect against the attack that bypass the firewall.
2. Does not protect against internal threats.
3. The firewall cannot protect against the transfer of virus-injected programs or files (because they are supported inside the perimeter)

← Trusted System

Book
no short
notes

Birthday Attack

Collision

→ Hash(x_1) = Hash(x_2)
But $x_1 \neq x_2$

Eg { 12 mod 10 = 2 } but $12 \neq 22$
{ 22 mod 10 = 2 }

Same {birthday} attacks.
pass → B.date
(2 person same day)
pass exchange.)

Probability

	not same	same
9 →	90%	10%

1 → 1

2 → $1 \times \frac{364}{365}$ 3 = $1 \times \frac{364}{365} \times \frac{363}{365}$

9 = $1 \times \frac{364}{365} \times \frac{363}{365} \cdots$ 9 Person

23 →	< 50%	> 50%
50 →	3 %	97%
57%	1%	99%

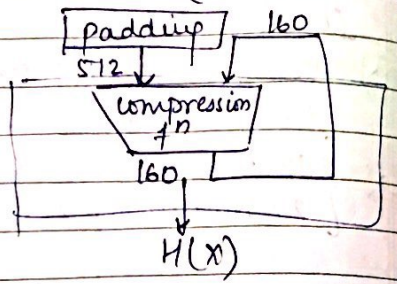
1 2 3 4 5 6 7 8 9 10

Scanned with CamScanner

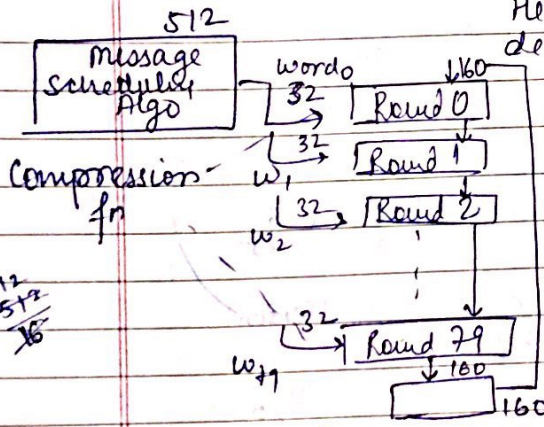
SHA 1

$X(X_1, X_2 \ldots X_n)$

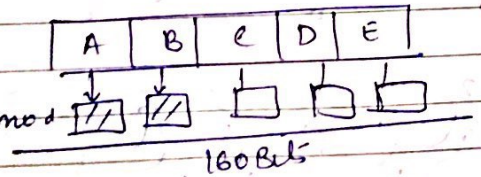
Arbitrary length → X → SHA 1 → 160 bit H(X)



Padding ⇒ divide i/p into 448 bits.
then use padding to make 512
448 + 64 = 512
Hexa decimal



160 Bits into 5 parts



5/Dec '18.

Sri

PPT

Authentication Appl^n.
↓
Developed to support appl^n level auth. & digital signature

Services → Kerberos (private-key authen)
→ X.509 (public key dir auth).

Kerberos

→ Athena project past developed at MIT.
→ Symm encryption (no public keys)
→ Centralised private-key third party authentication in a Dis N/w.

Kerberos
version 4 | version 5

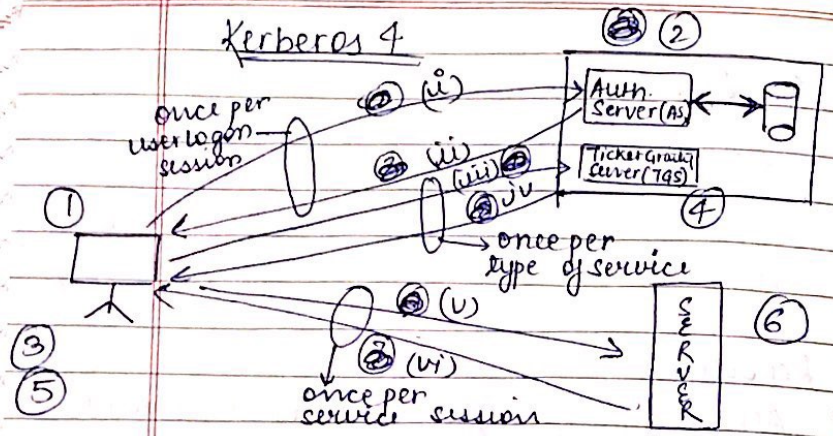
Motivation
→ provide security in a distr Arch. consisting of dedicated users workstations (clients) & distributed over centralised servers.
→ Require the user to prove his identity for each service invoked.
→ Server prove their identity to client.

Adv → Secure, reliable, transparent & scalable

→ Use protocol Needham & Schroeder (NS78)
→ C & S trust Kerberos to mediate their mutual Authentication.

Scanned with CamScanner

Kerberos 4



(1) User logon to work station & request service on host.

(i) (ii) Request ticket-Granting ticket.

(iii) (iv) ticket + session key

(2) AS verifies user access right in DB, create ticket-granting ticket & session key. Result are encrypted using key derived from user's password

(iii) request service granting ticket

(iv) ticket + session key

(3) workstation ask usr for pass, with pass he decrypt the message then send ticket

(4) TGS decrypt ticket & authenticator, verifies request then creates ticket for requested server

(5) workstation send ticket & authenticator to server

(v) request service

(vi) provide server authenticator.

(6) Server matches ticket & authenticator match, then grants access to service.
If Mutual Authentication is required, server returns an authenticator

Roles of AS
- → Knows all user pas & stores in a DB
- → Shares a unique secret key with each server
- → Issue an encrypted ticket Grant Ticket

TGS
- → TGT contains a lifetime & stamp
- → Issue ticket to users authenticated by AS
- → Encrypted with a key only known by AS & TGS
- → Return a Service Granting ticket.
  - ↓ contain TS & lifetime

Kerberos Dialog

(1) Prob :- lifetime & no Server authe. to user.
- use a session key

(2)(3) Message Exchange
- AS exchange to obtain TGT.
- TGS exchange to obtain Service GT
- C/S authentication exchange to obtain Servic

Scanned with CamScanner

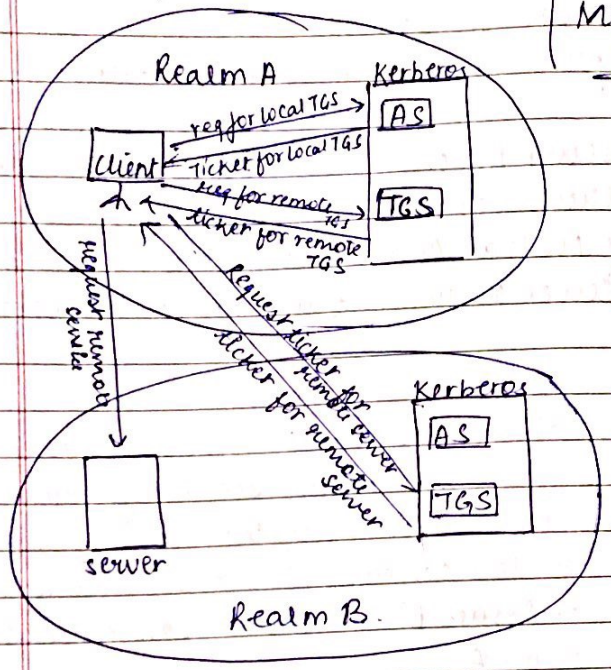
Ker. Environment consist

1. Server
2. no. of client, all registered with Server
3. appl^{n} server, sharing keys with Server

Kerberos Realms

→ Set of Managed nodes that share the same Kerberos database.

Multiple Kerberi

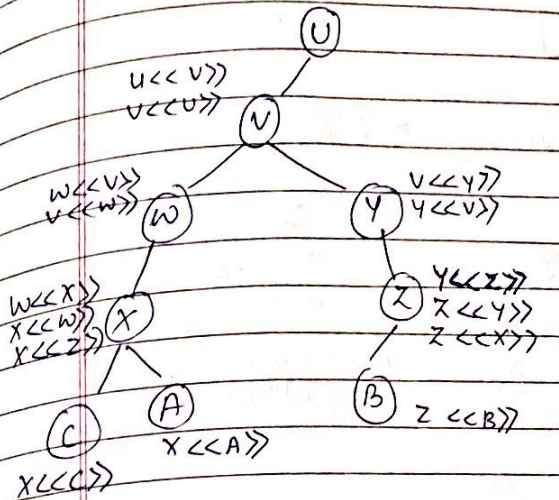


Version 5

→ fixes Version 4 environmental shortcomings
→ New element for AS exchange
(i) Realm, (ii) Option (iii) Times (iv) Nonce
→ C/S authentication exchange
- Subkey
- Seq NO.

→ Kerberos Ticker flag

CA Hierarchy



Certificate Revocation

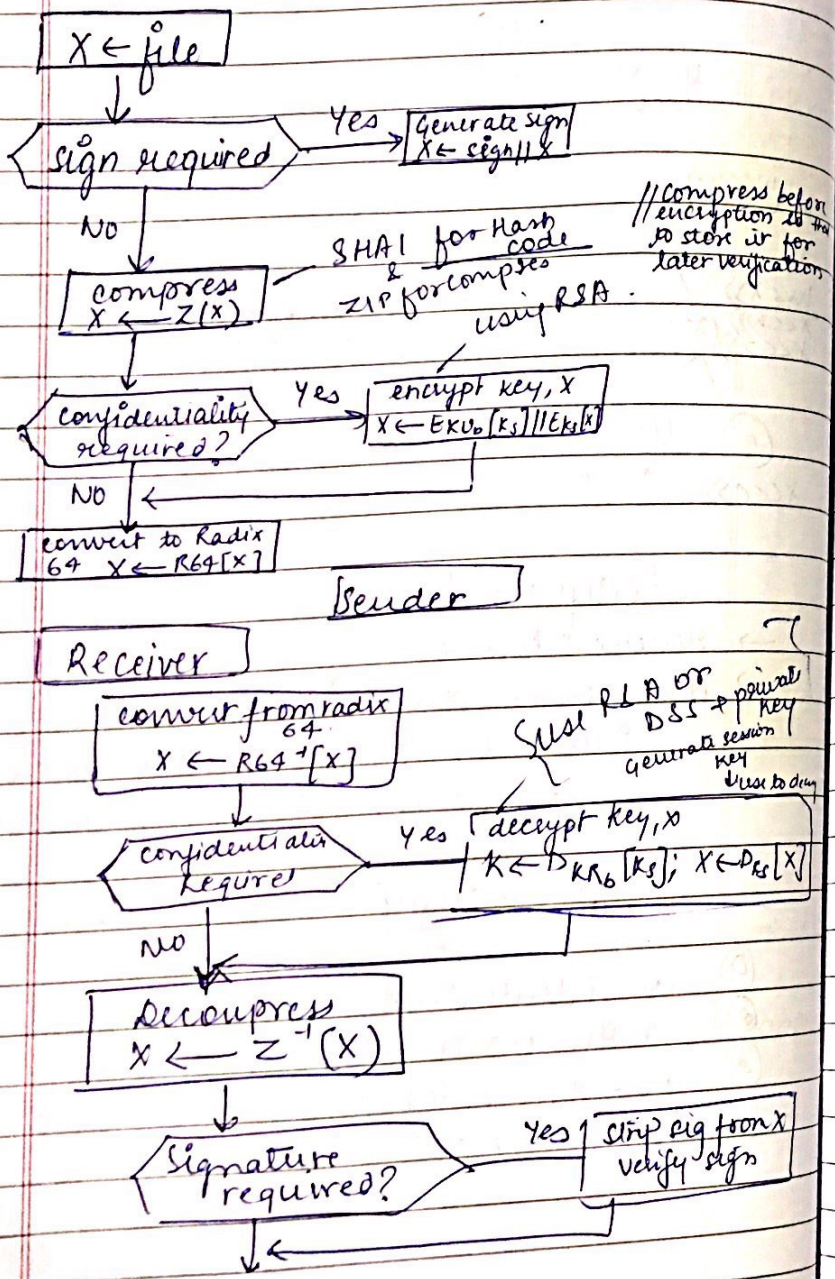
→ renew before expiry
→ else • user's private Key is compromised
- user is no longer certified by this CA
- CA's certificate is compromised

Email security Enhancement

1. Confidentiality
2. authentication
3. Message integrity
4. non-repudiation of origin

Scanned with CamScanner

PGP



PGP Email Compatibility

→ Binary data to send (every msg etc)
→ Mail designed only for Text
→ PGP must encode raw binary into printable ASCII char.
→ radix 64 algo
  → 3 byte to 4 printable char (map)
  → append CRC
→ pgp perform segmentation

PGP Public & Private key

→ Many Pub/Pri key so need to select which to use for every session key
  • could send full public key with every msg
  • but it is inefficient.
→ Use key Identifier based on
→ Least significant 64 bits.

Key Ring

Public key Ring — user knows all the public key of all other user that are known to him

Private key Ring — contain pub/private key pair for this user, Indexed by ID & every

Scanned with CamScanner

S/MIME (Secure/Multipurpose Internet Mail Extensions)

→ Security enhancement to MIME email.
- original internet was only text
- MIME provide support for varying content types & multipart message.
- encoding from binary to textual form
- S/MIME added security enhancement

ff

- enveloped data
  encrypted content & associated keys
- signed data
  encoded msg + signed digest
- clear-signed data
  cleartext msg + encoded signed digest
- signed & enveloped data
  nesting of signed & encrypted entities

S/MIME Cryptographic algo.

1) hash f" → SHA1 & MD5
2) dig sign → DSS & RSA
3) session key encry : Elgamel & RSA
4) msg-encry :- Triple DES

→ procedure to decide which algo to use

provide
(1) authentication
(2) confidentiality
(3) key mgmt

Benefits of IPsec

1) firewall security to all traffic crossing the Perimeter
2) IPsec is resistant to bypass in firewall / Router
3) transparent to end user
4) secures routing architecture.
5) security to individual user.

Services

1) Access control
2) connectionless integrity
3) Data Origin authentication
4) Limited traffic flow confidentiality
5) Rejection of replayed packets

Prev

ESP

uses padding
→ to expand plaintext to req. length.
→ to align pad length & next header fields
→ to provide partial traffic flow confidentiality.

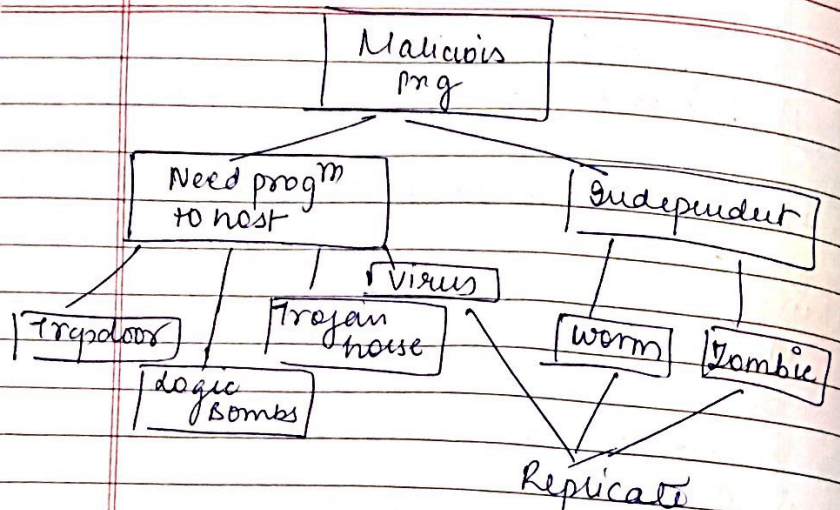
Prev

approach to Intrusion Detection

→ statistical anamoly detection
  → threshold
  → profile based
→ rule-based detection.
  → anamoly
  → penetration identification.

Scanned with CamScanner

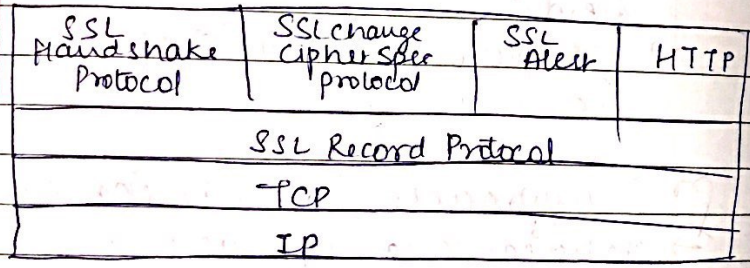
classmate
Date
Page



SSL (Secure Socket Layer)

→ provide Transport layer security (TLS)
→ Developed by Netscape
→ became Internet standard known as (TLS)
→ Use TCP to provide end to end service
→ 2 layer of protocol

Arch



SSL session

→ association b/w c/s
→ Created by Handshake protocol
→ Shared by multiple SSL conn
→ define set of Crypto. paramtr

classmate
Date
Page

SSL connection

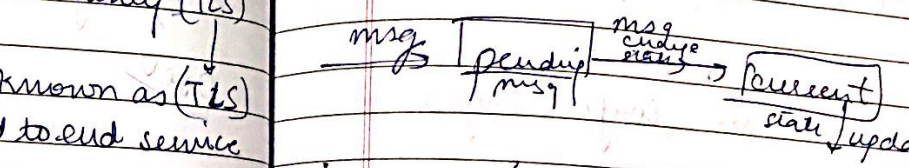
→ A transient, peer to peer, communication link
→ associated with 1 SSL session

Confidentiality

→ using symm encryption with a shared key
→ msg compressed before encryption

Integrity

→ using MAC with shared secret key
→ similar to HMAC but diff padding



SSL Handshake Protocol

* allow client/server to
  → authenticate each other
  → negotiate encry & MAC
  → negotiate cryptographic keys
* comprises a series of msg exchanges
  → Establish Security Capabilities.
  → Server authentication & key exchange
  → Client " " " "
  → Finish

Scanned with CamScanner

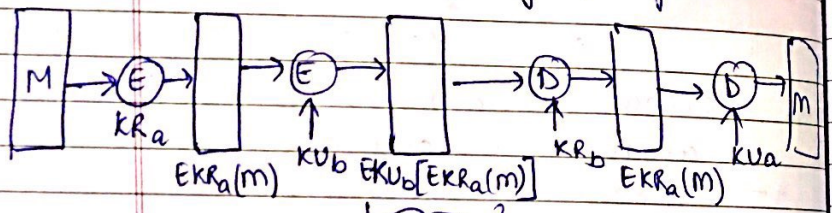
Confi - only particular receiver can decrypt

Sign + Auther → only sender can encrypt

Msg encryption

- public-key
  - encryption provides no confidence of sender
  - since anyone potentially knows public key
- however if
  - → sender sign message using private key
  - → then encrypt with rece. public key
  - → have both secrecy & authentication
- Again need to recognize corrupted msg
- but at cost of 2 public-key uses on msg

To ensure all 3 authentication, confi, Signature:



- provide conf because of KU_b
- provide auth & sign because of KR_a

MAC

→ Generated by an algo that creates a small fixed-sized block.
- Depending on both msg & some key
- like ency though need not be reversible

→ append to msg as a signature

→ receiver → computation → {msg = MAC}

→ If = provide assurance that msg is unaltered and comes from sender

Q Why use MAC?

A When only authentication is needed & we need authentication to persist longer than the encryption (eg. archival uses)

Properties

→ cryptographic checksum MAC = $C_K(M)$
- condenses a variable-length msg M
- using a secret key K to a fixed length size authenticator

→ Many to one f°
many msg (same MAC) but finding them needs to be very difficult.

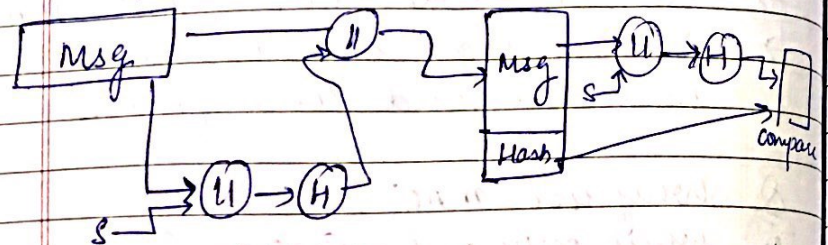
Requirement for MAC

1. Infeasable to find another msg with same MAC
2. Should be uniformly distributed
3. Should depend equally on all bits of msg

Scanned with CamScanner

Hash f^n

→ arbitrary msg to fixed length
→ HF is public not keyed like MAC
→ use to detect changes to msg
→ Can use in various ways with msg
→ used to create DS (widely



Req.
① applied to any size
② fixed length O/P = h . which is easy to compute $h = H(M)$ for any msg
③ h is infeasible to find
④ XOR of msg blocks
⑤ not secure

MD5

① Padding

congruent to 448 modulo 512.
msg is 64 bits less of being a multiple of 512
Padding is always performed.
Single '1' bit rest 0's are appended
→ at least 1 bit & at most 512 bits added

② Append length

→ 64 bit length msg appended in prev rest
→ If $b > 2^{64}$ then only lower order 64 bits are used
now msg is exact multiple of 512

③ Initialize MD Buffer
A 4 word buffer (A,B,C,D) is used to compute msg digest
each 32 bit register

A = 01 23 45 67
B = 89 ab cd ef
C = fe dc ba 98
D = 76 54 32 10

④ Process Message in 16 word block
→ take 3(32) bit as input & give 1(32) bit O/P

Scanned with CamScanner

(5) Output:

O/p as A, B, C, & D. begin with A & ends with D

Summary

→ simple

→ fingerprint or message digest of msg of arbitrary length.

Scanned with CamScanner

A	S	Prob(S) = 3/5
great	S	
Game	S	Prob(NS) = 2/5
The	NS	
election	NS	P(sport / Avery close game)
was	NS	
over	NS	→ P(Avery close game / sport) / P(sports)
very	S	
Clean	S	P(Not a sport / Avery close game)
Match	S	
A	S	→ P(Avery close game / Not sport) / P(Not sport)
clean	S	
but	S	
forgettable	S	
game	S	
It	NS	
was	NS	
a	NS	
close	NS	
election	NS	

P(A/sport) * P(very/sport) * P(close/sport) * P(game/sport) * P(sport)

→ 2/11 * 1/11 * (0/11) * 2/11

Laplace

→ (2+1)/(11+14) * (1+1)/(11+14) * (0+1)/(11+14) * (2+1)/(11+14).

2/154 * 2/154 * 1/154 * 3/154 + 18/(154)^4.

→ 3.200 × 10^-8 * 3/5

Scanned with CamScanner