Cryptography & Network Security (KCS074)

Unit-1 :- Introduction to security attacks, services and mechanism, Classical encryption techniques substitution ciphers and transposition ciphers, cryptanalysis, steganography, stream and block ciphers. Modern Block Ciphers: Block ciphers principles, Shannon's theory of confusion and diffusion, fiestal structure, Data encryption standard (DES), Strength of DES, Idea of differential cryptanalysis, block cipher modes of operations, Triple DES.

Unit-2 :- Introduction to group, field, finite field of the form GF(p), modular ~~arithmatic~~ arithmetic, prime and relative prime numbers, Extended Euclidean Algorithm, Advanced Encryption Standard (AES) encryption and decryption fermat's and Euler's theorum, Primarily testing, Chinese Remainder theorum, Discrete Logarithmic Problem, ~~Principle~~ Principles of Key crypto systems, RSA algorithm, security of RSA.

Unit-3 :- Message Authentication Codes: Authentication requirements, authentication functions, message authentication code, hash functions, birthday attacks, security of hash functions, Secure has algorithm (SHA) Digital signatures: Digital signatures, Elgamal Digital Signature Techniques, Digital signature standards (DSS), proof of digital signature algorithm.

Date.....

Unit-4 :- Key Management and distribution : Symmetric key distribution , Diffie - Hellman Key Exchange , Public key distribution , X.509 Certificates , Public key Infrastructure . Authentication Application : Kerberos , Electronic mail security : pretty good privacy (PGP) , S/MIME.

Unit-5 :- IP Security : Architecture , Authentication header , Encapsulating security payloads , combining security associations , key management , Introduction to Secure Socket layer , Secure electronic , transaction (SET) System Security : ~~Introduction to~~ Introductory idea of Intrusion , Intrusion detection , Viruses and related threats , firewalls.

Date: 09/08/18

Day:- Wednesday

Subject: CRYPTOGRAPHY & NETWORK SECURITY

⇒ CRYPTOGRAPHY:-

It consists of two words: Crypto & graphy.

> Crypto means: hidden
> Graphy means: writing.

It is a art of hiding or conceiling intangible message into a non-intangible message so that a opponent can not understand the message or information which is in turn over a communication channel.

⇒ IMP SECURITY ATTACKS:-

Any action that leads to compromise the security of information is called Security Attack.
It is of two types:-

1. Active Attack
2. Passive Attack

1. Active Attack:

It involve some modification of data or the false creation of stream. It is easy to detect but difficult to prevent.

a) Masquerade:

It involves the creation of false identity when a third party behaves as an authenticated identity.

b) Replay:

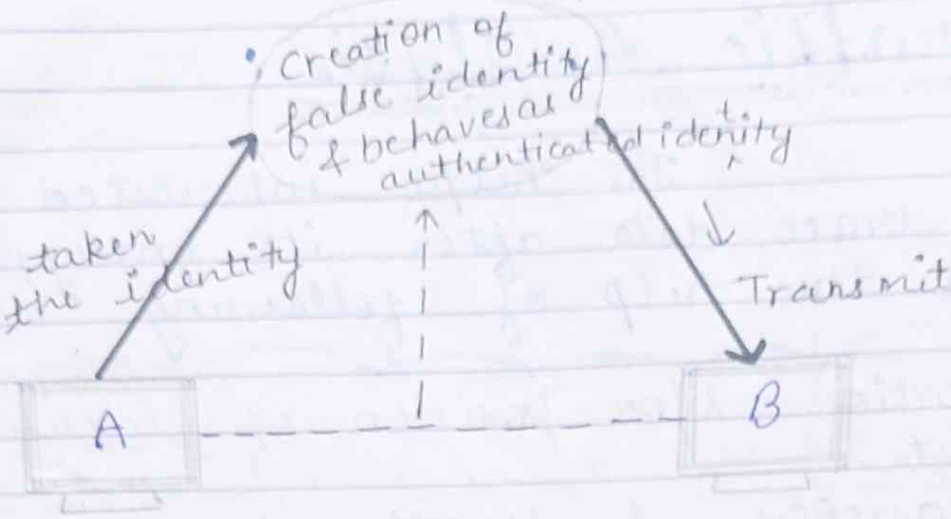
It involves the passive capture of data-unit & its subsequent re-transmission to produce an unauthorized effect.

c) Modification of message:

It means that some portion of a message is altered, delayed or re-ordered.

d) Denial of Service:

Creation of problems in network so that authenticated users cannot communicate.

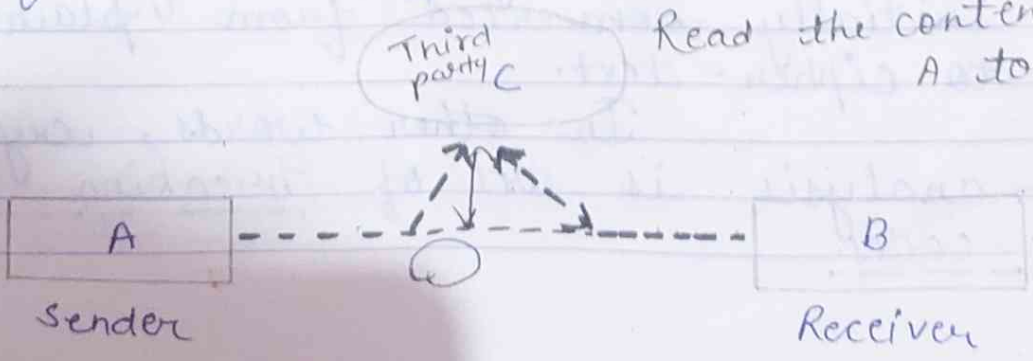


2. Passive Attack :-

These are in the nature of (अनाधिकृत)
keeps Evasdropping or monitoring of transmitted datd.

a) Release of Message :

Information passes over two communication channels or network is always subject to interaction like- an email messages. The need is to prevent those data from the opponent.



b) # Traffic Analysis :

It helps interested people to trace data after its encryption via the help of following details-

* Location &/or position of identity of hosts.
* Frequency & length of message.
* Collection of Cipher text.

Date:- 10/08/18 Day:- Friday

CRYPTOGRAPHY:

The process of converting from plain - text to cipher - text is known as enciphering or encryp - tion.

Crypt - Analysis :-

It is technique of decoding cipher - text into plain - text without knowing how they are initially converted from plain - text to cipher - text.

In other words, crypt - analysis is art of breaking secret - codes.

Crypt - Analyst :-

It is a person who attends to break cipher-text message to obtain the original plain-text message.

✡ Difference b/w Threat & Attack :-

	Threat	Attack
1.	A threat tends to be a promise of an attack to come.	1. An attack tends to be an act, of which is in processing.
2.	A potential operands that malicious or anything that may harm an asset.	2. An action taken to harm an asset

Substitution Technique.

⇒ Monoalphabetic Cipher :

In monoalphabetic ciphers, a character or symbol in the plain-text is always changed to

same characters or symbol in the cipher text regardless of its position in the text. for eg: Here, a scheme for encrypt message by replacing each alphabet with an alphabet -3 places down the line is shown.

Key = 3

Plain Text	C	R	Y	P	T	O	G	R	A	P	H	Y
Cypher Text	F	U	B	S	W	R	J	Q	D	S	K	B

⇒ Additive Cipher :

Encryption

$$C = (P + K) \bmod 26$$

C = Cipher Text.
P = Plain Text.
K = Key

Decryption

$$P = (C - K) \bmod 26$$

Ques: Encrypt the plain-text "Hello" with key = 15 using Additive cipher.

Soln Plain Text :-

h	e	l	l	o
7	4	11	11	14

Add key :- + 15 15 15 15 15

22	19	26	26	29

Taking mod 26 : 22 19 0 0 3

W	T	A	A	D

Date:- 13/08/18 Day:- Monday

Playfair Cipher :- Substitution

The best known multiple letter encryption cipher is the Playfair, algorithm is based on the use of a 5x5 matrix of letters constructed using a keyword. Eg:

Sentence:- Hello John. How are you?

Keyword:- PLAYFAIR

Make matrix -

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

In this case keyword is PlayFair.

1. Repeating plain-text letters that are in the same pair are separated with a filler letter. such as- X, so, thus Hello would be treated as- HELXLO

2. Two plain-text letters that fall in the same row of the matrix are each replaced by the letter to the right. with the first element of the row circularly following the last. eg PF is encrypted as - LP

3. Two plain-text letters that fall in the same column of the matrix are each replaced by the letter beneath with the top element of the column circularly following

the last eg

LV is encrypted as- RL

4. Each plain-text letter in a pair is replaced by the letter that lies in its own row & the column occupied by the other plain-text letters. Thus-

He is encrypted as- KG / GK

Date:- 14/08/18 Day:- Tuesday

Hill Cipher :-

This encryption takes 'm' successive plain-text letters & substitutes for them 'm' cipher-text.
It can be expressed in terms of column - vectors & matrices.

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

or

$$C = K P \mod 26$$

eg Plain-text- Pay More Money

$$K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}_{3\times3} \begin{bmatrix} P \to 15 \\ A \to 0 \\ Y \to 24 \end{bmatrix}$$

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

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

$$K = \begin{bmatrix} L \\ N \\ S \end{bmatrix}$$ Ans

* Polyalphabetic Cipher :-

Another way to improve on the simple monoalphabetic technique is to use different monoalphabetic substitutions as one proceeds to the plain-text message.

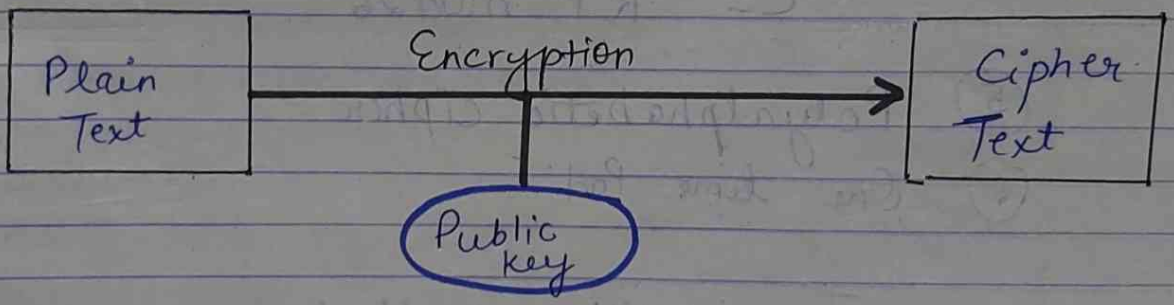
It has the following features in common-

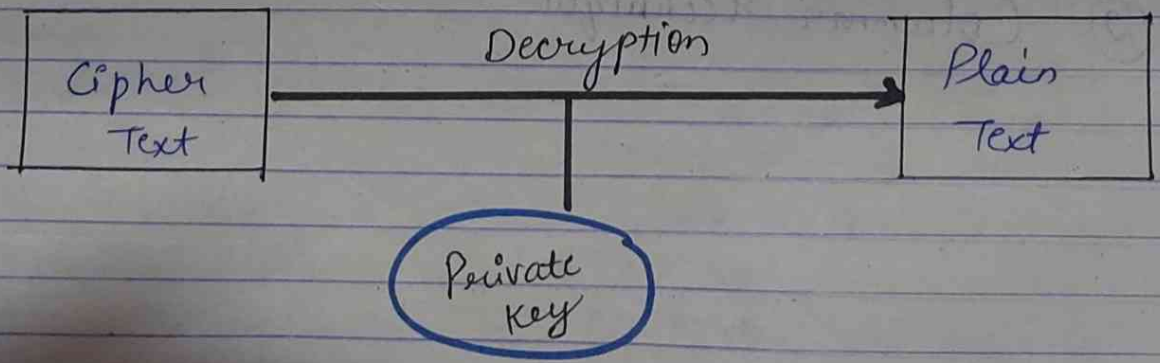
(a) A set of related mono-alphabetic substitution rules is based.

(b) A key determines which particular rule is choosen for a given transformation.

Table important -

P.T.		A a	B b	C c	. . . . .	Z z
Key	A a	A	B	C	D	
	B b	B	C	D	E	
	C c	C	D	E	F	
	.					
	.					
	.					
	Z z	Z	A	B	. . . . .	Y





Substitution Technique

1. Monoalphabetic Cipher (1 cha./sy change)
2. Additive Cipher-

   Encryption -

   $C = (P + K) \bmod 26$
3. Playfair cipher (multiple letter encryption)
   5 x 5 matrix, Keyword.
4. Hill cipher

   $C = KP \bmod 26$
5. Polyalphabetic cipher
6. One time Pad

Transposition method

1. Rail fence
2. Columnar technique

Date:- 16/08/18 Day:- Thursday

One-Time Pad :-

Each new message requires a new key of the same length as the new message. Such as- Scheme is called- One Time Pad.

It produces random output that bears no statistical relationship to the plain- text.

P.T. ⇒ Save Yourself.
Key MOWY abcfgkpt
C.T. ⇒ Key ⇒ gazg yrsmmuwm

P.T. ⇒ Save yourself.
Key ⇒ pxlm vmsydofu
C.T. ⇒ HXGQ TAMPVSQZ

Transposition Method :-

Rail fence :- All the techniques examine so far involved the substitution of a cipher- text symbol for a plain- text symbol; A very different kind of mapping is a cheap performing some sout of permutation on the plain- text letters. This technique refers to

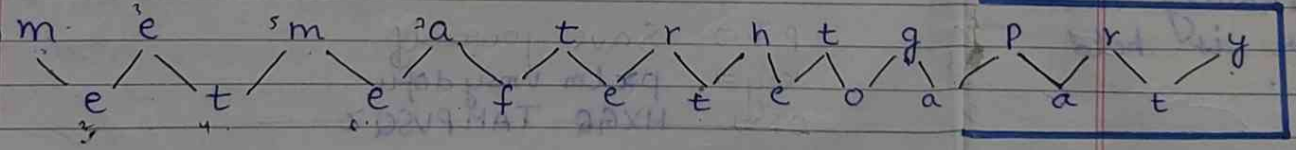
the transposition.

Its of two types -

Rail fence :- In this, plain-text is written-down as a sequence of diagonals & then read of as a sequence of Rows.

For eg:- To in cipher the message-

✓Meet me after the toga party.
with a rail-fence of depth - 2.
we write the following -



C.T. ⇒ memat rh t g p r y e t e f e t e o a a t

Columnar Technique :-

A more complex scheme is to write a message in a rectangle, row by row & read the message of column by column but permute the order of the columns.

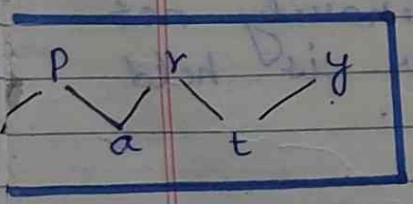
for eg:-

Key:- 4 3 1 2 5 6 7

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

C.T. ⇒ ttnaaptmtsuoaodwcoi
xknlypetz

Steganography:-



-y The method of staganograph conceil the existence of the message whereas the method of cryptography render the message unintelligible to outsiders by various transformations of text. Other techniques have been used historically are-

1. Character Marking:-

Selected letters of printed or type written text are over-written (text) in pencil. The marks are ordinary

not visible unless the paper is held at an ∠ (Right angle)

2. Invisible Ink-

A no. of substances can be used for writing but leave no visible place until heat or some chemical is applied to the paper.

3. Pin - Punctures :-

Small Pin- Punctures on selected letters are ordinarily not visible unless the paper is held up infront of a light.

4. Type - writer correction ribbon:-

Used b/w lights typed with a black- ribbon. The results of typing with the correction tape are visible only a strong light.

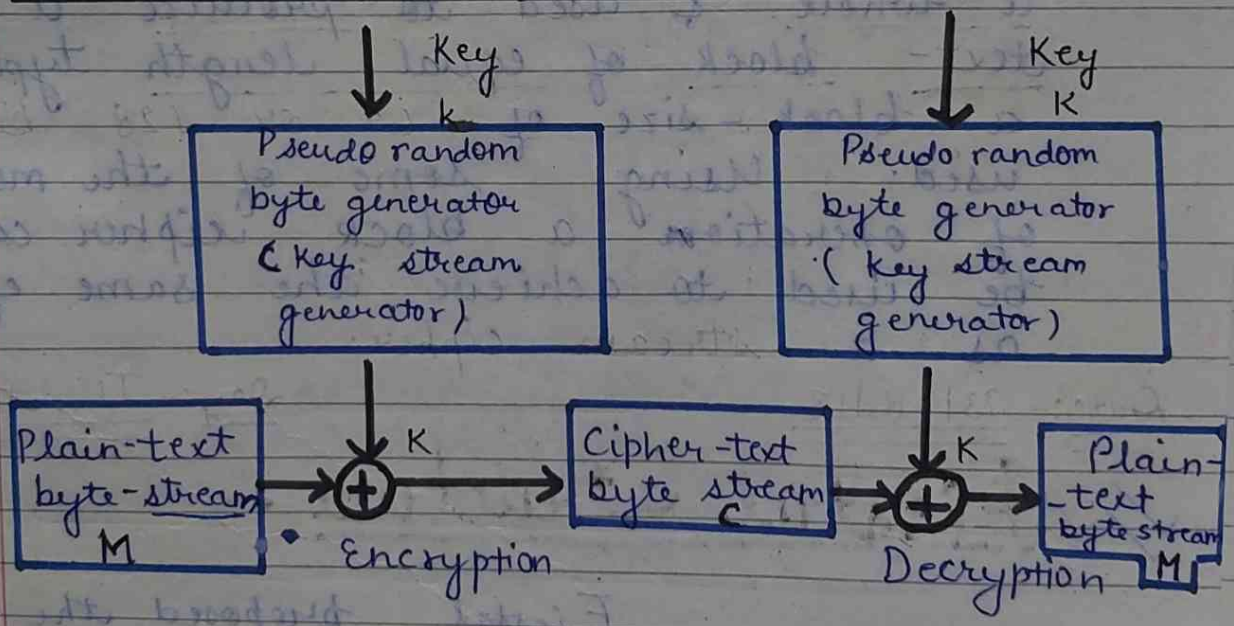
Date:- 17/08/18 Day: Friday

Stream Cipher :-

A stream cipher is one that encrypts a digital data stream one bit or one byte at a time. eg.

→ Vigenere Cipher
→ Vernam Cipher

Stream Cipher Structure:-



A Typical stream cipher encrypts plain-text one byte at a time although a stream cipher may be design to operate on one bit at a time or one-unit larger than a byte at a time. It is similar to the one time pad. The difference

is that one time pad uses are genuine random number stream whereas stream cipher uses a pseudo random stream.

Block - cipher principle :-

It is one in which a block of plain - text is treated as a whole & used to produce a cipher text- block of equal length typically a block - size of 64 or 128 bits used. Using some of the modes of operation a block cipher can be used to achieve the same effect as a stream cipher.

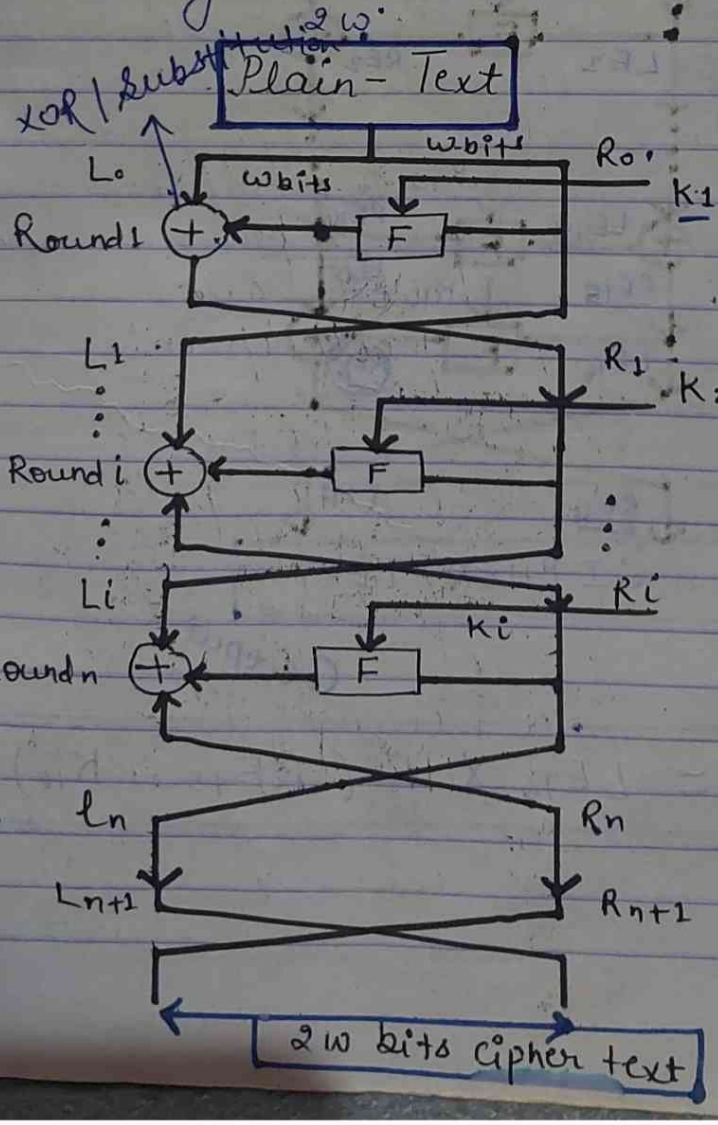
Date:- 23/08/18 Day:- Thursday

Fiestal Structure :-

Fiestal proposed the use of a cipher that alternates substitution & permutations. Infact, there is a practical application of a proposal by Claude Shanon to develop a product cipher that alternates. confusion & Diffusion functions. To capture the to basic-building block for any cryptographic

system.]]

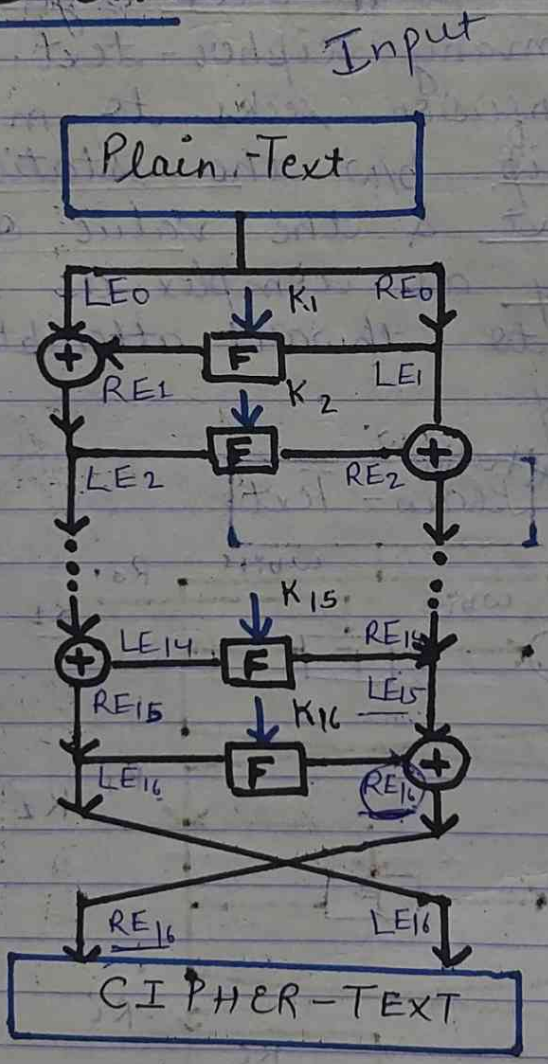
In Diffusion, the statistical structure of the plain-text is dissipated into long range statics of the cipher-text achieved by having each plain-text digit affect the value of many cipher-text. On the other hand, Confusion seeks to make the relationship b/w the statistics of the cipher-text & the value of the encry-ption key as complex as possible against to thwart attempts to discover the key.



Note:- The substitution is applied to the left side halves of the data.

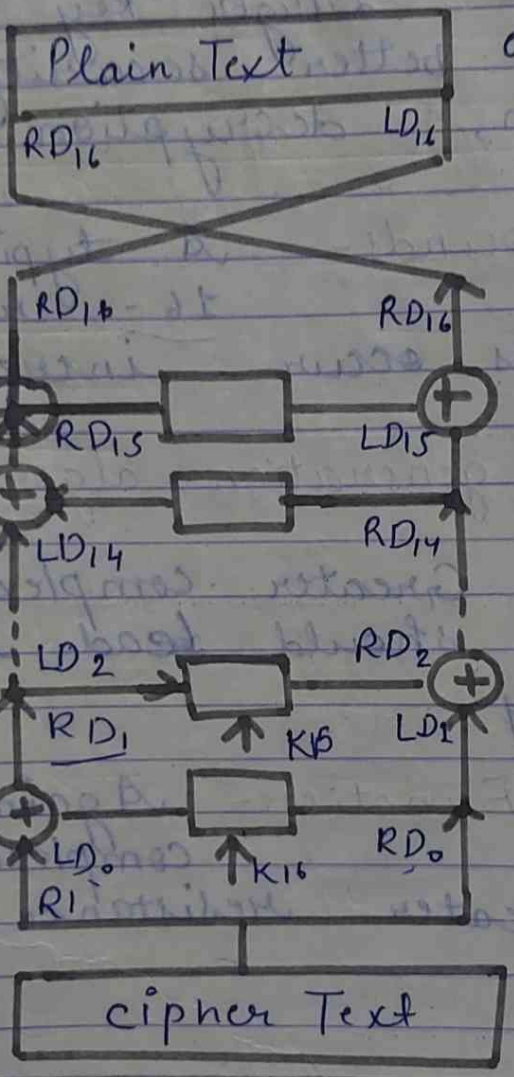
Date:- 24/08/18 Day:- Friday

Encryption :-



$$RE_{16} = LE_{15} \times F(RE_{15}, K_{16})$$

Decryption -



$$RD_1 = LD_0 \times F(RD_0, K_1)$$
$$= RE_{16} \times F(LE_{16}, K_1)$$

Fiestal network depends on the choice of the following parameters & design features -

Block - size - Larger the block-

- size, greater the security achieved by greater difussion.

Key - size - Larger key -size means better security but decrease encryption, decryption speed.

No. of rounds - A typical size is 16 - rounds, multiple rounds occur increasing security.

Sub - Key generation algorithm -

Greater complexity in the algorithm should lead to greater difficulty.

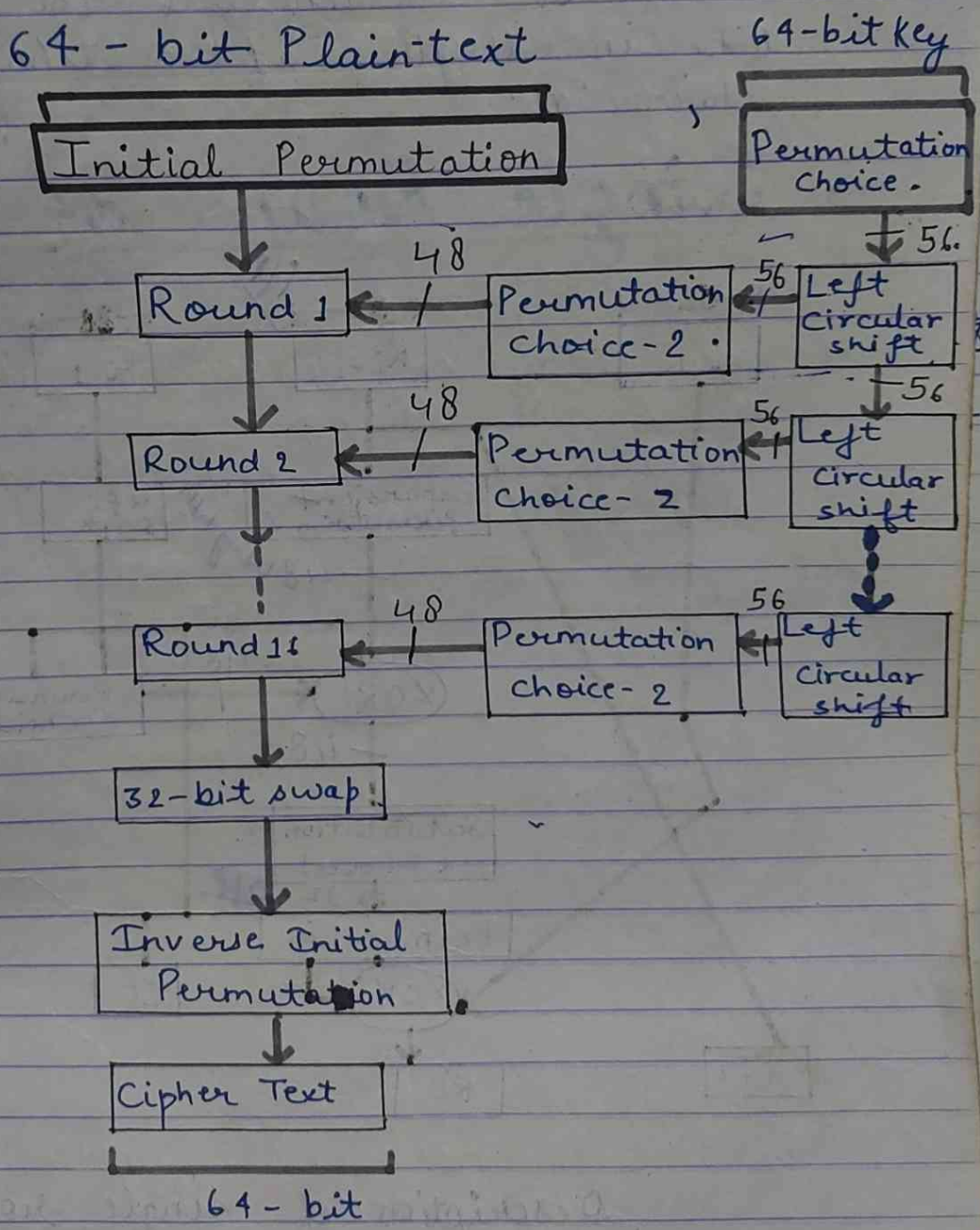
Round - Function - Again greater complexity generally needs greater resistance to crypt-analysis.

Date:- 25/08/18

Day:- Saturday

22

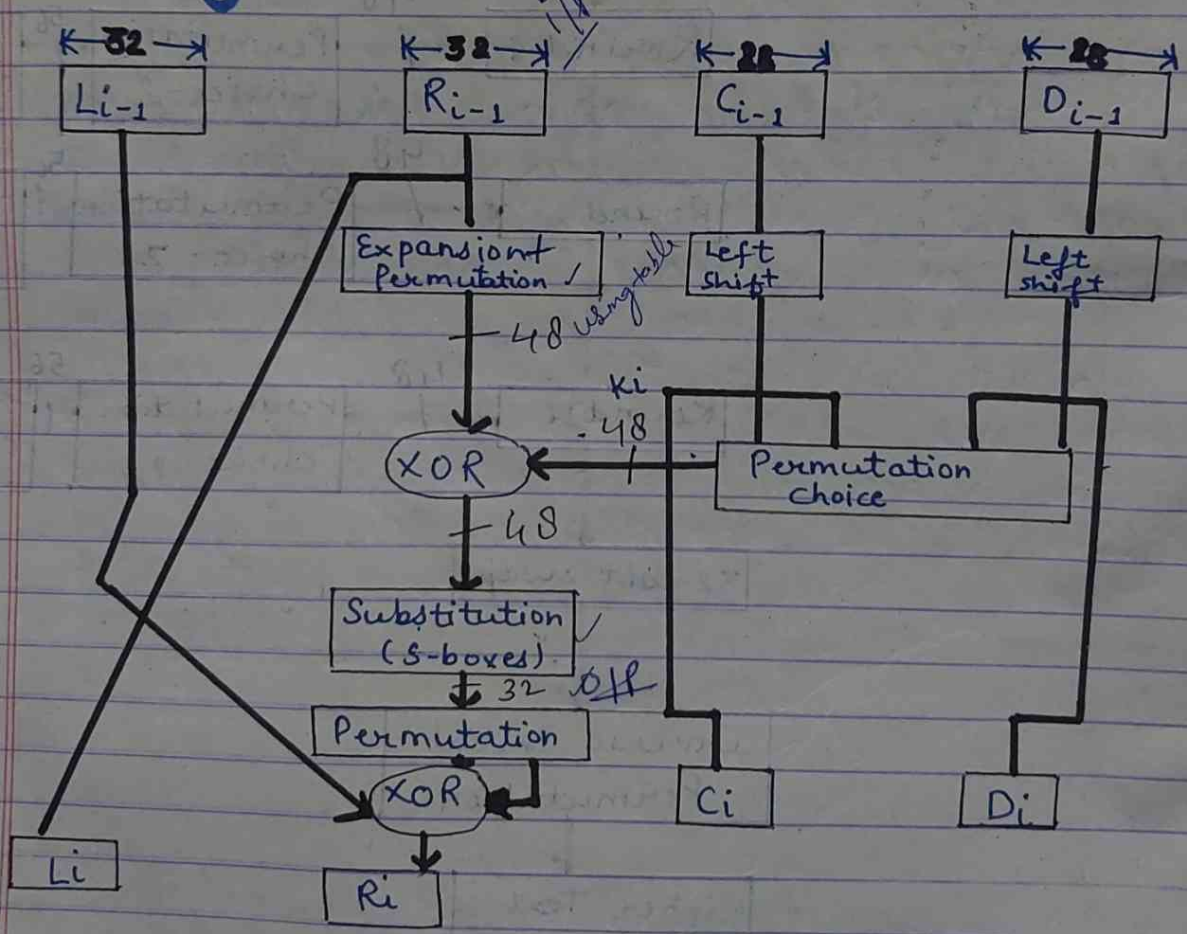
D.E.S. (Data Encryption Standard)



General Structure

There are two inputs in the encryption function - Plain text & Key. The plain-text must be 64-bit in length & the key is 56 bits in length after the permutation choice "1".

→ Single Round of D.E.S.-



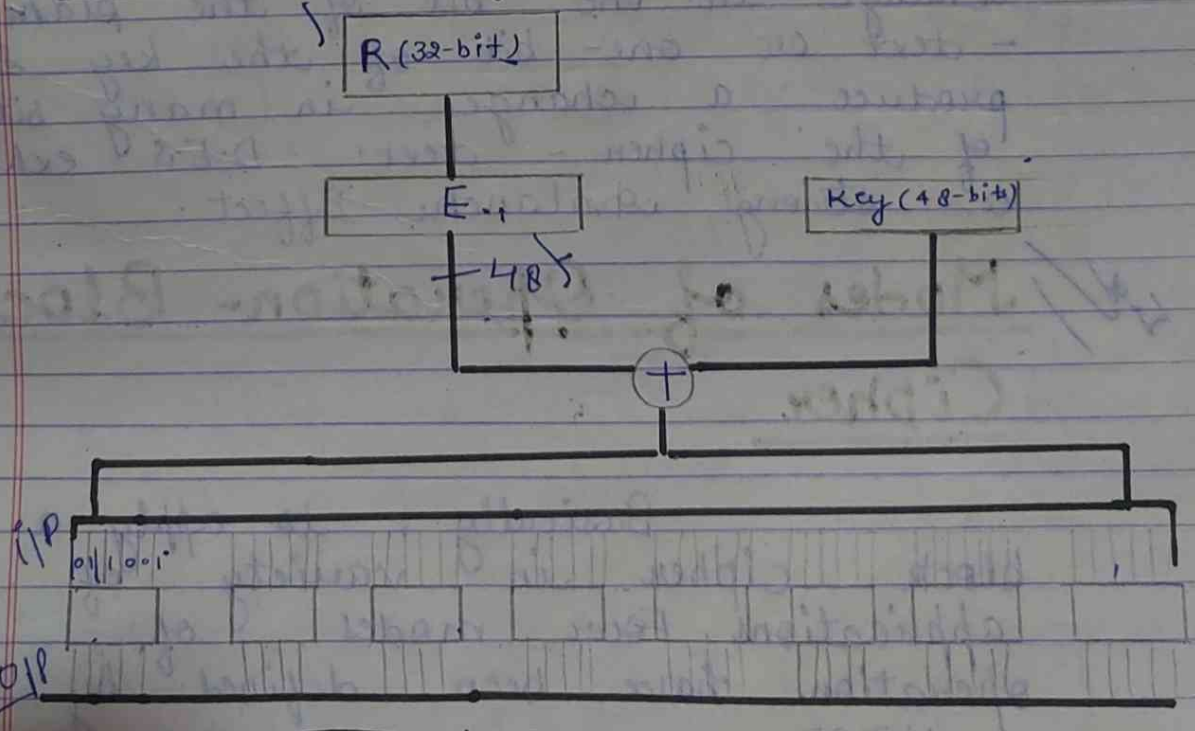
Description of single round of D.E.S.

Ki = The round key 48

The R- inputs is 32- bits which is first expanded to 48- bits by using a table that defines a permutation plus expansion that involves duplication of 16 of the R-bits. The resulting 48- -bits are XORed with 48- bits Ki which passed through a substitution function that produces a 32- bit output which is permuted. The role of the S- boxes is defined as the substitution consists of a set of 8-S-b- -oxes each of which accepts 6-bits as input & produces 4- bits as output

Date:- 27/08/18 Day:- Monday

⇒ S- boxes Representations :-



eg 011001 — row

01 - row

1100 ⇒ 12 ⇒ column

⇒ 9 = 1001 (Table)

12 Column

Date:- 29/08/18

Day:- Wednesday

25

D·E·S. Decryption :-

As with any fiestal ciph decryption uses the same algorithm as encryption except that the application of sub-keys is reversed.

Avalanche Effect :-

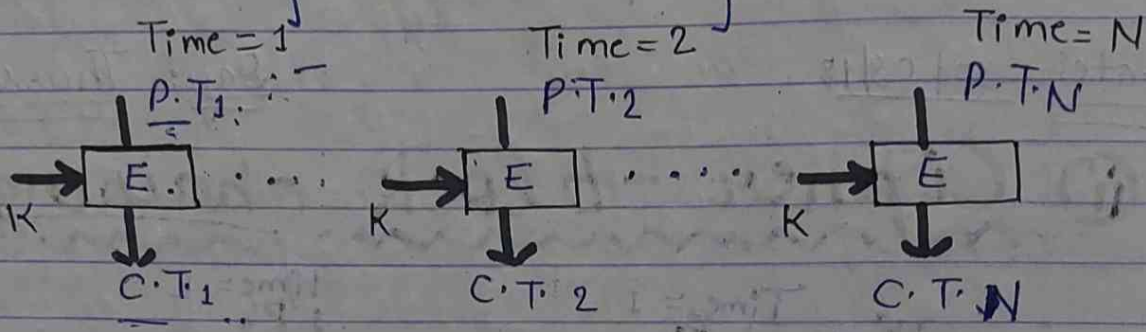
A desirable property of any encryption algorithm is that a small change in either the plain text or the key should produce the significant change in the cipher text. In particular, a change in one bit of the plain-text or one-bit of the key should produce a change in many bits of the cipher-text. D·E·S exhibits a strong Avalanche Effect.

Modes of Operation- Block Cipher

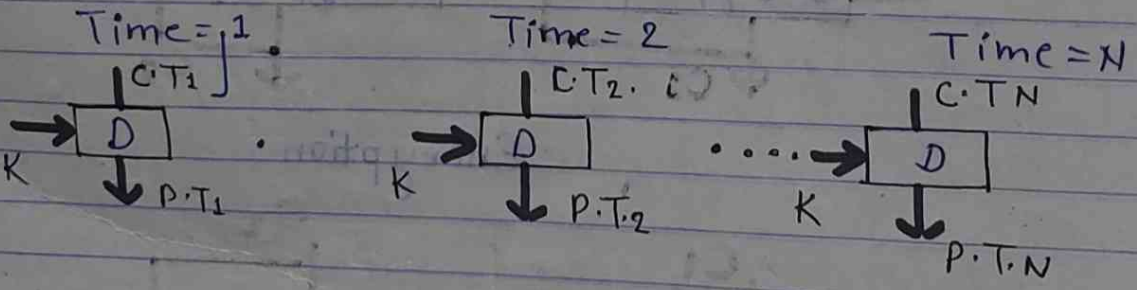
Basically, to apply a block cipher in variety of applications. Four modes of operation have been defined by NIST.

Later on, new applications & requirements have appear so modes of operations expanded to five by NIST-

(i) Electronic Codebook mode :-



Encryption



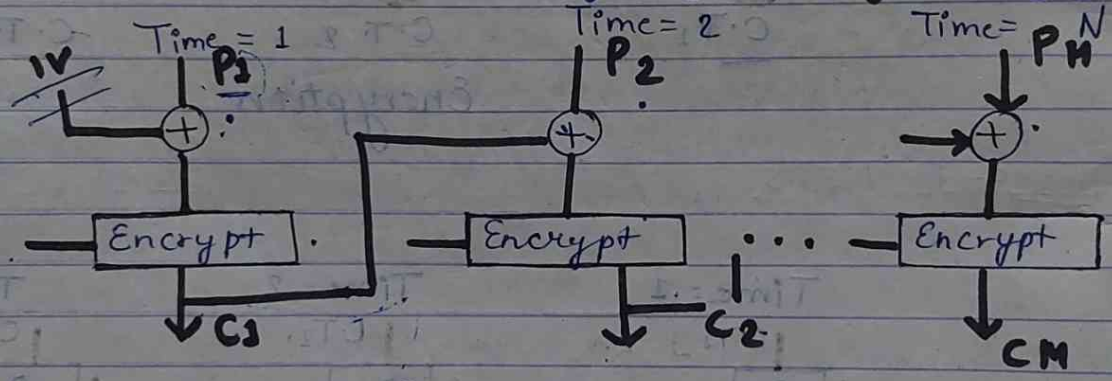
Decryption

Plain-text is handled one block at a time. Each block of plain-text is encrypted using the same key. It is called 'codebook' because for a given key there is a cipher-text for every ~~decrypt~~ b-bit block of cipher-text. Decryption is perform

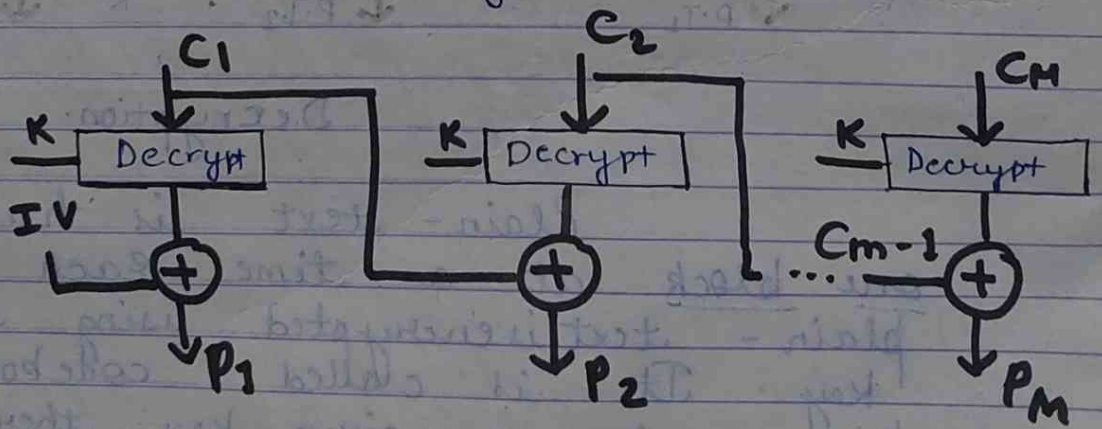
-ed similarly always using the same key.
It is ideal for short amount of data
- Encryption key.
To transmit D.E.S. key security E.C.B is the appropriate mode to use.

Date:- 30/08/18 Day:- Thursday

(ii) Cipher - block chaining mode-



Encryption.



In this same plain-text block if repeated produces different cipher-text-block.

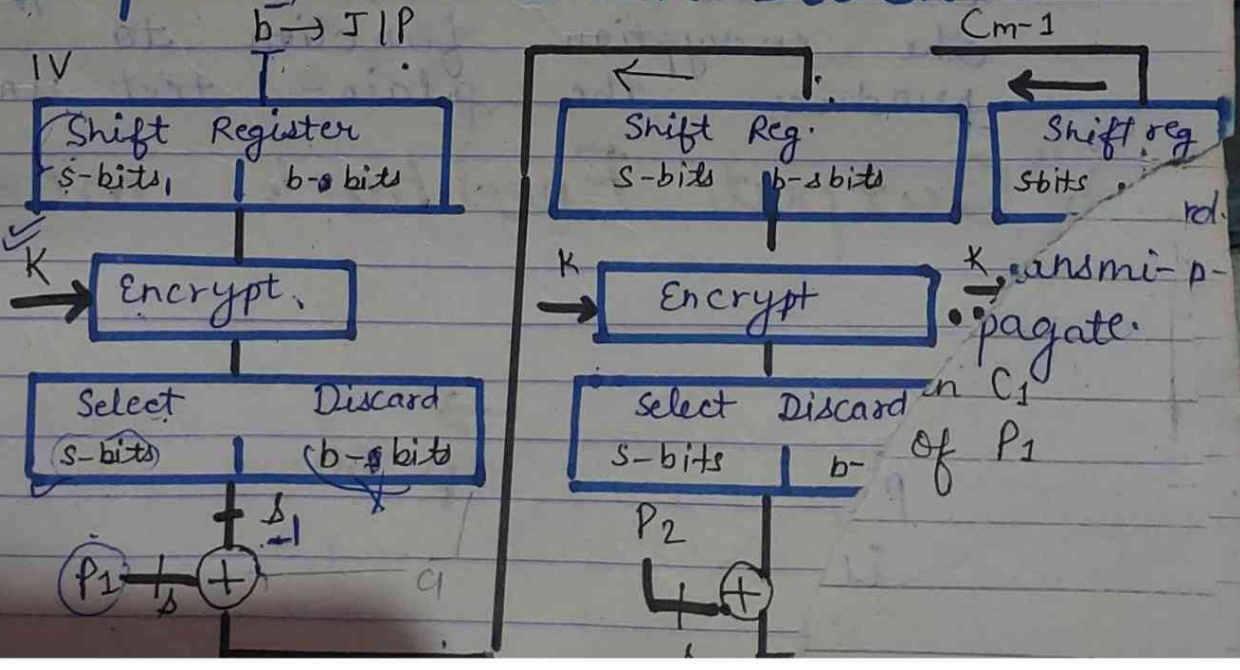
i/p ⇒ XOR of P.T.

In this method the input to the encryption algorithm is the XOR of the current plain-text block & the preceeding cipher-text block. The same key is used for each block. In decryption each cipher block is passed to the decryption algorithm. The result is XORed with the preceeding Cipher-text block to produce the plain-text block.

IV (Initialization Vector) -

It is a data-block i.e. of same size as the cipher--block. It must be known to both sender & receiver.

Cipher feedback block -



I/P ⇒ b-bit shift reg.

In the given fig. it is assume that the unit of transmiss-ion is s-bits. The common value s = 8

Encryption -

Input is b-bit shift-register initially set to IV left-most s-bits of the O/P of the encryption function are XORed with the first segment of the plain-text to produce the I^st unit of cipher-text which is then transmitted as a input to to the next block.

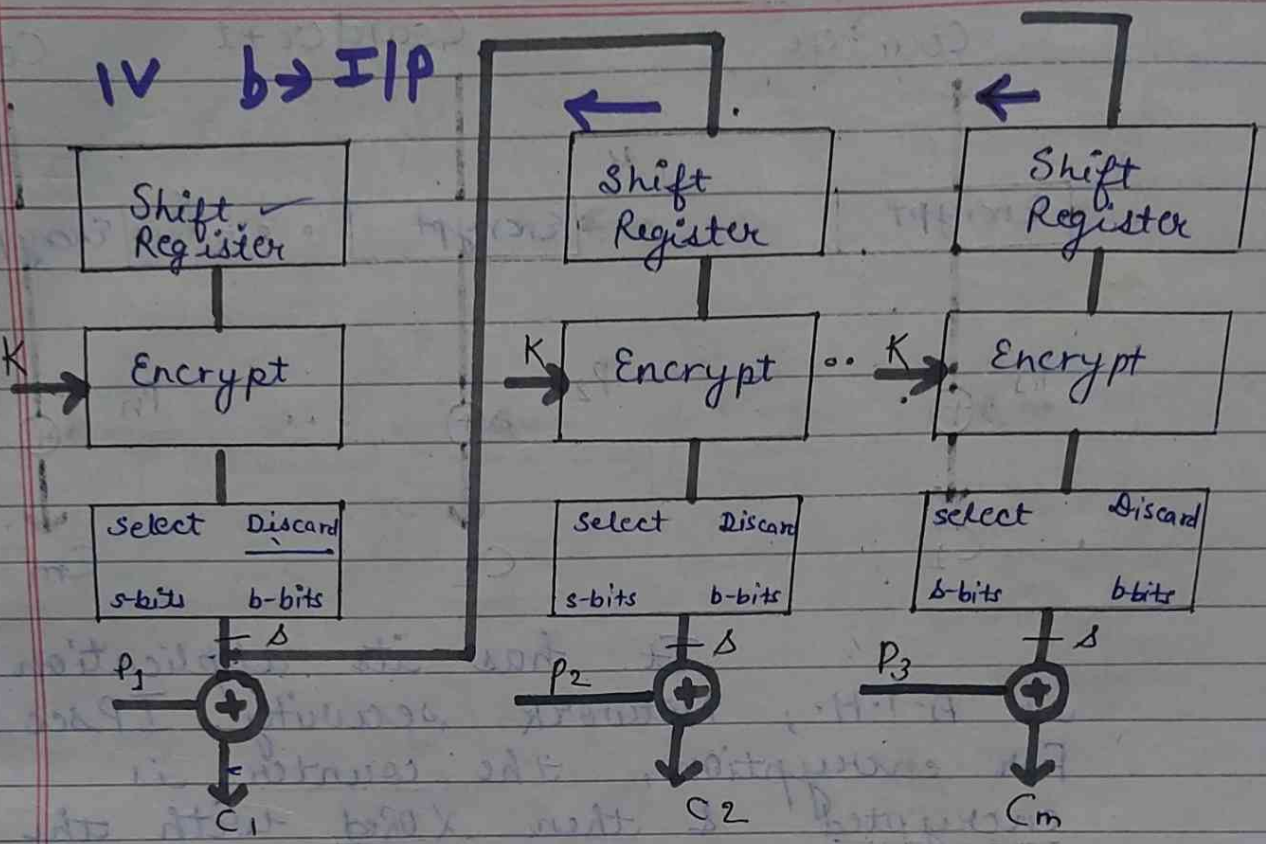
Decryption -

Same process is repeated except that the received cipher-text unit is XORed the O/P of the encryption function to produce the plain-text unit.

iv) Output Feedback mode :-

- tex
differ

→ P.T.O



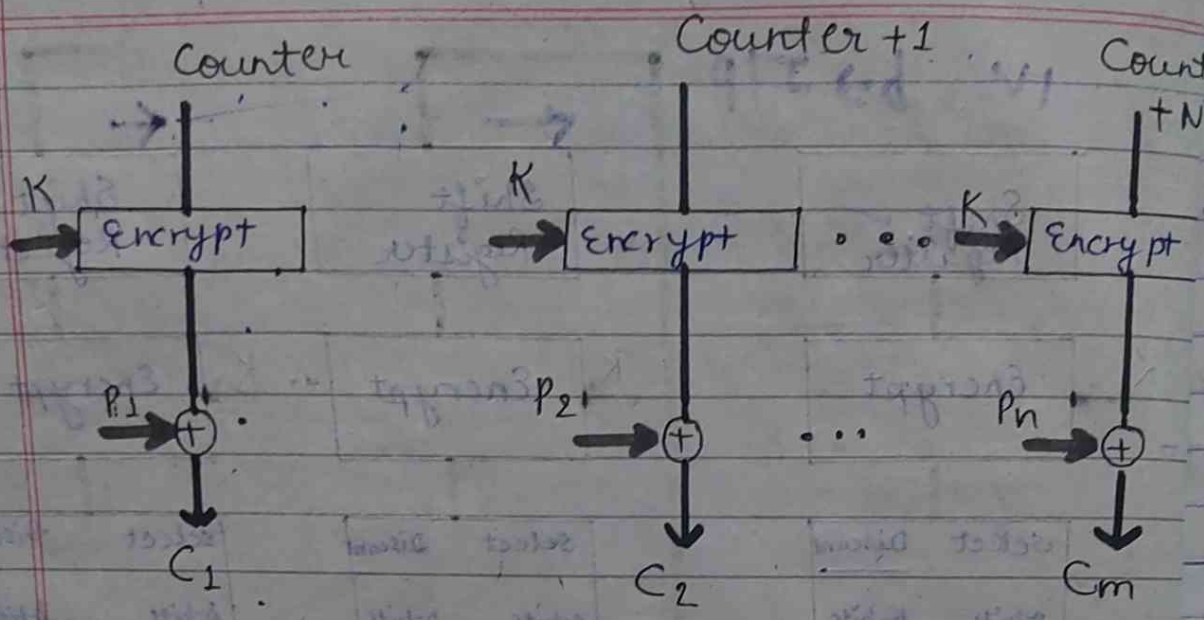
This is the output of the encryption function i.e. feedback to the shift register in output feed back mode. There is a cipher-text whit is feedb--ack to the shift-register.

Advantage:-

Big Errors in transmi--ssion do not propagate.

for eg: In a big-error occurs in C_1 only the recovered value of P_1 is effected.

v) Counter mode-



It has its application in A.T.M., Network security, IPsec. For encryption, the counter is encrypted & then XORed with the plain-text block to produce the cipher-text block there is no chaining. for decryption, the same sequence of counter-values is used with each-encrypted counter XORed with a cipher-te block to recover the correspondin plain-text block.

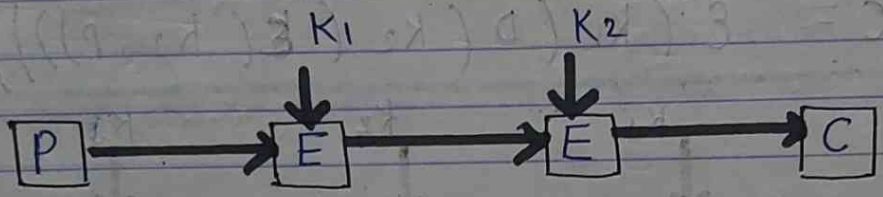
Double D.E.S-

Given a plain-text P & key K_1, K_2, cipher-text is represented as-

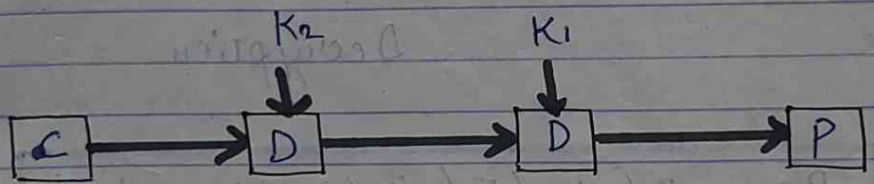
$$C = E(K_2(E(K_1, P)))$$

Decryption requires the keys in reverse.

$$P = D(K_1(D(K_2, C)))$$



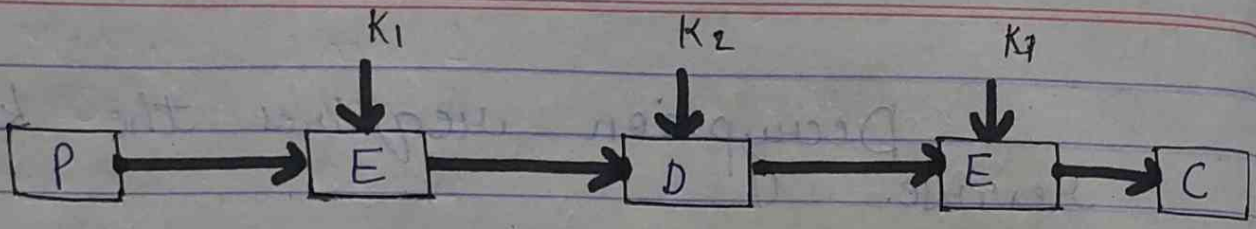
Encryption



Decryption

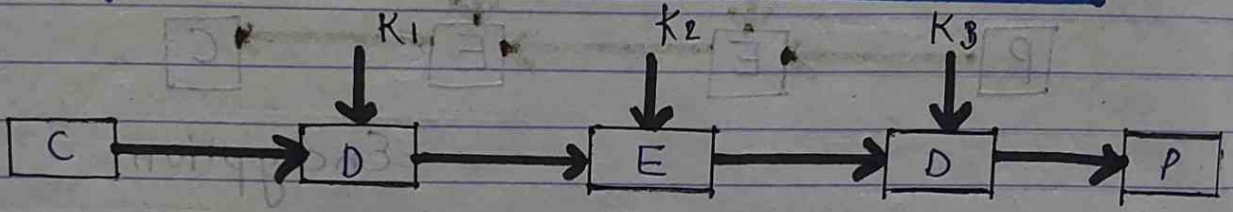
Triple D.E.S.

3-D.E.S. with two keys is a relatively popular alternative to D.E.S. & has been adopted for use. In the key management standard Tuchman proposed a triple encryption method that uses only two keys follows-Encrypt- decrypt- encrypt sequence.



Encryption

$$C = E(K_1(D(K_2(E(K_1, P)))))$$



Decryption

$$P = D(K_1(E(K_2(D(K_1, C)))))$$

Strength of D.E.S.

① The use of 56-bit keys.
② The nature of algo.
③ Timing attack.

Weakness of D.E.S.

① Weakness in Cipher-Design - (i) S-Boxes
(ii) D-Boxes

② Weakness in Cipher-Key - (i) Key Size
(ii) Weak keys

Unit-2 A.E.S.

Date:- 07/09/18 Day:- Friday

Euclidean algorithm :-

1. $A \leftarrow a$, $B \leftarrow b$
2. while $B > 0$
   $A = B \times Q + R$ $\Rightarrow$ $(R = A \bmod B)$
   $A \leftarrow B$, $B \leftarrow R$
3. $gcd(a, b) \leftarrow A$

Ques:1 Find gcd (1970, 1066)
(a = 1970, b = 1066)

$a = 1970$
$b = 1066$
$B > 0$

$1970 = 1066 \times 1 + 904$
$1066 = 904 \times 1 + 162$
$904 = 162 \times 5 + 94$
$162 = 94 \times 1 + 68$
$94 = 68 \times 1 + 26$
$68 = 26 \times 2 + 16$
$26 = 16 \times 1 + 10$
$16 = 6 \times 1 + 4$
$10 = 4 \times 1 + 2$
$6 = 2 * 2 + 0$
$4 = 0$

gcd (1970, 1066) = 2

Extended Euclidean Algorithm *

1. $r_1 \leftarrow a$, $r_2 \leftarrow b$
   $s_1 \leftarrow 1$, $s_2 \leftarrow 0$
   $t_1 \leftarrow 0$, $t_2 \leftarrow 1$
2. while $(r_2 > 0)$
   $q = r_1 / r_2$
   $r \leftarrow r_1 - (q \times r_2)$
   $r_1 \leftarrow r_2$, $r_2 \leftarrow r$
   $s \leftarrow s_1 - (q \times s_2)$
   $s_1 \leftarrow s_2$, $s_2 \leftarrow s$
   $t \leftarrow t_1 - (q \times t_2)$
   $t_1 \leftarrow t_2$, $t_2 \leftarrow t$
3. gcd $(a, b) \leftarrow r_1$
   $s \leftarrow s_1$
   $t \leftarrow t_1$

$27 \times y_1 = 1 \bmod n$

$r \leftarrow r_1 - (q \times r_2)$
$r_1 \leftarrow r_2$, $r_2 \leftarrow r$

$s \leftarrow s_1 - (q \times s_2)$
$1 - (5 \times 0) = 1$

$t \leftarrow t_1 - (q \times t_2)$

Que a = 161, b = 28

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
5	161	28	21	1	0	1	0	1	-5
1	28	21	7	0	1	-1	1		
3	21	7	0						
	7	0							
	⑦								
	gcd = 7			-1			6		

$(s_1 \times r_1) + (t_1 \times r_2)$
$(-1 \times 161) + (6 \times 28)$
$-161 + 168 = 7$ Ans

Date:- 10/09/18 Day:- Monday

Chinese-Remainder Theorem-

It is used to solve simultaneous equations. It gives a unique solution to simultaneous equations with co-prime modelling.

It determine a no. that when divided by some given by some divisors leaves given remainder having the same remainders when divided by a specified integer.

Qu.1. imp | $x = 1 \bmod P$ ∀ , P(2, 3, 5, 7)

$$\left.\begin{aligned} x &= 1^{a_1} \bmod 2 \\ x &= 1^{a_2} \bmod 3 \\ x &= 1^{a_3} \bmod 5 \\ x &= 1^{a_4} \bmod 7 \end{aligned}\right\} \begin{matrix} m_1 \\ m_2 \\ m_3 \\ m_4 \end{matrix}$$

$M = m_1 \times m_2 \times m_3 \times m_4$

$= 2 \times 3 \times 5 \times 7 = 210$

$M_1 = \frac{M}{m_1} = \frac{210}{2} = 105$

$M_2 = \frac{M}{m_2} = \frac{210}{3} = 70$

$M_3 = \frac{M}{m_3} = \frac{210}{5} = 42$

$M_4 = \frac{M}{m_4} = \frac{210}{7} = 30$

M_5.

210 | 421 | 2
420
1

105
70
126
120
6

42
x 3
126

37

$M_1 y_1 = 1 \bmod 2$
$105\, y_1 = 1 \bmod 2$
$1 \cdot y_1 = 1 \bmod 2$

$\boxed{y_1 = 1}$

$M_2 y_2 = 1 \bmod 3$
$70\, y_2 = 1 \bmod 3$
$1 \cdot y_2 = 1 \bmod 3$

$\boxed{y_2 = 1}$

$M_3 y_3 = 1 \bmod 5$
$42\, y_3 = 1 \bmod 5$
$3 \cdot 2 \cdot y_3 = 3 \cdot 1 \bmod 5$
$6\, y_3 = 3 \bmod 5$

$\boxed{y_3 = 3}$

$M_4 y_4 = 1 \bmod 7$
$30\, y_4 = 1 \bmod 7$
$4 \cdot 2\, y_4 = 4 \cdot 1 \bmod 7$

$\boxed{y_4 = 4}$

$x = (a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 + a_4 M_4 y_4) \bmod M$

$= (1 \times 105 \times 1 + 1 \times 70 \times 1 + 42 \times 3 \times 1 + 1 \times 30 \times 4) \bmod 210$

$= 421 \bmod 210$

$= 1$ Ans

Applications:

(a) CRT can also be used to solve quadratic congruence

(b) Used to represent a very large integer interms of a list of small integers

H.W Ques. $x = 2 \bmod 3$
$x = 3 \bmod 5$
$x = 2 \bmod 7$

Homework

Ques. use these values in last question

$x = 2 \bmod 3 \rightarrow m_1$
$x = 3 \bmod 5 \rightarrow m_2$
$x = 2 \bmod 7 \rightarrow m_3$

$M = m_1 \times m_2 \times m_3$
$= 3 \times 5 \times 7 = 105$

$M_1 = \frac{M}{m_1} = \frac{105}{3} = 35$

$M_2 = \frac{M}{m_2} = \frac{105}{5} = 21$

$M_3 = \frac{M}{m_3} = \frac{105}{7} = 15$

$M_1 y_1 = 1 \bmod 3$
$35\, y_1 = 2 \bmod 3$
$2 \cdot y_1 = 2 \cdot 1 \bmod 3$

$\boxed{y_1 = 2}$

$M_2 y_2 = 1 \bmod 5$
$21\, y_2 = 3 \bmod 5$
$1 \cdot y_2 = 3 \bmod 5$

$\boxed{y_2 = 3/1}$

$M_3 y_3 = 1 \bmod 7$
$15\, y_3 = 2 \bmod 7$
$1 \cdot y_3 = 2 \bmod 7$

$\boxed{y_3 = 2}$

$\Rightarrow x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3$

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

$x = 106 \bmod 105$

$\boxed{x = 1}$ Ans

361, 561, 61, 27

Day:- Tuesday

Date:- 11/09/18

→ Algorithm to find the mod in the form of $a^y \bmod n$

$\Rightarrow a^y \bmod n$

$\Rightarrow 17^{22} \bmod 21$

$= 4$

Algorithm -

```
y ← 1
{
for (i ← 0 to n_b - 1)        // n_b → no. of bits in x_i
{
if (x_i = 1)
  y ← a x y mod n
a ← a^2 mod n                 // → not calculated in last iteration
}
else
a ← a^2 mod n
}
return y
}
```

2	22	0
2	11	1
2	5	1
2	2	0
	1	

a

Sol^n

i	x_i	$y \leftarrow a \times y \bmod n$	a
0	0	$y = 16 \times 1 \bmod 21 = 16$	$a = 17^2 \bmod 21 = 16$
1	1	$y = 16 \times 4 \bmod 21 = 1$	$a = 16^2 \bmod 21 = 4$
2	1		$a = 4^2 \bmod 21 = 16$
3	0		$a = 16^2 \bmod 21 = 4$
4	1	$y = 1 \times 4 \bmod 21 = 4$	

Date:- 17/09/18 Day:- Monday

→ Miller Rabin's Test – for primality test

1. $n-1 = 2^k \cdot m$ (m = odd no.) → as eg.
2. Choose $1 < a < n-1$ [$a = 2$]
3. $b_0 = a^m \bmod n \Rightarrow b_0 = +1, -1$ } Probably Prime

if $k = 1$

Then no. is composite.

else *for ($i = 1 \leftarrow k-1$)

$b_1 = b_0^2 \bmod n$

$b_1 = +1 \rightarrow$ composite no.

$b_1 = -1 \rightarrow$ Prime no.

Ex.

$n = 53$

Step-1 $n-1 = 53-1 = 52$

$n-1 = 2^k \cdot m$

$53-1 = 2^2 \cdot 13$

2	52
2	26
2	13

$52 = 2 \times 2 \times 13 = 52$

$K = 2$

जहाँ पर 0 आता है, no calculation जहाँ पर 1 आता है वहाँ $a \times y \bmod n$ आता है।

Step2 $a = 2$

Step3 $b_0 = a^m \bmod n$

$b_0 = 2^{13} \cdot \bmod 53$

$b_0 = ?$

2	13	1
2	6	0
2	3	1
2	1	1

$a^y \bmod n$

$2^{13} \cdot \bmod 53$

initially $y = 1$

S.No	x_i	$2 \times 1^y \bmod 53$	a
1.	1	$a \times y \bmod n = 2$	$a \leftarrow a^2 \bmod n = 4 \bmod 53 = 4$
2.	0	$\cdot 2 \cdot$	$a \leftarrow 4^2 \bmod 53 = 16$
3.	1	$16 \times 2 \bmod 53 = 32$	$a \leftarrow 16^2 \bmod 53 = 44$
4.	1	$32 \times 44 \bmod 53 = 30$	$a \leftarrow 32^2 \bmod 53 = 17$

$b_0 = 30$

$K = 2$

So, $b_1 = b_0^2 \bmod n$

$b_1 = (30)^2 \bmod 53$

$b_1 = 900 \bmod 53$

$b_1 = -1$

Since, $b_1 = -1$ so, it is Prime no.

```
      17
53 ) 900 (
     53
    ---
    370
    424
    ---
     46
      17
53 ) 900
     53
    ---
    370
    371
    ---
     -1
```

eg:- $n = 27$

Sol^n $n-1 = 2^K \cdot m$

$27-1 = 2^1 \cdot 13$

$26 = 26$

$\boxed{K=1}$, $\boxed{a=2}$

$b_0 = a^m \bmod n$

$= 2^{13} \bmod 27$

S.No.	x_i	y	a
0.	1	$2 \times 1 \bmod 27 = 2$	$a \leftarrow 4 \bmod 27 = 4$
1.	0	2	$a \leftarrow 16 \bmod 27 = 16$
2.	1	$16 \times 2 \bmod 27 = 5$	$a \leftarrow 256 \bmod 27 = 13$
3.	1	$13 \times 5 \bmod 27 = (11)$ ↓ b_0	$a \leftarrow 169 \bmod 27 = 7$

$b_i = (b_0)^2 \bmod n$

$b_1 = (11)^2 \bmod (27)$

$b_1 = 13$

$b_2 = (b_1)^2 \bmod (n)$

$b_2 = (13)^2 \bmod 27$

$b_2 = 7$

$b_3 = (7)^2 \bmod 27$

$= 22$

CS = 361 Assignment - 2 Day:- Monday

Date:- 17/09/18 Homework

Ques:1 Perform Primarity test by Miller Rabin Test method for the given two numbers.

(i) n=21

Step:1 $n-1 = 2^k \cdot m$

$21-1 = 2^2 \cdot 5$.

$20 = 20$

$\boxed{m=5}$, $\boxed{K=2}$.

Step:2 Choose , $a=2$

Step3 $b_0 = a^m \bmod n$

$b_0 = 2^5 \bmod 21$

$b_0 = 32 \bmod 21$

$b_0 = 11$

So, $b_1 = (b_0)^2 \bmod n$

$b_1 = (11)^2 \bmod 21$

$b_1 = 121 \bmod 21$

$b_1 = 16$

$b_2 = (16)^2 \bmod 21$

$b_2 = 256 \bmod 21$

$b_2 = 4$

$b_3 = (4)^2 \bmod 21$

$b_3 = 16 \bmod 21$

$b_3 = 16$

(ii) $n = 61$

Step-1

$n - 1 = 2^k \cdot m$

$61 - 1 = 2^2 \cdot 15$

$60 = 60$

$K = 2$, $a = 2$.

Step-2

$b_0 = a^m \bmod n$

$b_0 = 2^{15} \bmod 61$

$b_0 \Rightarrow$

S.No.	x_i	$y \leftarrow a \cdot y \bmod n$	$a \leftarrow a^2 \bmod n$
0.	1	$2 \times 1 \bmod 61 = 2$	$a \leftarrow 4 \bmod 61 = 4$
1.	1	$4 \times 2 \bmod 61 = 8$	$a \leftarrow 16 \bmod 61 = 16$
2.	1	$16 \times 8 \bmod 61 = 6$	$a \leftarrow 256 \bmod 61 = 12$
3.	1	$12 \times 6 \bmod 61 = 11$	$a \leftarrow 144 \bmod 61 = 22$

Step-3

$b_0 = a^m \bmod n$

$b_0 = 2^{15} \bmod 61$

$\Downarrow$

$b_1 = (b_0)^2 \bmod n$

$b_1 = (11)^2 \bmod (61)$

$b_1 = -1$

Since, $b_1 = -1$, so, 61 is Prime

Ques.2 $x = 2 \bmod 3$
$x = 3 \bmod 5$
$x = 2 \bmod 7$

Solve these equations by Chinese Remainder theorem.

Soln.

Step 1

$x = 1 \bmod P$, $a_1 = 2$, $a_2 = 3$, $a_3 = 2$

$M = m_1 \times m_2 \times m_3$

$M = 3 \times 5 \times 7$

$M = 105$

$$M_1 = \frac{M}{m_1} = \frac{105}{3} = 35$$

$$M_2 = \frac{M}{m_2} = \frac{105}{5} = 21$$

$$M_3 = \frac{M}{m_3} = \frac{105}{7} = 15$$

$M_1 y_1 = 1 \bmod 3$
$35\, y_1 = 1 \bmod 3$
$2 \cdot 2\, y_1 = 2 \cdot 1 \bmod 3$
$\boxed{y_1 = 2}$

$M_2 y_2 = 1 \bmod 5$

$21\ y_2 = 1 \bmod 5$

$\boxed{y_2 = 1}$

$M_3 y_3 = 1 \bmod 7$

$15\ y_3 = 1 \bmod 7$

$\boxed{y_3 = 1}$

$x = (a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3) \bmod M$

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

$x = (70 + 63 + 15) \bmod 105$

$x = 148 \bmod 105$

$\boxed{x = 23}$

$8 = 2 \bmod 3$

Verification -

$23 = \underline{2} \bmod 3$ · Verified

$23 = \underline{3} \bmod 5$ verified

$23 = \underline{2} \bmod 7$ verified

Date:- 17/09/18 Day:- Monday

C.N.S. Assignment -1

Ques-1 Find the following- using C.R.T.

* $x = 1 \bmod 7$
$x = 2 \bmod 5$
$x = 4 \bmod 3$

Soln

Step-1.

$x = 1 \bmod P$

$M = m_1 \times m_2 \times m_3$

$M = 7 \times 5 \times 3$

$M = 105$

$M_1 = \frac{M}{m_1} = \frac{105}{7} = 15$

$M_2 = \frac{M}{m_2} = \frac{105}{5} = 21$

$M_3 = \frac{M}{m_3} = \frac{105}{3} = 35$

$M_1 y_1 = 1 \bmod 7$
$15\, y_1 = 1 \bmod 7$
$y_1 = 1$

$M_2 y_2 = 1 \bmod 5$
$21\, y_2 = 1 \bmod 5$
$y_2 = 1$

$M_3 y_3 = 1 \bmod 3$
$3.5 y_3 = 1 \bmod 3$

$y_3 = 2$

$x = (a_1 y_1 M_1 + a_2 M_2 y_2 + a_3 M_3 y_3) \bmod M$

$x = (233) \bmod 105$

$x = 23$

All conditions are verified.

Ques 2 Explain 'Cryptanalysis' in detail.

Soln.

CRYPTANALYSIS

Introduction

Cryptanalysis is the study of ciphertext, ciphers & cryptosystems with the aim of understanding how they work & finding & improving techniques for defeating or weakening them. for eg.

Cryptanalysts seek to decrypt ciphertexts without knowledge of the plain-text source, encryption key or the algorithm used to encrypt it; It also target source hashing, digital signatures & other cryptographic algorithms.

Cryptanalysis is the art of trying to decrypt the encrypted message without the use of the key that was used to encrypt the messages. It uses mathematical analysis & algorithms to decipher the ciphers. The success of cryptanalysis attack depends -

- Amount of time available.
- Computing power available.
- Storage Capacity available.

TYPES of CRYPTANALYSIS

(i) Differential Cryptanalysis
(ii) Linear Cryptanalysis

(i) Differential Cryptanalysis

This attack is very complex. The overall strategy of it's is - based on single round.

The procedure is begin with two plain-text messages M & M' with a given difference & trace through a probable pattern or difference after each round for the cipher-text.

Equation is -

$$M_{i+1} = M_{i-1} \text{ XOR } f(M_i, K_i)$$

(ii) Linear Encryption cryptanalysis -

It is a more recent development. This attack is based on finding linear approximation to describe the transformation performed in D.E.S.

This method can find a D.E.S key given 2^{47} known-plain-text. As compare to 2^{47} chosen plain-text for differential cryptanalysis, although this is a minor development because it may be easy to acquire known plain-text rather than chosen plain-text. So, the linear cryptanalysis is infeasible as an attack on D.E.S.

For a cipher with n-bit plain-text & cipher-text blocks & m-bit keys so the plain-text block will be a set of -

$$P = P[1], P[2], P[3] \ldots\ldots, P[n]$$

& the cipher-text will be a set of -

$$C = C[1], C[2], C[3] \ldots, C[n]$$

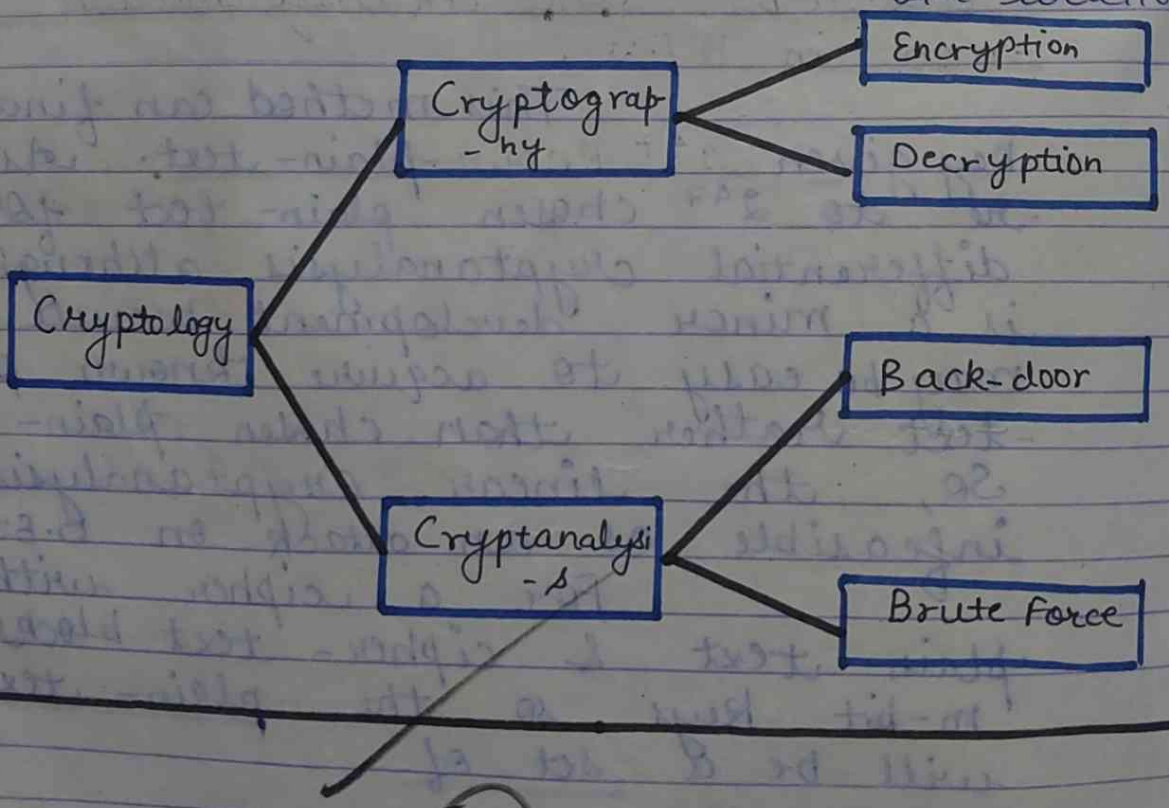
& the set of key will be -

$K = K[1], K[2], K[3] \ldots K[m]$

So, the effective linear equation in the form of -

$$P[\alpha_1, \alpha_2, \alpha_3 \ldots \alpha_n] \text{ XOR } C[\beta_1, \beta_2, \beta_3 \ldots \beta_n] = K[\alpha_1, \alpha_2, \alpha_3 \ldots \alpha_m]$$

α, β & α = unique bit location



10

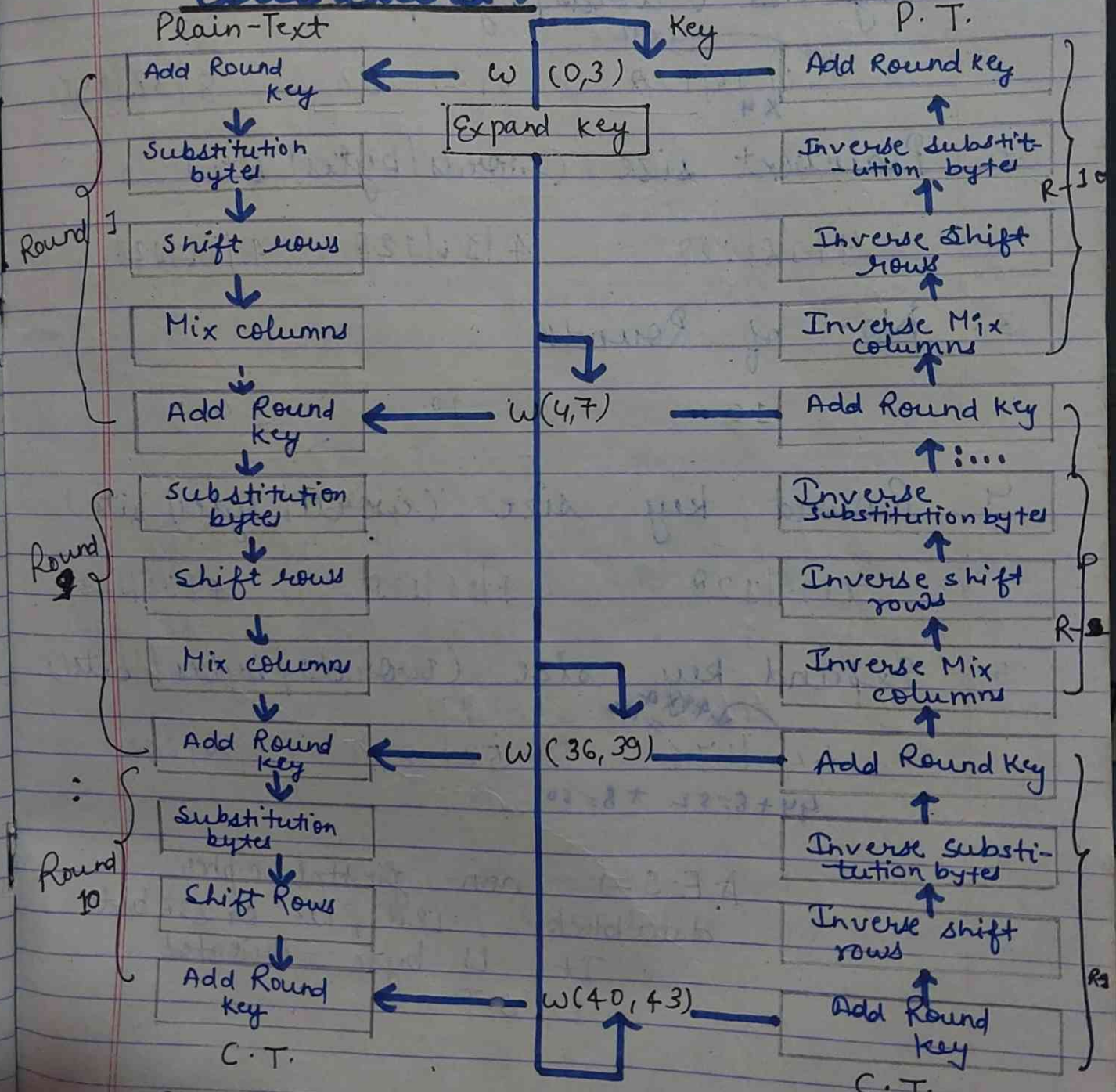
18/9

Date:- 18/09/18 Day:- Tuesday

Block-cipher-length - 128 bits

43

A.E.S. (Advance Encryption Standard)



Parameters -

1. Key size (words / bytes / bits):

4 / 16 / 128 (×4, ×32) 6 / 24 / 192 8 / 32 / 256

2. Plaintext size (words / bytes / bits)

4 / 16 / 128 4 / 16 / 128 4 / 16 / 128

3. No. of Rounds

10 12 14

4. Round key size (words / bytes / bits)

4 / 16 / 128 4 / 16 / 128 4 / 16 / 128

5. Expand key size (words / bytes / bits)

44 / 176 (4 × 44 = 176) 52 / 208 60 / 240

44 + 8 = 52 + 8 = 60

A.E.S ⇒ non-fiestal cipher

data-block - 128, 192 or 256 bit

It is byte-oriented

1 B.T. =

Date :- 19/09/18 Day :- Wednesday

Fermat's Theorem -

It states that if p is prime no. & a is a (+ve) integer not divisible by - P

$$a^{p-1} \equiv 1 \bmod P$$

Proof -

Consider the set of +ve integer & multiply each element by a.

$$X = a, 2a, \ldots a(P-1)$$

None of the element of $X = 0$ because p does not divide a. No two of integers in X are equal. To see that, assume that

$$ja = Ka \pmod p$$

$$\boxed{1 \leq j < K \leq p-1}$$

a is relative prime to p, so we can eliminate 'a' from both sides of eqn a -

$$j \equiv K \pmod p$$

This equality is impossible because j & k are both positive

integer less than p. So, we can conclude X consist of set of +ve integer - {1, 2, ... p-1}

$a \times 2a \times \ldots a(p-1) \equiv (1 \times 2 \times \ldots (p-1)) \bmod p$

$a^{p-1}(p-1)! \equiv (p-1)! \bmod p$

$\Rightarrow \boxed{a^{p-1} \equiv 1 \bmod p}$

Or alternative form

$\boxed{a^p \equiv a \bmod p}$

eg: if $a = 2$, $p = 17$

$2^{17-1} \equiv 1 \bmod 17$

$2^{16} \equiv 1 \bmod 17$

Euler's Theorem -

It states that for every a & n that are relatively prime -

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

Proof :-

$\phi(n)$ = no. of +ve integers $< n$ that are relatively prime to n

consider the set of such integers as follows -

$$R = \{ x_1, x_2 \ldots x_{\phi(n)} \}$$

Each element x_i of R is a unique +ve integer less than n with $\gcd(x_i, n) = 1$, $1 \leq x_i < n$

$\phi(1) = 1$

Now, multiply each element by a

$$S = \{ ax_1, ax_2 \ldots ax_{\phi(n)} \}$$

- The set S is a permutation of R because if a is relatively prime to n, x_i is also relative prime to n. Thus, all the members of S are integers that are less than n & are relatively prime to n.

There are no duplicates in S.

$\Rightarrow a x_i \bmod n = a x_j \bmod n$

$$x_i = x_j$$

Therefore,

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

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

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

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

Euler's Totient Function-

$\phi(n)$ define as the no. of +ve integers less than n & relatively prime to n for $n = p \times q$.

$$\phi(n) = \phi(pq)$$
$$= (p-1) \times (q-1)$$

Consider the set of +ve integers is the set less than

20

1, 3, 5, 7, 11, 13,

$X = \{1, 2, \ldots\ldots p-1\}$ mod p

The integers are in the set that are not relatively prime to n -

$\{1, \ldots\ldots (pq-1)\}$

$\{p, 2p, \ldots\ldots (q-1)p\}$

$\{q, 2q, \ldots\ldots (p-1)p\}$

Accordingly,

$$\phi(n) = (pq-1) - [(q-1) + (p-1)]$$
$$= (pq) - (p+q) + 1$$
$$= (p-1)(q-1)$$
$$= \phi(p)\,\phi(q)$$

eg $n = 15$.

$$\phi(n) = \phi(15)$$
$$= \phi(3) \cdot \phi(5)$$
$$= 5 \times 3$$
$$= (4) \times 2)$$
$$= 8$$

Q4

$$\phi(15) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)$$
$$= 15\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)$$
$$= 15 \times \frac{2}{3} \times \frac{4}{5}$$

$\phi(15) = 8$

Date:-20/09/18 Day:- Thursday

Unit -3

Authentication Requirements

1. **Disclosure** ⇒ Release of Message Contents to any person not processing the appropriate cryptographic key.
2. **Traffic analysis** ⇒
3. **Masquarede**
4. **Content Modification**
5. **Sequence Modification**
6. **Timing Modification**
7. **Source Repudiation** - Denial of transmission of message by source.
8. **Destination Repudiation** - Denial of receive of message by destination.

Message authentication is a procedure to verify that received messages come from the alleged source & have not been alter. It may also verify sequencing & timeliness.

Date:- 24/09/18 Day:- Monday

Authentication Function -

The types of function to produce authentication can be grouped into 3 classes -

1. MAC (Message Authentication Code)
2. Message Encryption.
3. Hash function.

Message Encryption :-

The cipher-text of the entire - message act as its authenticator.

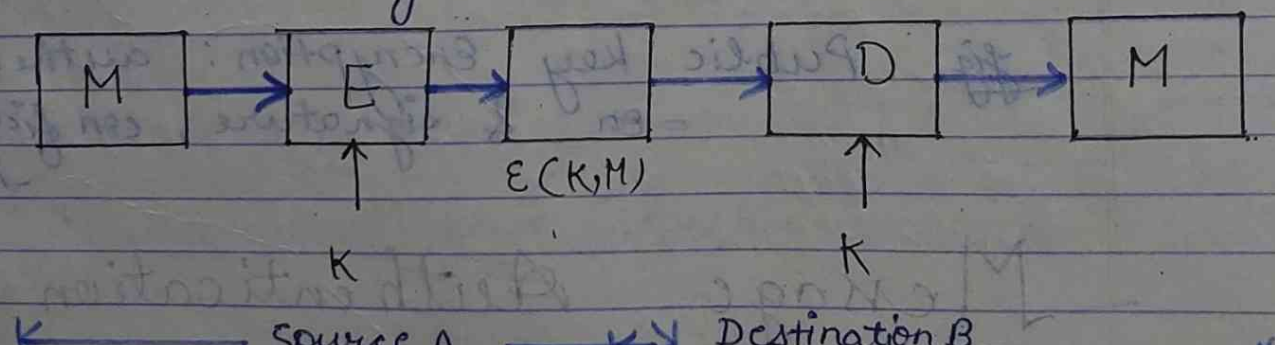


Fig - Message Encryption

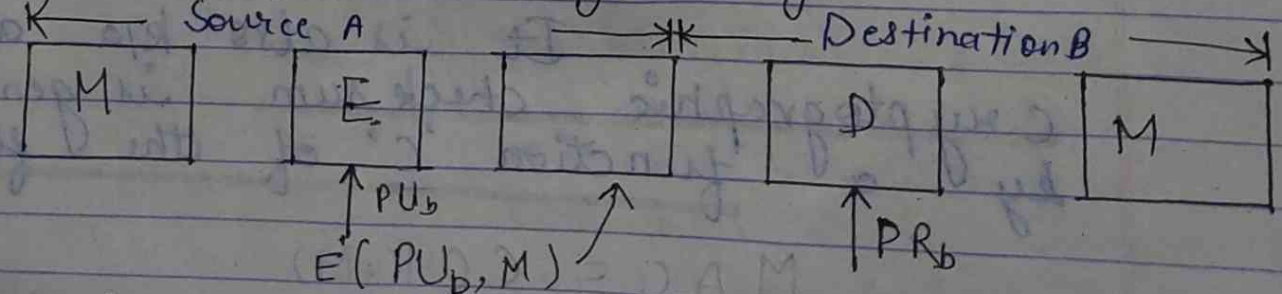
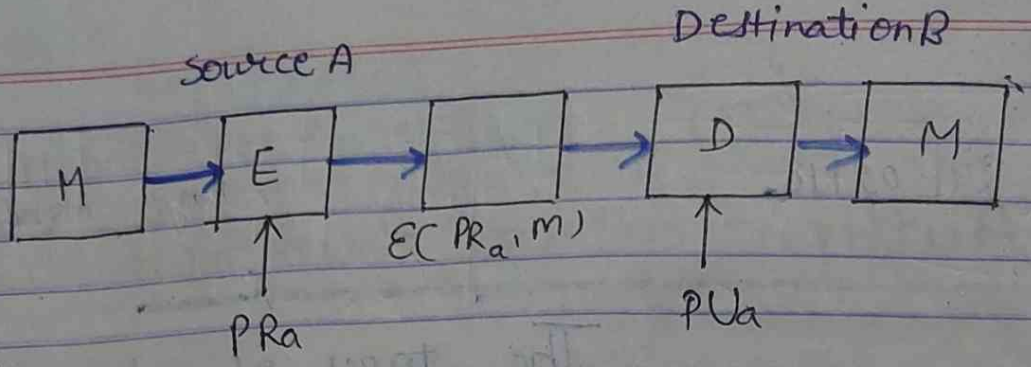
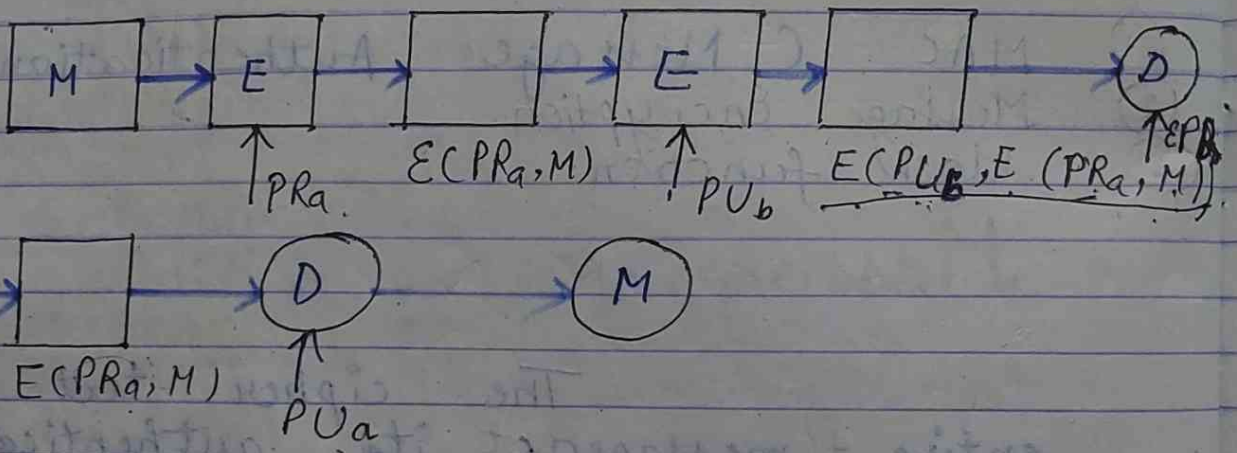


Fig : Publickey Encryption : Confidentiality



~~fig~~ Public key Encryption: authentication & signature



~~fig~~ Public key Encryption: authentication & signature, confidentiality.

Message Authentication Codes -

It is also k/a a cryptographic checksum is generated by a function 'C' of the form

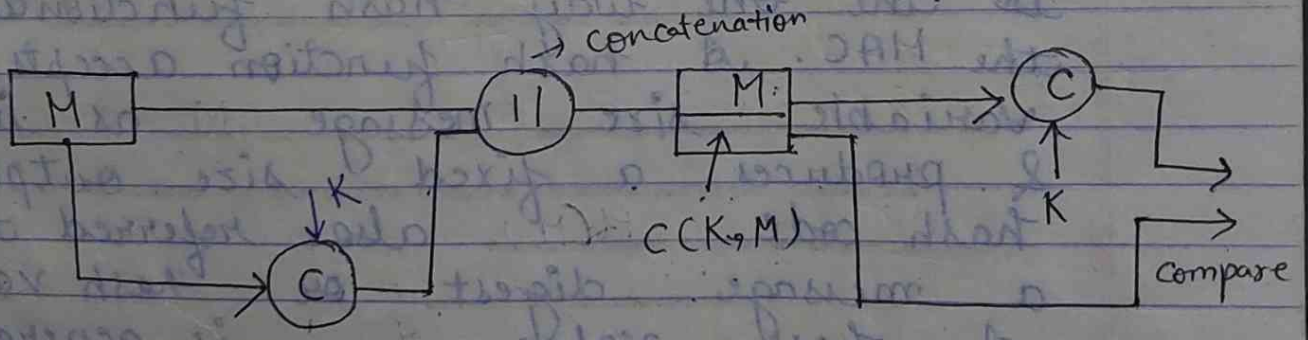
$$MAC = C(K, M)$$

where,

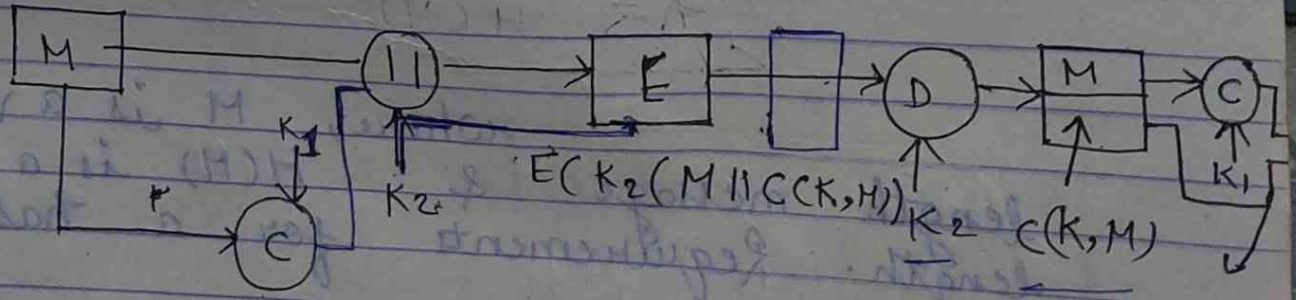
M = Variable length message
K = Secret key shared only by sender & receiver
C(K, M)

C(K;M) = fixed length authenticator.

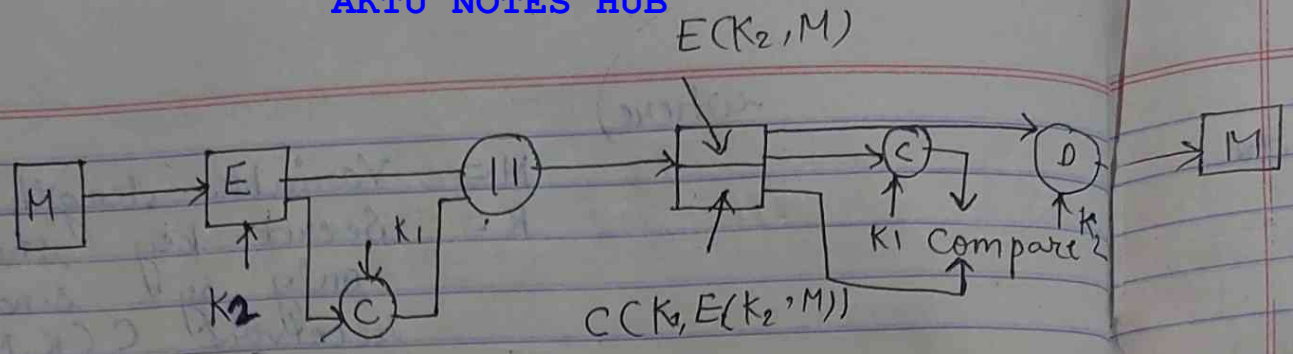
The MAC is appended to the message at the source at a time when the message is assume or known to be current. The receiver that authenticate by recomputing the MAC.



(a) Message Authentication



(b) Message authentication & confidentiality : authentication tied to plain-text.



(a) Message Authentication & confidentiality: authentication tied to cipher-text.

imp 1.

Date: 25/09/18 Day:- Tuesday

2.

3.

4.

Hash Function-

A variation on the MAC is the one way hash function as with the MAC. A hash function accepts a variable size message M as input & produces a fixed size output or hash code H(M) also referred to as a message digest or hash value. A hash value h is generated by a function of the form

imp

$$h = H(M)$$

where, M is a variable length message & H(M) is a fixed length. Requirements for a hash function -

The purpose of a hash function

→ M is to produce a finger print of a file or other block of data. To be useful for message authentication H. H must have a following properties -

imp
1. H can be applied to a block of data of any size.
2. H produces a fixed length output.
3. H(M) is relatively easy to compute for any given message M.
4. For any given value h it is computationally infeasible to find such that -

$$H(M) = h$$

This is kla 'one-way property.'

imp For any given block - 'M' it is computationally infeasible to find $N \neq M$ such that -

$$H(N) = H(M)$$

Sometimes preferred to as - 'Weak- collision resistance'. It is computationally infeasible to find any pair (N, M) such that -

$$H(N) = H(M)$$

Sometimes, referred to as strong collision resistance.

Simple Hash Function -

One of the simplest hash function is the bit-by-bit XOR of every block. This can be expressed as follows -

$$C_i = b_{i_1} \oplus b_{i_2} \oplus \ldots \oplus b_{im}$$

where, C_i = i^{th} bit of the hash code.

$1 \leq i \leq n$

m = no. of n bits block in the input.

$\oplus$ = XOR operation

b_{ij} = i^{th} bit in j^{th} block.

Revision

Solve by Extended Euclidean algo.

$a = 431, 111$

$t \leftarrow 0-(3\times 1)$ $\quad 111\times 2=222$ $\quad 111\times 3=333$ $\quad 111\times 4=444$

$111\overline{)431}\,(3$ (312), 333, 98

$s \leftarrow s_1-(q\times s_2)$
$\leftarrow 1-(3\times 0)$

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
							0	1	
3	431	111	98	1	0	1			−3
1	111	98	13	0	1	−1	1	−3	4
7	98	13	7	1	−1	8	−3	4	−31
1	13	7	6	−1	8	−9	4	−31	35
1	7	6	1	8	−9	17	−31	35	−66
6	6	1	0	−9	17	−111	35	−66	431
	1	0		17	−111		−66	431	

gcd $= (s_1\times r_1)+(t_1\times r_2)$

$(17\times 431)+(-66\times 111)$

$3 = 17$
96
$\times 6$
576
35
611

$(s_1\times r_1)+(t_1\times r_2)$

$(17\times 431)+(-66\times 111)$

$7327 - 7326$

$= 1$

431×17
3017
431
7327

gcd $(1)\,111$

$s \leftarrow -9-(6\times 17)$
$s \leftarrow -9-102$
$s \leftarrow -111$

$t \leftarrow 35-(6\times(-9))$
$35+576$
$t \leftarrow 35-(6\times($

0

431
$\times 66$
2586
28446

$111\overline{)28446}\,(256$

$111\overline{)98}\,(1$
$7\overline{)13}\,(1$
7
6 (r1)
$\frac{6}{1}$

$s \leftarrow -1-(1\times 8)$
$s \leftarrow -1-8$
$s \leftarrow -9$

$t \leftarrow 4-(1\times(-31))$
$t \leftarrow 4+(31)$
$t \leftarrow 35$

$s \leftarrow 8-(1\times(-9))$
$8+9$
$t \leftarrow -31-(1\times(35))$
$-31-35$

Rough

98
$98\overline{)111}\,(1$
98
13

$s \leftarrow 0-(1\times 1)$
$t \leftarrow 1-(1\times(-3))$
$t \leftarrow 1+3$
$t \leftarrow 4$

$13\overline{)98}\,(7$
91
7
-28
3
31

$s \leftarrow 1-(7\times(-1))$
$\leftarrow 1+7$
$t \leftarrow -3-(7\times 4)$
$\leftarrow -3-28$
$\leftarrow -31$

Date:- 26/09/18

Encryption - public key
decryption - private key

Day:- Wednesday

R.S.A. :-

(Rivest, Shamir, Adleman)

It is a block-cipher each plain-text block is an integer b/w 0 to n-1 for some n which leads to a block-size <= $\log_2 n$
Size of 'n' is 1024-bits.

1. Choose 2 prime no:s p & q such that $p \neq q$
2. Calculate $n = p * q$.
3. Calculate $\phi(n) = (p-1)*(q-1)$
4. Select e such that $\gcd(e, \phi(n)) = 1$, $1 < e < \phi(n)$, e should not be a factor of $\phi(n)$
5. Find d such that $de = 1 \bmod \phi(n)$
6. Calculate Public key $(PU) = (e, n)$
7. Calculate Private key $(PR) = (d, n)$

$$C = M^e \bmod n$$
$$M = C^d \bmod n$$

e = Public key
d = Private key

Date:- 01/10/18 Day:- Monday

Assignment -3

Qu.1 $p=3$, $q=11$, $e=7$, $m=5$

Que.2. $p=11$, $q=13$, $e=11$ find private key.

Qu.3. $e=3$, $d=11$, $n=15$ consider a p.7 alpha-bet G(M=7)

Qu.4. $p=17$, $q=11$, $e=7$, $M=88$

Qu.5 $p=7$, $q=17$, $e=5$

Qu.6. $p=47$, $q=71$, $e=79$

Soln.1.

$M = C^d \bmod n$

$C = M^e \bmod n$

$n = pq$

$n = 3 \times 11 = 33$

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

$= (3-1)(11-1)$

$= 20$

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

$d \times 7 = 1 \bmod 20$

$3 \times 7 = 1 \bmod 20$

$21 = (1) \bmod 20$

$C = M^e \bmod n$

$C = 5^7 \bmod 33$

$C = 14$

Soln 2:

$n = pq$

$n = 11 \times 13$

$n = 143$

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

$= (10) \times (12)$

$\phi(n) = 120$

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

$d \times 11 = 1 \bmod 120$

$11 \times 11 = 1 \bmod 120$

$\boxed{d = 11}$

$C = M^e \bmod n$

Soln 3:

$n = 15 \quad = p \times q = 3 \times 5$

$d = 11, \quad M = 7$

$e = 3$

$\phi(n) = (p-1)(q-1) = (3-1) \times (5-1) = 2 \times 4 = 8$

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

$11 \times 3 = 1 \bmod 8$

$\boxed{d = 11}$

$C = M^e \bmod n$

$C = 7^3 \bmod 15$

$\boxed{C = 13}$

Soln 4: $p = 17, \quad q = 11, \quad e = 7, \quad M = 88$

$n = p \times q = 17 \times 11$

$n = 187$

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

$= 16 \times 10$

$= 160$

$de = 1 \bmod \phi(n)$
$dx7 = 1 \bmod 160$
$23x7 = 1 \bmod 160$

$\boxed{d = 23}$

$C = M^e \bmod n$
$C = (88)^7 \bmod 187$

i	x_i	$y \leftarrow a x y \bmod n$	$a \leftarrow a^2 y \bmod n$
0	1	$y \leftarrow 88 x 1 \bmod 187 = 88$	$a \leftarrow (88)^2 \bmod 187 = 77$
1	1	$y \leftarrow 77 x 88 \bmod 187 = 44$	$a \leftarrow (77)^2 \bmod 187 = 132$
2	1	$y \leftarrow 132 x 44 \bmod 187 = 11$	

$\boxed{C = 11}$

Sol^n:5

$p = 7, \quad q = 17, \quad e = 5$
$n = pq$
$n = 7x17$
$n = 119$
$\phi(n) = (p-1) \times (q-1) = 6 \times 16 = 96$

$d \cdot e = 1 \bmod 96$
$d \cdot 5 = 1 \bmod 96$
$77 x 5 = 1 \bmod 96$
$\boxed{d = 77}$

Sol^n:6

$p = 47, \quad q = 71, \quad e = 79$
$n = p x q$
$n = 47 x 71$
$\boxed{n = 3337}$

$s \to s_1 - (q \times s_2)$ $\quad s = 4$

$4 - (4 \times 0)$

$t \to t_1 - (q \times t_2)$

$0 - (4 \times 1) = -4$

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

$\phi(n) = (47-1) \times (71-1)$

$\phi(n) = 46 * 70$

$\phi(n) = 3220$

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

$d \cdot 79 = 1 \bmod 3220$

$\cdot 79 = 1 \bmod 3220$

$d = 1019$

$b = 79$, $a = 3220$

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
40	3220	79	60	1	0	1	0	1	-40
1	79	60	19	0	1	-1	1	-40	41
3	60	19	3	1	-1	4	-41	41	-163
6	19	3	1	-1	4	-25	41	-163	119
3	3	1	0	4	-25	79	-163	119	-476
	1	0		-25	41		1019		Inverse

$d = 1019$ Ans

$t \Rightarrow 1019$

$s \to -1 - (6 \times 4)$

$-1 - 24 = -25$

$-1 - (6 \times 4)$

$-1 - 24$

$6 \cdot -12 - (3 \times -1)$

$t \to 5 - (6 \times (-19))$

$+ 114$

$t \to 1 - (1 \times 40)$

$0 - (1 \times 1)$

$1 + (1 \times 40)$

$t \to (1) - (1 \times -4)$

$\to 1 + 4$

$a - (3 \times 119)$

$4 + (3 \times 275) + (6 \times 19)$

Rough

79 | 3220 (40
316
60

1
60 | 79 (1
60
19

19 | 60 (3
57
3

3220
3220 (1
4
3220
2
6440
6441

79
109 B
711
702
411
79 B
1019
1
1019
719
9171
7132
80501
3220

A B C D E F G H I J K L
0 1 2 3 4 5 6 7 8 9 10 11

Day :- Thursday

Date :- 11/10/18

ASSIGNMENT- 4 & 5

Qu-1. By using hill-cipher technique encrypt the message 'AT' with the help of key.

$$K = \begin{bmatrix} 5 & 3 \\ 3 & 4 \end{bmatrix}$$

message = AT

$$\begin{bmatrix} 0 \\ 19 \end{bmatrix}$$

$$C = KP \bmod 26$$

$$= \begin{bmatrix} 5 \cdot 3 \\ 3 \cdot 4 \end{bmatrix} \bmod \begin{bmatrix} 0 \\ 19 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 0+57 \\ 0+76 \end{bmatrix} = \begin{bmatrix} 57 \\ 76 \end{bmatrix} \bmod 26$$

$$K \rightarrow \begin{bmatrix} 5 \\ 24 \end{bmatrix} = \begin{bmatrix} F \\ Y \end{bmatrix}$$

Qu-2. P.T ⇒ 'I am a hacker'
Keyword - 'COMPUTER'.

Soln.

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

→ replaced

I AM A HACKER

26 × 4 = 104 | 26) 124 (4 , 104 , 20 | 26) 57 (2 , 52 , 5 | 26) 86 (3 , 78 | 26) 76 (2 , 52 , 24 | 26 × 3 = 78 | 108 , 16 , 124 | 26) 68 (2 , 52 , 16

HB PR HQHTVRA

Ques P.T ⇒ ME using 'Hill-Cipher Technique'

$$K = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \qquad \text{Message} = \begin{bmatrix} M \\ E \end{bmatrix}$$

$$C = KP \bmod 26$$

$$= \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 12 \\ 4 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 108 + 16 \\ 60 + 28 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 124 \\ 88 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 20 \\ 10 \end{bmatrix} = \begin{bmatrix} U \\ K \end{bmatrix}$$

Ques Determine 27^{-1} mod 100 using Extended Euclidean algorithms.

As 27 inverse mod 100

Soln

$b = 27 = r_1$

$a = 100 = r_2$

$b > 0$ i.e. $r_2 > 0$

$26+(2\times37)$ $\quad -7-(2\times10)$ $\quad -7-20$ $\quad 3+(1\times7)$ $\quad -11-(1\times26)$

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
				1	0	1	0	1	-3
3	100	27	19	0	1	-1	1	-3	4
1	27	19	8	1	-1	3	-3	4	-11
2	19	8	3	-1	3	-7	4	-11	26
2	8	3	2	3	-7	10	-11	26	-37
1	3	2	1	-7	10	-27	26	-37	100
2	2	1	0	10	-27		-37	100	
	(1)	0							

$\downarrow$ gcd = 1

$27^{-1} \bmod 100 = \boxed{-37} = t_1$

$= (s_1 \times r_1) + (t_1 \times r_2)$

$= (10\times100) + ((-37)\times27)$

$= 1$ Ans

Ques $r_1 = x^4+x+1$

$r_2 = x^2+1$

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
				1	0	1	0	1	$-x^2$
x^2	x^4+x+1	x^2+1	$x-x^2+1$	0	1	-1	1	$-x^2$	$1+x^2$
1	x^2+1	$x-x^2$	$x+1$	1	-1	$1+x$	$-x^2$	$1+x^2$	$-x^2-x$
x	$x-x^2$	$x+1$	$2x$	-1	$1+x$	$-2x$	$1+x^2$	$+x^3-x^2-x$	$2x^3-$
1	$x+1$	$2x$	$-x+1$	$1+x$	$-2-x$	$2x+3$	$-x^3-x^2-x$	$2x^3-x^3$	$2x^3-$
1	$2x$	$-x+1$	$x-1$	$-2-x$	$2x+3$	$-3x-5$	$2x^3-x^3$	$2x^3-x^2$	$-x^3+$
1	$-x+1$	$x-1$	$2x$	$2x+3$	$-3x-5$	$5x+8$	$2x^3-x^2$	$-2x^3-x^3$	$3x^3-$
1	$x-1$	$2x$	$-2x-1$	$-3x-5$	$5x+8$		$-2x$	$+3x$	
	$2x$	$-2x-1$							

P.T.O

$-1-(2\times3)$

$-1-6=$ $\quad 4+(2\times11)$

26

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
x^2+1	x^4+x+1	x^2+1	x	1	0	1	0	1	$-(x^2+1)$
x	x^2+1	x	1	0	1	$-x$	1	$-(x^2+1)$	x^3+x+1
x	x	1	0	1	$-x$	$1+x^2$	$-(x^2+1)$	x^3+x+1	$-x^4-x+1$
	1	0		$-x$	$1+x$		x^3+x+1		

inverse

This means that $(x^2+1)^{-1}$ modulo (x^4+x+1) is $-(x^3+x+1)$

$\Rightarrow (s_1 \times r_1) + (t_1 \times t_2)$

$\Rightarrow [(+x\times(x^4+x+1)) + ((x^3+x+1)\times(x^2+1))]$

$\Rightarrow -x^5-x^2-x+x^5+x^3+x^2+x^3+x+1$

$\Rightarrow 1$ Ans

Ques.7 Find inverse of 1234 mod 4321

inverse

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
3	4321	1234	619	1	0	1	0	1	-3
1	1234	619	615	0	1	-1	1	-3	4
1	619	615	4	1	-1	2	-3	4	-7
153	615	4	3	-1	2	-307	4	-7	1075
1	4	3	1	2	-307	309	-7	1075	-1082
3	3	1	0	-307	309	-1234	1075	-1082	4321
	(1)	0		309	-1234		-1082	4321	

↓ gcd

Inverse of 1234 mod 4321 = -1082

Ans

Ques.8 Using Miller-Rabin's Test -

$n = 341$

Step-1

$n-1 = 2^k \cdot m$

$341-1 = 2^k \cdot m$

$340 = 2^2 \cdot 85$

2	340
2	170
5	85
17	17
	1

$m = 85$, $K = 2$

Step-2

$b_0 = a^m \bmod n$

$b_0 = 2^{85} \bmod 341$

Let, $a = 2$

2	85	1
2	42	0
2	21	1
2	10	0
2	5	1
2	2	0
	1	

i	x_i	$y \leftarrow a^x y \bmod n$	$a \leftarrow a^2 \bmod n$
0	1	$y \leftarrow 2 \times 1 \bmod 341 = 2$	$a \leftarrow 4 \bmod 341 = 4$
1	0	$y \leftarrow 2$	$a \leftarrow 16 \bmod 341 = 16$
2	1	$y \leftarrow 16 \times 2 \bmod 341 = 32$	$a \leftarrow 256 \bmod 341 = 256$
3	0	$y \leftarrow 32$	$a \leftarrow 65536 \bmod 341 = 64$
4	1	$y \leftarrow 64 \times 32 \bmod 341 = 2$	$a \leftarrow 4096 \bmod 341 = 4$
5	0	$y \leftarrow 2$	$a \leftarrow 16 \bmod 341 = 16$
6	1	$y \leftarrow 16 \times 2 \bmod 341 = 32$	$a \leftarrow 256$

$b_0 = 32$

$b_1 = (b_0)^2 \bmod 341$

$b_1 = (32)^2 \bmod 341$

$\boxed{b_1 = +1}$

So, 341 is Composite no..

Qu9 $x = 2 \bmod P$ for all $P = (3, 5, 7)$

Sol^n Given eq^{ns} -

$$\begin{cases} x = 2 \bmod 3 \\ x = 2 \bmod 5 \\ x = 2 \bmod 7 \end{cases}$$

$M = m_1 \times m_2 \times m_3 = 3 \times 5 \times 7 = 105$

$M_1 = \frac{M}{m_1} = \frac{105}{3} = 35$

$M_2 = \frac{M}{m_2} = \frac{105}{5} = 21$

$M_3 = \frac{M}{m_3} = \frac{105}{7} = 15$

105) 6326 (60
630
2

105) 422 (4
420
2

13) 61 (

$M_1 y_1 = 1 \bmod 3$

$35 y_1 = 1 \bmod 3$

$2 \times 2\ y_1 = 2 \times 1 \bmod 3$

$\boxed{y_1 = 2}$

$M_2 y_2 = 1 \bmod 5$

$21 y_2 = 1 \bmod 5$

$1 \cdot y_2 = 1 \bmod 5$

$\boxed{y_2 = 1}$

$M_3 y_3 = 1 \bmod 7$

$15 \cdot y_3 = 1 \bmod 7$

$1 \cdot y_3 = 1 \bmod 7$

$\boxed{y_3 = 1}$

$x = (M_1 a_1 y_1 + M_2 a_2 x y_2 + M_3 y_3 a_3) \bmod M$

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

$\boxed{x = 212} \bmod 105 \Rightarrow 212$

$212 = 2 \bmod 3 \Rightarrow$ verified

↓ R

$420 = 2 \bmod 5 \Rightarrow$ verified

↓ R

$420 = 2 \bmod 7 \Rightarrow$ verified

↓ R

=

$1092\overline{)6192}^{5}$ -5460 732

$12\overline{)37}^{3}$ 36 1 6

$12\overline{)14}^{1}$ 12 2

$12\overline{)28}^{2}$ 24 4

$13\overline{)18}^{1}$ 13 5

$13\overline{)84}^{6}$ 78 6

Q4 (10)

$x = 4 \bmod 7$

$x = 4 \bmod 13$

$x = 0 \bmod 12$

$M = m_1 \times m_2 \times m_3 = 7 \times 13 \times 12 = 1092$

$M_1 = \frac{M}{m_1} = \frac{1092}{7} = 156$

$M_2 = \frac{M}{m_2} = \frac{1092}{13} = 84$

$M_3 = \frac{M}{m_3} = \frac{1092}{12} = 91$

$M_1 y_1 = 1 \bmod 7$

$156\, y_1 = 1 \bmod 7$

$4 \cdot 2 \cdot y_1 = 4 \cdot 1 \bmod 7$

$\boxed{y_1 = 4}$

$M_2 y_2 = 1 \bmod 13$

$84\, y_2 = 1 \bmod 13$

$156\, y_2 = 11 \times 1 \bmod 13$

$\boxed{y_2 = 11}$

$M_3 y_3 = 1 \bmod 12$

$91\, y_3 = 1 \bmod 12$

$7 \cdot 7\, y_3 = 7 \cdot 1 \bmod 12$

$\boxed{y_3 = 7}$

$x = M_1 a_1 y_1 + M_2 a_2 y_2 + M_3 a_3 y_3$

$x = (156 \times 4 \times 4 + 84 \times 4 \times 11 + 91 \times 0 \times 7) \bmod 1092$

$x = 6192 \bmod 1092$

$\boxed{x = 732}$

$732 = 4 \bmod 7 = 4 (R)$

$732 = 4 \bmod 13 = 4 (R)$

$732 = 0 \bmod 12 = 0 (R)$

10) 54 (5 10) 45 (4 10) 99 (9 9) 110 (12
50 40 90 9 28
4 50 9 18
10 2

Qu'n 1 mp

$x = 3 \bmod 9$
$x = 2 \bmod 10$
$x = 3 \bmod 11$

$M = m_1 \times m_2 \times m_3 = 9 \times 10 \times 11 = 990$

$M_1 = \frac{M}{m_1} = \frac{990}{9} = 110$

$M_2 = \frac{M}{m_2} = \frac{990}{10} = 99$

$M_3 = \frac{M}{m_3} = \frac{990}{11} = 90$

$M_1 y_1 = 1 \bmod 9$
$110\, y_1 = 1 \bmod 9$
$5 \times 2\, y_1 = 5 \times 1 \bmod 9$
$y_1 = 5$

$M_2 y_2 = 1 \bmod 10$
$99\, y_2 = 1 \bmod 10$
$99\, y_2 = 9 \cdot 1 \bmod 10$
$y_2 = 9$

$M_3 y_3 = 1 \bmod 11$
$90 \cdot y_3 = 1 \bmod 11$
$6 \cdot 2\, y_3 = 61 \bmod 11$
$y_3 = 6$

$x = (5 \times 3 \times 110 + 9 \times 2 \times 99 + 6 \times 3 \times 90) \bmod 990$
$x = 5052 \bmod 990$
$x = 102$

$102 = 3 \bmod 9 = R \Rightarrow 3$
$102 = 2 \bmod 10 = R \Rightarrow 3$
$102 = 3 \bmod 11 = R \Rightarrow 3$

Proved

9) 110 (12
9
20
18
2

5
990) 5052 (
4950
102

8
11) 90 (
88
2

11
9) 102 (11
9
12
9
3

(12) $x = 2 \bmod 3$

$x = 3 \bmod 5$

$$M = m_1 \times m_2 = 3 \times 5 = 15$$

$$M_1 = \frac{M}{m_1} = \frac{15}{3} = 5$$

$$M_2 = \frac{M}{m_2} = \frac{15}{5} = 3$$

$M_1 y_1 = 1 \bmod 3$

$15\, y_1 = 1 \bmod 3$

$2 \cdot 2\, y_1 = 2 \cdot 1 \bmod 3$

$\boxed{y_1 = 2}$

$M_2 y_2 = 1 \bmod 5$

$2 \cdot 3\, y_2 = 2 \cdot 1 \bmod 5$

$\boxed{y_2 = 2}$

$x = (M_1 a_1 y_1 + M_2 a_2 y_2) \bmod M$

$x = (15 \times 2 \times 2 + 3 \times 3 \times 2) \bmod 15$

$x = 38 \bmod 15$

$\boxed{x = 8}$

$8 = 2 \bmod 3 \Rightarrow R = 2$ verified

$8 = 3 \bmod 5 \Rightarrow R = 3$ verified.

---

(13) $x = 2 \bmod 3$

$x = 1 \bmod 4$

$x = 3 \bmod 5$

$M = m_1 \times m_2 \times m_3 = 3 \times 4 \times 5$

$= 60$

$M_1 = \frac{M}{m_1} = \frac{60}{3} = 20$

$M_2 = \frac{M}{m_2} = \frac{60}{4} = 15$

$M_3 = \frac{M}{m_3} = \frac{60}{5} = 12$

$M_1 y_1 = 1 \bmod 3$

$20 y_1 = 1 \bmod 3$

$2 \cdot 2 y_1 = 2 \cdot 1 \bmod 3$

$\boxed{y_1 = 2}$

$M_2 y_2 = 1 \bmod 4$

$15 y_2 = 1 \bmod 4$

$3 \cdot 3 y_2 = 3 \cdot 1 \bmod 4$

$\boxed{y_2 = 3}$

$M_3 y_3 = 1 \bmod 5$

$12 y_3 = 1 \bmod 5$

$3 \cdot 2 y_3 = 3 \cdot 1 \bmod 5$

$\boxed{y_3 = 3}$

$x = (M_1 a_1 y_1 + M_2 a_2 y_2 + M_3 a_3 y_3) \bmod M$

$x = (20 \times 2 \times 2 + 15 \times 1 \times 3 + 12 \times 3 \times 3) \bmod 60$

$x = 233 \bmod 60$

$\boxed{x = 53}$

Verification -

$53 = 2 \bmod 3 \Rightarrow R = 2$ verified

$53 = 1 \bmod 4 \Rightarrow R = 1$ verified

$53 = 3 \bmod 5 \Rightarrow R = 3$ verified

(14) $x = 2 \bmod 7$

$x = 3 \bmod 9$

$M = m_1 \times m_2 = 7 \times 9 = 63$

$M_1 = \frac{M}{m_1} = \frac{63}{7} = 9$

$M_2 = \frac{M}{m_2} = \frac{63}{9} = 7$

$M_1 y_1 = 1 \bmod 7$, $M_2 y_2 = 1 \bmod 9$

$9 \times y_1 = 1 \bmod 7$ $\quad 4.7 \times y_2 = 4.1 \bmod 9$

$4 \cdot 2 \cdot y_1 = 4 \bmod 7$ $\quad \boxed{y_2 = 4}$

$\boxed{y_1 = 4}$

$x = (M_1 a_1 y_1 + M_2 a_2 y_2) \bmod M$

$x = (9 \times 2 \times 4 + 7 \times 3 \times 4) \bmod 63$

$x = 156 \bmod 63$

$\boxed{x = 30}$

$30 = 2 \bmod 7 \Rightarrow R = 2$ verified

$30 \div 3 \bmod 9 \Rightarrow R = 3$ verified.

---

(15) $E = 7$, $N = 3$, message = "ME" using 0 to 25 (A=Z)

$M = 12$, $E = 4$ 7

$d\,e = 1 \bmod \phi(n)$, $C \equiv M^7 \pmod 3$

$d \cdot 7 = 1 \bmod \phi(n)$ $\quad C \equiv (12)^7 \bmod 3$

$C \equiv 0 \pmod 3 = 0$

for $E = 4$

$C \equiv M^7 \pmod 3$ $\quad \because C = M^e \bmod n$

$C \equiv (4)^7 \bmod 3$

$C \equiv 1$

The encrypted cipher-text = 0 : 1

x_i	y	a
1	$y \leftarrow 12 \times 1 \bmod 3 = 0$	$a \leftarrow 0$
1	$y \leftarrow 0 \times 0 = 0$	$a \leftarrow 0$
1	$y \leftarrow 0$	$a \leftarrow 0$
1	$y \leftarrow 4 \times 1 \bmod 3 = 1$	$y \leftarrow 1$.
1	$y \leftarrow 1 \times 1 \bmod 3 =$	
1		
1		

(16) $p=17, q=31, m=2, e=7$ find remaining-

$n = pq = 17 \times 31 = 527$

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

$= 16 \times 30 = 480$

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

$d \cdot e = 1 \bmod 480 \Rightarrow d \cdot 7 = 1 \bmod 480$

$d = -137 \bmod 480 = (480-137)$

$M = C^d \bmod n$	$C = M^e \bmod n = 343$
$M = (128)^{343} \bmod 527$	$C = (2)^7 \bmod 527$
$M = 2$	$C = 128$

Public key $\Rightarrow$ (e, n)	$\Rightarrow (7, 527)$
Private key $\Rightarrow$ (d, n)	$\Rightarrow (343, 527)$

Ans

(17) $p=11, q=13, e=7, m=9$

$n = pq = 11 \times 13 = 143$

$\phi(n) = (p-1)(q-1) = 10 \times 12 = 120$

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

$d \cdot 7 = 1 \bmod 120$

$7d = 1 \bmod 120 \Rightarrow -17 \bmod 120$

$d = 103$

$C = M^e \bmod n = (9)^7 \bmod 143$

i	x_i	$y \leftarrow 9 x_i y \bmod n$	$a \leftarrow a^2 \bmod n$
0	1	$y \leftarrow 9 \times 1 \bmod 143 = 9$	$a \leftarrow 81 \bmod 143 = 81$
1	1	$y \leftarrow 81 \times 9 \bmod 143 = 14$	$a \leftarrow 196 \bmod 143 = 53$
2	1	$y \leftarrow 53 \times 14 \bmod 143 = 27$	

$C = 27$

Public-key = (7, 143)

Private Key = (103, 143)

$M = 9$

143)729(5 → 5×7=121, 715, 14

143)196(1, 143, 53

143)742(5, 715, 27

$M = C^d \bmod n$

Date:- 16|10|18 Day:- Tuesday

Soln-7) $3^{201} \bmod 11$

$3^{201-1} \bmod 11$

$3^{200} \bmod 11$

$(3^5)^{40} \bmod 11$

$3^1 \equiv 3 \bmod 11$

$3^2 \equiv 9 \bmod 11$

$3^3 \equiv 5 \bmod 11$

$3^4 \equiv 4 \bmod 11$

$3^5 \equiv 1 \bmod 11$

Apply By Fermat's theorem

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

$3^{p-1} \equiv 1 \bmod p$

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

$3^{10} \equiv 1 \bmod 11$

$\Rightarrow 3^{200} \cdot 3^1 \bmod 11$

$(3^{10})^{20} \cdot 3^1 \cdot \bmod 11$

$1 \cdot 3^1 \cdot \bmod 11$

$3 \bmod 11$

$= 3$ Ans

eg $3^{69} \bmod 11$

$3^{69-1} \bmod 11$

$3^{68} \bmod 11$

$(3^5)^{42} \bmod 11$

↓ Similar as above.

Qus $3^{2005} \bmod 500$

$3^{p-1} \equiv 1 \bmod 500$

$3^{} \equiv 3 \bmod 500$

$3^{500} \equiv 3 \bmod 500$

$(3^{10})^{50} \equiv 3 \bmod 500$

$(1)^{50} \Rightarrow 1$

$3^{2005} \bmod 500$

$= (3^{500 \times 4})^{+5} \bmod 500$

$= (3^{500})^4 \cdot 3^5 \bmod 500$

$= (3^4) \cdot 3^5 \bmod 500$ $= 19683 \bmod 500$

$= 183.$

Date – 17/10/18

Diffie-Hellman Algo

Ans.1 $q = 71$ ✓
$A = 7$
$X_A = 5$ ✓
$X_B = 12$
} private

$Y_A, Y_B, K_A, K_B = ?$

2 | 12 | 0
2 | 6 | 0
2 | 3 | 1
1

Soln $y_A = a^{x_a} \bmod q$

$y_A = (7)^5 \bmod 71$

$y_A = 51$

$y_B = a^{x_b} \bmod q$

$y_B = (7)^{12} \bmod 71$

$y_B = 4$

i	x_i	y	a
0	0	→	$a \leftarrow a^2 \bmod 71 = 49$
1	0	→	58
2	1	58	27
3	1	$27 \times 58 \bmod 71 = 4$ (y_B)	

$K_A = y_A^{x_B} \bmod 71$

$= (51)^{12} \bmod 71$

$= 30$

$K_B = y_B^{x_A} \bmod 71$

$= 4^5 \bmod 71$

$= 30$

Private Key

Ques Given, $P = 11$

$g = 2$

$y_A = 9, \quad y_B = 3$

$y_A = g^{x_A} \bmod P$

$9 = 2^{x_A} \bmod 11$

$9 = 2^6 \bmod 11$

$y_B = g^{x_B} \bmod P$

$3 = 2^{x_B} \bmod 11$

$= 2^8 \bmod 11$

$K_A = 9^8 \bmod 11 = 3$

$K_B = 3^6 \bmod 11 = 3$

Ans

Ques Imp $P = 23$, Primitive root $g = 7$

Private key = $X_A = 3$

$X_B = 5$

$y_A = (g)^{x_A} \bmod P$

$y_A = (7)^3 \bmod 23$

$y_A = 21$

$y_B = (7)^5 \bmod 23$

$y_B = 17$

$K_A = (y_A)^{x_B} \bmod P$

$K_A = (21)^5 \bmod 23$

$K_A = 14$

$K_B = (17)^3 \bmod 23$

$K_B = 14$

imp

(21)

$q = 83$

$\alpha = 13$

$x_A = 5$, $x_B = 12$

$y_A = (\alpha)^{x_A} \bmod q$

$y_A = (13)^5 \bmod 83$

$y_A = 34$

$y_B = (\alpha)^{x_B} \bmod q$

$y_B = (13)^{12} \bmod 83$

$y_B = 65$

2	12	0
2	6	0
2	3	1
	1	

i	x_i	y	a
0	0	$\longrightarrow$	$a \leftarrow (13)^2 \bmod 83 = 3$
1	0	$\longrightarrow$	$a \leftarrow 9 \bmod 83 = 9$
2	1	$9 \times 1 \bmod 83 = 9$	$a \leftarrow 81 \bmod 83 = 81$
3	1	$81 \times 9 \bmod 83 = 65$	

$K_A = (y_A)^{x_B} \bmod q$

$K_A = (34)^{12} \bmod 83 = 10$

i	x_i	y	a
0	0	$\longrightarrow$	$a \leftarrow (34)^2 \bmod 83 = 77$
1	0	$\longrightarrow$	$a \leftarrow (77)^2 \bmod 83 = 36$
2	1	$36 \times 1 = \bmod 83 = 36$	$a \leftarrow 51$
3	1	$51 \times 36 \bmod 83 = 10$	

(10)

$K_B = (y_B)^{x_A} \bmod q$

$K_B = (65)^5 \bmod 83$

$K_B = 10$

2	5	1
2	2	0
	1	

i	x_i	y	a
0	1	$y \leftarrow 65 \times 1 \bmod 83 = 65$	$(65)^2 \bmod 83 = 75$
1	0	$y \leftarrow 65$	$(75)^2 \bmod 83 = 64$
2	1	$y \leftarrow 64 \times 65 \bmod 83 = 10$	

Shared Secret key = 10 k

(22) $q = 353$, $\alpha = 3$, $x_a = 97$, $x_b = 233$

$y_A = (\alpha)^{x_A} \bmod q$

$y_A = (3)^{97} \bmod 353.$

$y_A = 0$

2	97	1
2	48	0
2	24	0
2	12	0
2	6	0
2	3	1
	1	

i	x_i	y	a
0	1	$y \leftarrow 3 \times 1 \bmod 353 = 3$	3
1	0		$81 \bmod 353 = 81$
2	0		207
3	0		136
4	0		0
5	1	$3 \times 0 = 0$	

$y_B = (\alpha)^{x_B} \bmod q$

$y_B = (3)^{233} \bmod 353$

2	233	1
2	116	0
2	58	0
2	29	1
2	14	0
2	7	1
	3	1

i	x_i	y	a
1	→	$y \leftarrow 3$	$a \leftarrow 9$
0	→	y →	$a \leftarrow 81$
0	→	→	$a \leftarrow 207$
1	→	$y \leftarrow 248$	$a \leftarrow 136$
0	→	y →	$a \leftarrow 140$
1	→	$y \leftarrow 102$	$a \leftarrow 185$
1	→	$y \leftarrow 111$	$a \leftarrow 337$
1	→	$y \leftarrow 248$	→

$y_B = 248$ ✓

Now, we calculate Symmetric Key -

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

$K_A = (248)^{97} \bmod 353$

i	x_i	y	a
0	1	$y \leftarrow 248 \times 1 \bmod 353 = 248$	$a \leftarrow (248)^2 \bmod 353 = 82$
1	0	→	$a \leftarrow 17$
2	0	→	$a \leftarrow 289$
3	0	→	$a \leftarrow 213$
4	0	→	$a \leftarrow 185$
5	1	$y \leftarrow 185 \times 248 \bmod 353$	
		$y \leftarrow 352$	

97 | 1
2 | 48 0
2 | 24 0
2 | 12 0
2 | 6 0
2 | 3 1
1
1

353) 61504 (174
353
2620
2471
1494
1412
82

353) 45880 (130
353
1058
706
352

1
353) 45369 (128
353
1006
706
3009
2824
185

19
353) 6724 (19
353
3194
3177
17

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

$K_B = (0)^{233} \bmod 353$

$K_B = 0$

THE END

Date:- 01/11/18 Day:- Thursday

Unit - 5

I.P. Security

Intro It is the capability that can be added to either current version of the internet protocol IP version 4 or 6 but means of additional headers. It is encompasses there functional areas: authentication, confidentiality & key management.

It defines a no. of techniques for key management.

→ Application of IP sec ⇒ It provides the capability to secure communication across a LAN, across private & public WAN & across the internet.

1. Secure Branch office connectivity over the internet.
2. Secure Remote Access over the internet
3. Establishing extranet & Intranet connecting with partners.
4. Enhancing electronic commerce security.

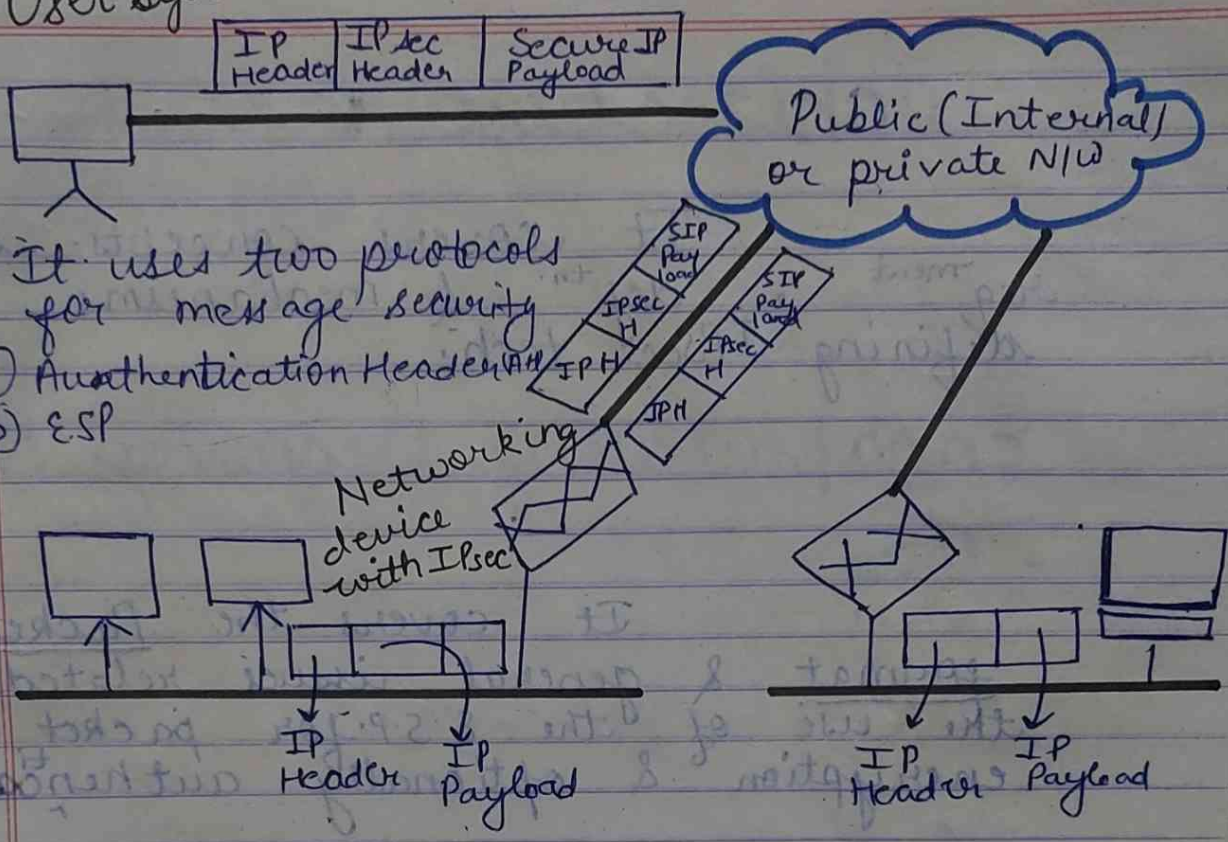
Repeated

Establishing Extranet & Intranet connectivity with partners.

Enhancing electronic commerce security.

* IPsec has two modes of operation (i) Transport mode (ii) Tunnel mode

User System with IPSec

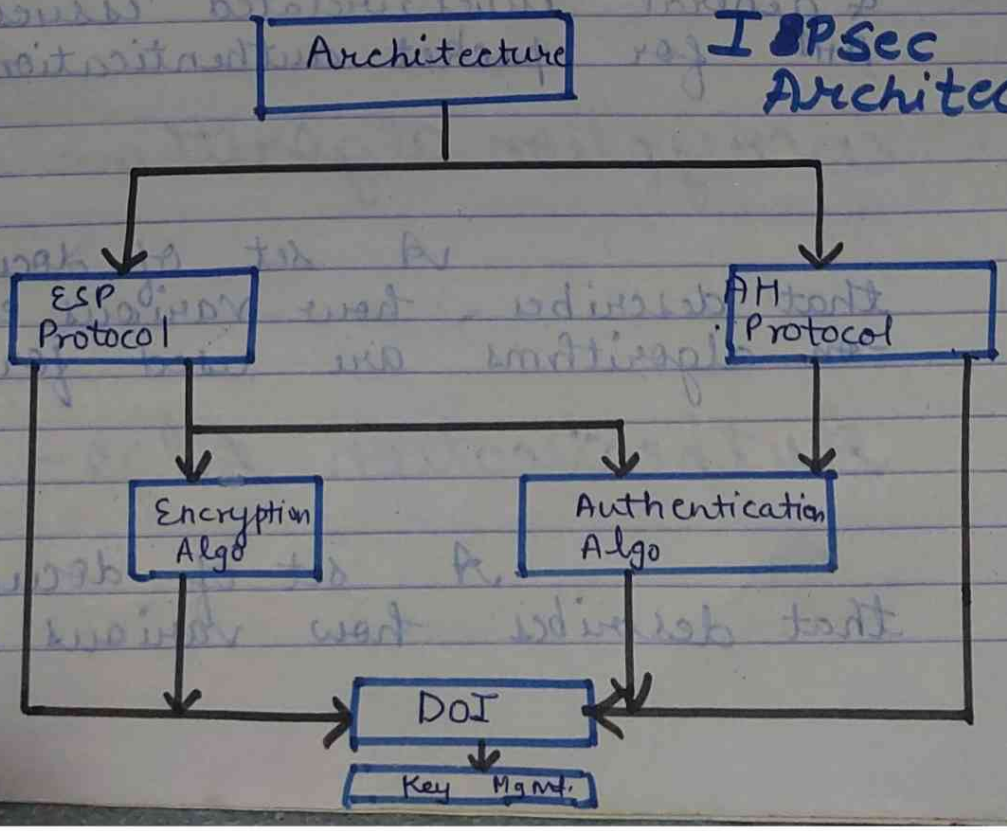


* It uses two protocols for message security
  (a) Authentication Header (AH)
  (b) ESP

Fig An IPSec Overview

IPsec document Overview

IPSec Architecture



Architecture :

It covers concepts, sec req^ment, def^th. & mechanisms defining IPSec tech.

Encapsulating Security Pay-load-

It covers the Packet format & general issues related to the use of the E.S.P. for packet encryption & optionally authentication.

Authentication Header-

Covers the packet format & general issues, related issues of AH for packet authentication.

Encryption algorithm-

A set of documents that describes how various encryption algorithms are used for E.S.P.

Authentication Algo-

A set of documents that describes how various authen-

- tication are used for A.H. & for the authentication option for E.S.P.

Domain of Interpretation (D.O.I

Contains values needed for the other document to relay to each-other.

Key Mgmt. -

Documents that describes Key mgmt. schemes.

imp → IPSec Services -

It provides security services at the IP layer with the help of two protocols - An authentication protocol A.H. & Combined Encryption/ Authentication protocols.

The services are -

~~A.H.~~	A.H.	ESP	ESP (both)
Access Control	✓	✓	✓
Connectionless Integrity	✓	X	✓
Data origin authentication	✓	✓	✓
Rejection or Replayed packets	✓	✓	✓

Confidentiality	X	✓	✓
Limited Traffic flow confidentiality	X	✓	✓

Date- 02/11/18

A security association is uniquely identified by 3 parameters-

1. Security Parameter Index.
2. IP destination address.
3. Security Protocol Identifier

modes of IPsec

Transport & Tunnel mode-

Both A.H. & E.S.P. support two modes of use - Transport & Tunnel mode

	Transport mode SA	Tunnel mode SA
AH	Authenticates IP payload & selected options of IP header & IP version-6 extension header.	Authenticates entire inner IP Packet & selected portions of outer IP extension header.
ESP	Encrypts IP payload & any IP version-6 extension header following the ESP header.	Encrypts entire inner IP Packets.

ESP with authentication	ESP with authentication encrypts IP payload & any IP version-6 extension header following the ESP header, authenticates IP payload but not IP header.	Encrypts entire inner IP Packets. Authenticates inner IP Packets.

imp E.S.P. (Encapsulating Security Payload) -

It provides confidentiality services, including confidentiality of messages & limited traffic - flow. It can also provide Authentication service.

imp E.S.P. Format :-

It contains the following fields -

→ Security Parameter Index - (32-bits)

Identifies a security association.

→ Sequence no. - (32-bits)

An increasing counting value provides an anti replay function as discussed for A.H.

→ Payload data (variable) —:

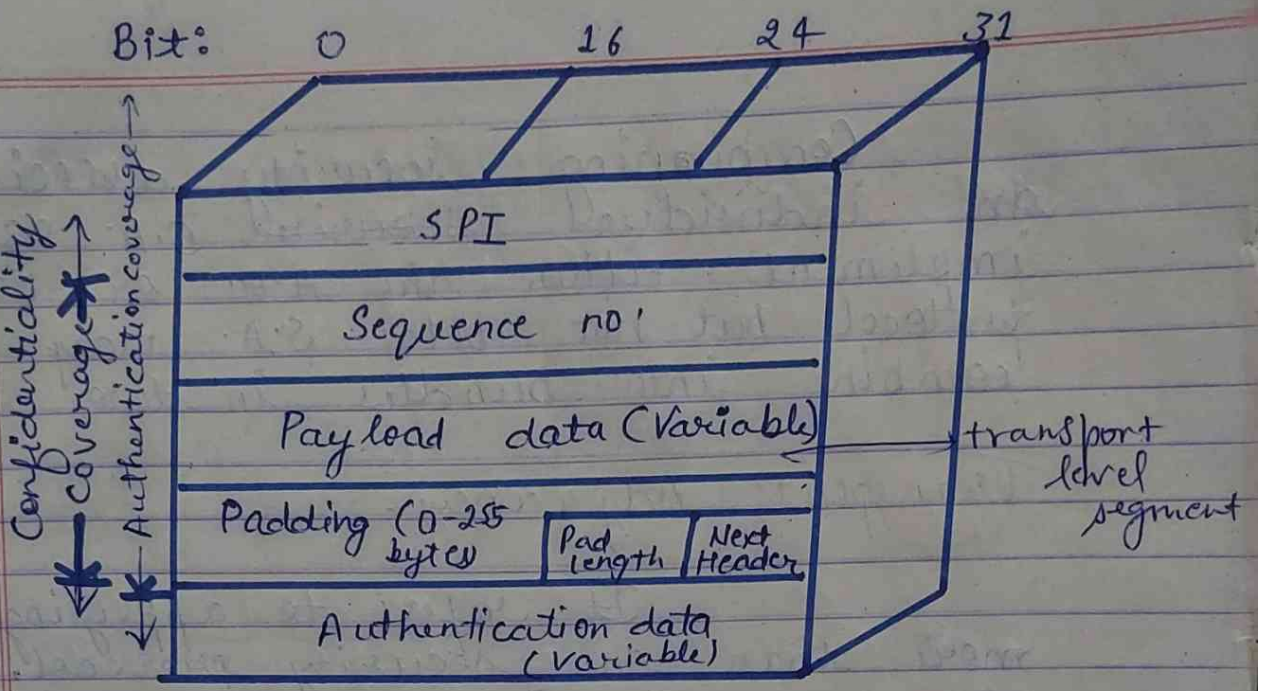
This is a transport level segment of IP Packet (Tunnel mode) i.e. protected by encryption

→ Padding (0 – 255 bytes) –

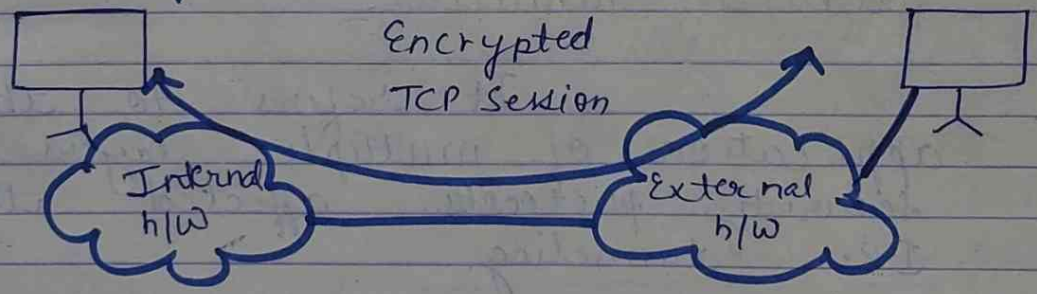
* Pad length (8-bits) – Indicates the no. of 8-bits immediately preceeding this field.

* Next Header (8-bits) – Identifies the types of data contained in the payload data-field by identifying the first header in that payload.

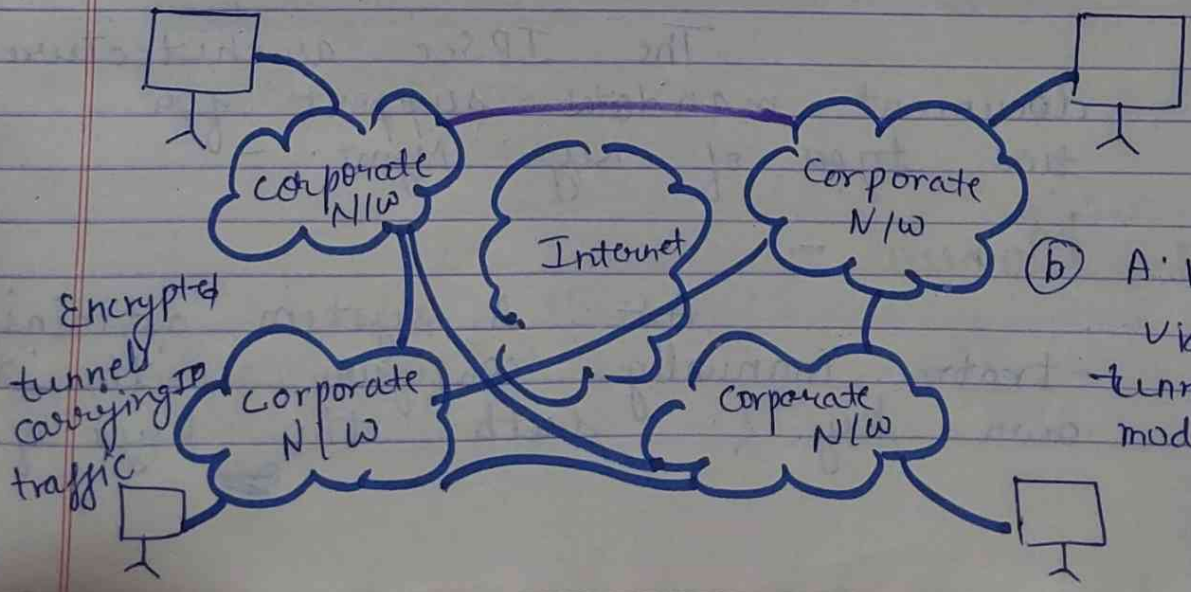
→ Authenticated data (a variable length field)



Transport & Tunnel mode



(a) Transport level security



(b) A VPN via tunnel mode

Date:- 12/11/18 Day:- Monday

Combining security associations.

An individual ~~securit~~ S.A. can implement either the A.H. or E.S.P. protocol but not both. S.A. may be combine into bundles in two ways -

Transport Adjacency -

It refers to applying more than one security protocol to the same I.P. Packet without invoking tunneling.

Iterated Tunneling -

It refers to the application of multiple layers of security protocols affected through I.P. tunneling.

KEY Management -

The IPSec architecture document mandates support for two types of Key- Mgmt. -

1. Manual -

A system administrator manually configure with its own key & with the keys of

other communicating system.

2. **Automated -**

An automated system enables the on demand creation of keys for security association & facilitate the use of keys in a large distributed system with an evolving configuration.

Imp **Internet Security Association & Key Mgmt. protocol - (Oakley) -**

consists of following elements -

1. **Oakley Key determination protocol -**

It is a key exchange protocol based on the diffie-hellman algorithm & but providing adding security.

2. **ISA KMP -**

It provides a framework for the internet key mgmt. & provides the specific protocol support including formats for negotiation of security attributes.

Features of Oakley -

Oakley is a refinement of the Diffie-Hellman Key Exchange algorithm.

It has two attractive features -

(i) Secret keys are created only when needed. There is no need to store secret keys for a long period of time.

(ii) The exchange requires no pre-existing infrastructure other than an agreement on the global parameters

It has 5 important features -

(a) It employs a mechanism k/a cookies.

(b) It enables the two parties to negotiate a group.

(c) It uses nonce to ensure against replay attacks.

(d) It enables the exchange of diffie

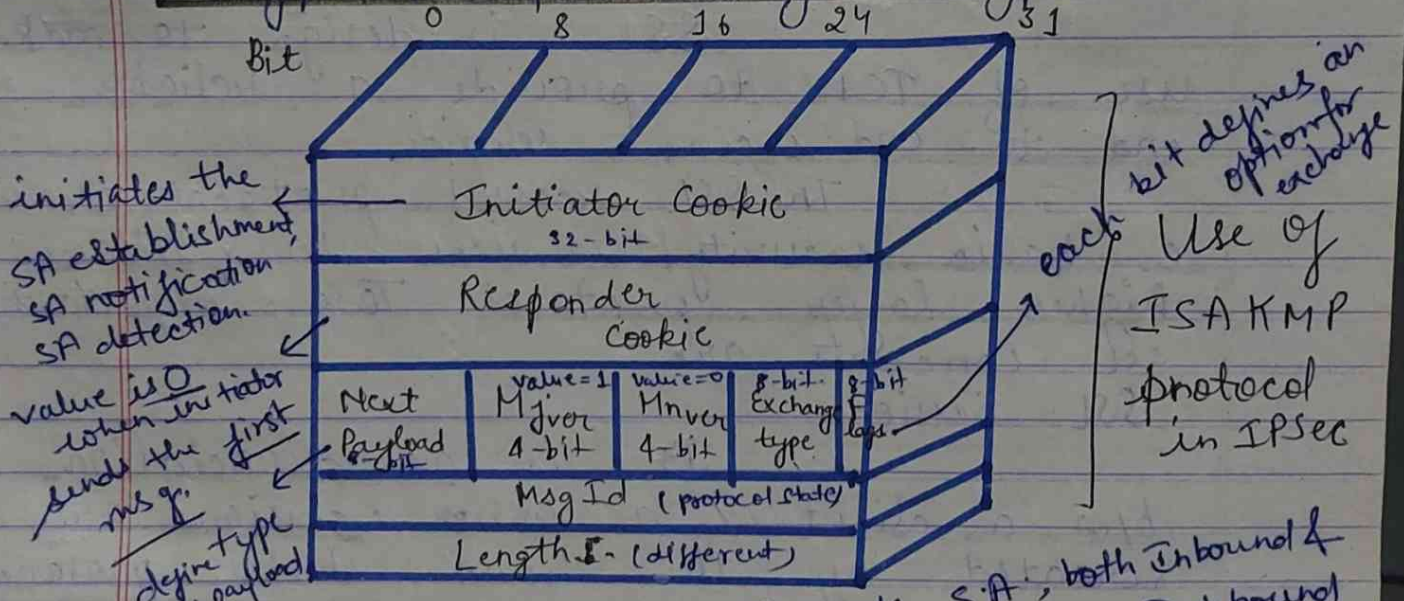
hellman public key values.

(e) It authenticates the diffie-hellman key exchange to thwart man in the middle attack.

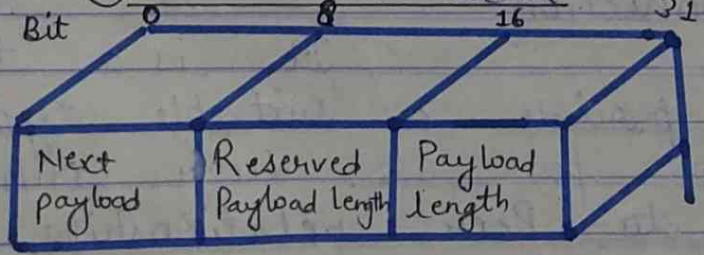
Date 13/11/18 Day:- Tuesday

3 different Authentication method

with Oakley can be used digital signature, symmetric key encryption, public-key Encryption.



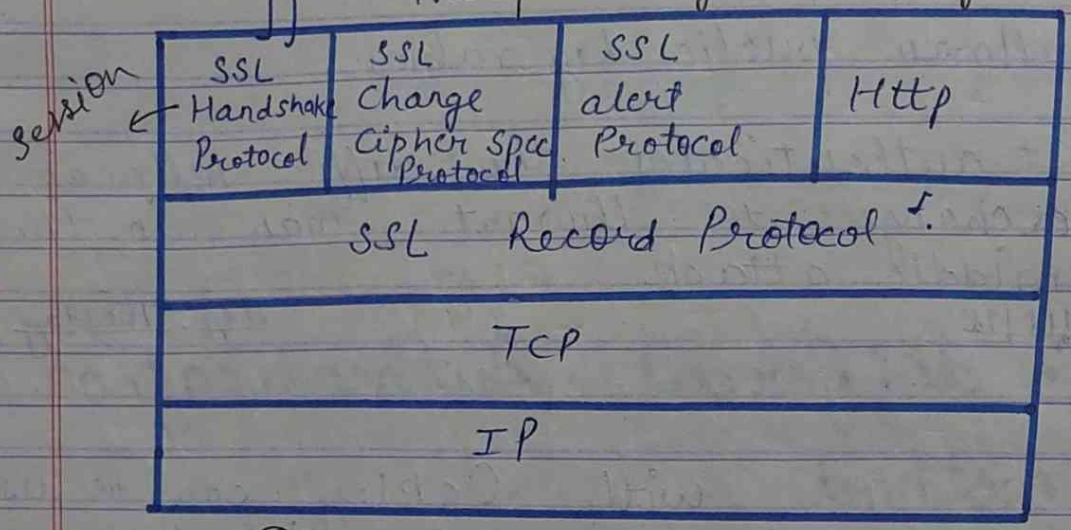
(a) ISA KMP header



(b) Generic Payload header

SSL & TLS - Architecture

Transport layer Security



ⓐ SSL Protocol Stack

SSL is design to make use of TCP to provide a reliable end to end secure service

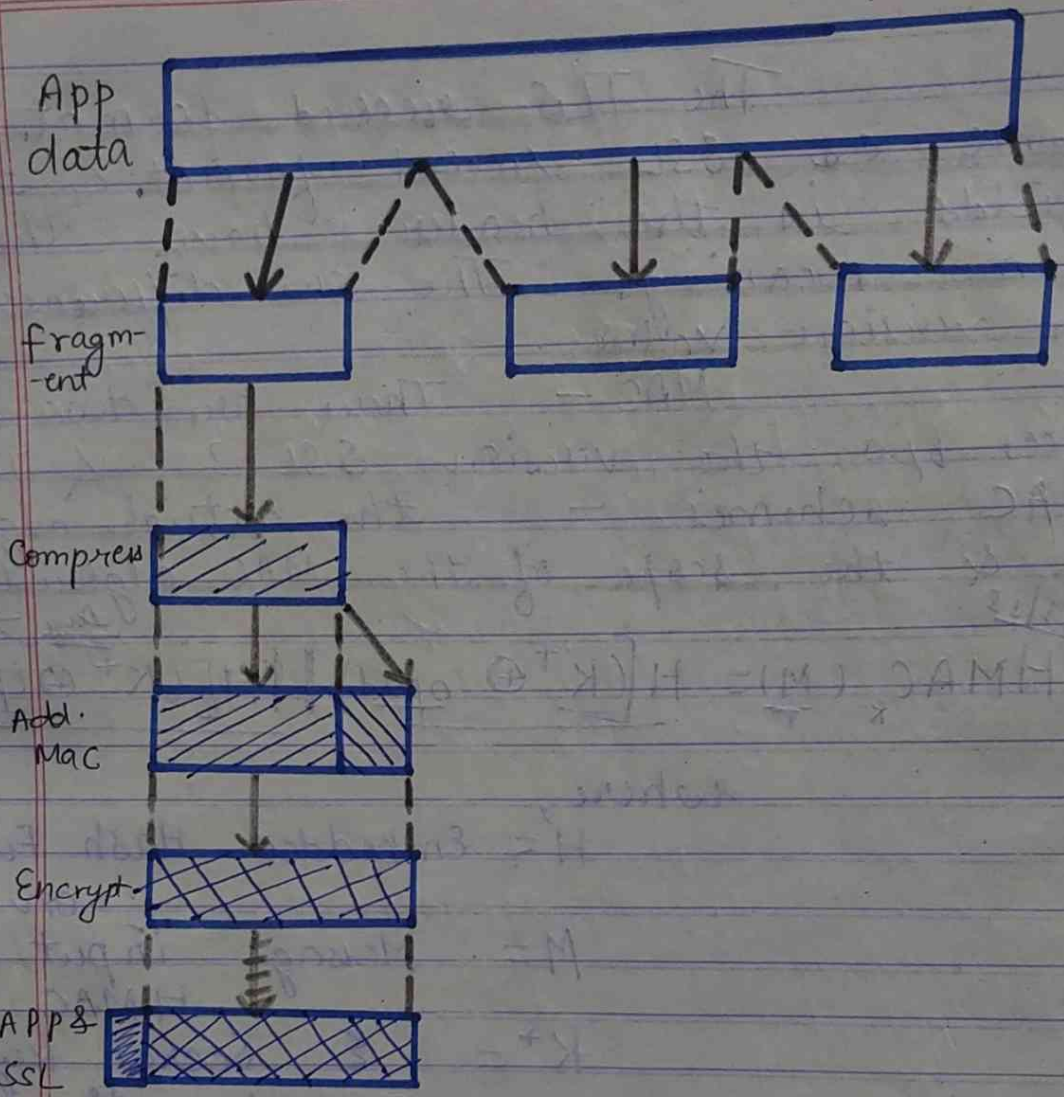
The SSL record protocol provide basic security services to various higher layer protocol. Two important SSL concepts are -

SSL Session -

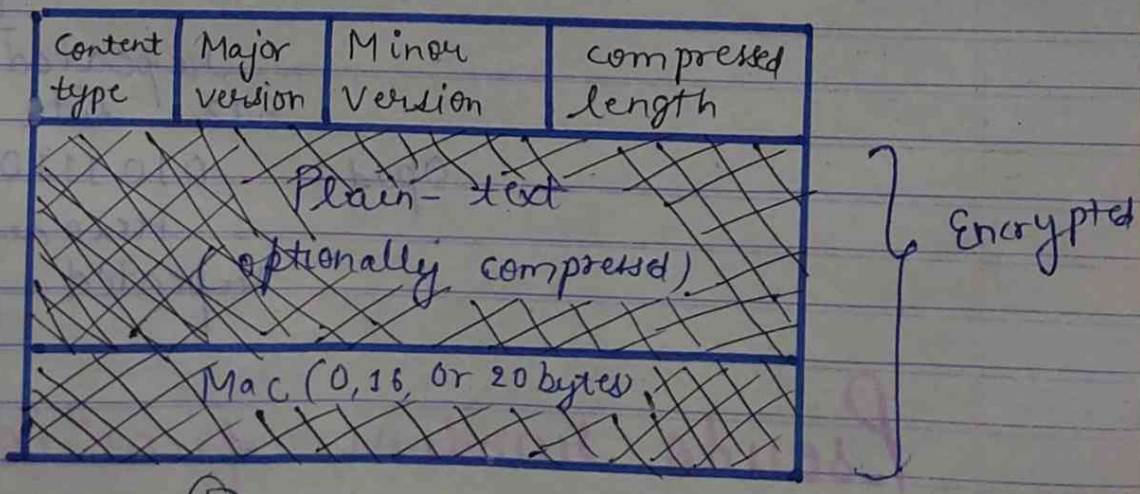
It is an association b/w a client & a server. sessions are created by the hand-shake protocols

SSL connection -

It is a transport that provide a suitable type of service for SSL such connections are- Peer-to-Peer relationships. Every connection is associated with one session.



(a) SSL Record Protocol Operation



(b) SSL Record format

The TLS record format is same as SSL record format & the fields in the header have the same meaning. The one difference is in version values.

MAC - There are two differences b/w the version SSL-3 & TLS: MAC schemes - the actual algorithm & the scope of the MAC algorithm.

Date - 15/11/18 Day - Thursday

$$HMAC_K(M) = H[(K^+ \oplus opad) || H[(K^+ \oplus ipad) || M]$$

where,

H = Embedded Hash Function

M = Message input to HMAC

K^+ = & Secret key added with 0 to the left.

ipad = 00110110 (36 in Hexadecimal) repeated 64 times 512 bits

opad = 01011100 (5C in Hexadecimal) repeated 64 times (512 bits)

Pseudo random function -

TLS makes use of a pseudo random function to expand secrets into blocks of data for purposes of key generation & validation.

The PRF is based on the following data expansion function -

P_hash(secret, seed) = HMAC_hash (secret, A(1) || seed) || HMAC_hash (secret, A(2) || seed) || HMAC_hash (secret, A(3) || seed) || ..... ;

where A() is defined as -

A(0) = seed

A(i) = HMAC_hash (secret, A(i-1))

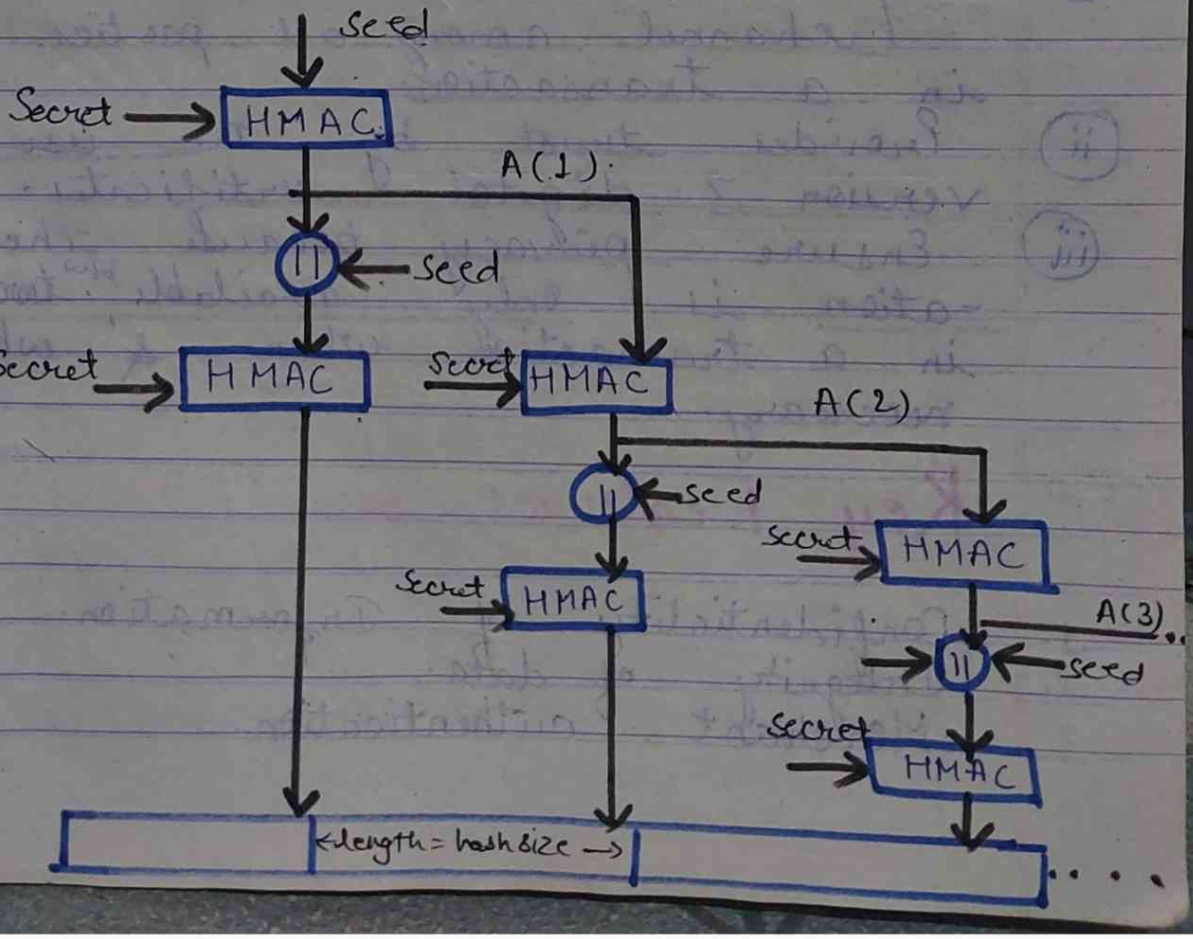


fig:- TLS function - P_hash(secret, seed)

SET:- (Secure Electronic Transaction)

It is an open function encryption & security specification design to protect credit-card transaction on the internet. SET is not itself a payment system whether it is a set of security protocol & formats that enable users to employ the existing credit-card payment infrastructure on an open n/w such as the Ethernet in a secure fashion. It provides 3 services -

(i) provides a secure communication channel among all parties involved in a transaction.

(ii) Provides trust by the use of X.509 version 3 digital certificates.

(iii) Ensure privacy because the information is only available b/w two parties in a transaction when & where necessary.

Key Features of SET-

1. Confidentiality of Information.
2. Integrity of data.
3. Merchant authentication.

4. Card holder a/c authentication.

SET Participants -

Card Holder -

It is an authorize holder of an payment card.

Merchant -

It Merchant is a person or organization that has goods or services to sell to the card-holder.

Issuer -

This is a financial institution such as- bank that provides the card-holder with the payment card.

Acquirer -

Establishes an a/c with merchant & processes payment card authorization & payment.

Payment - Gateway -

This is a function operated by the acquirer or a

Sequence of events -

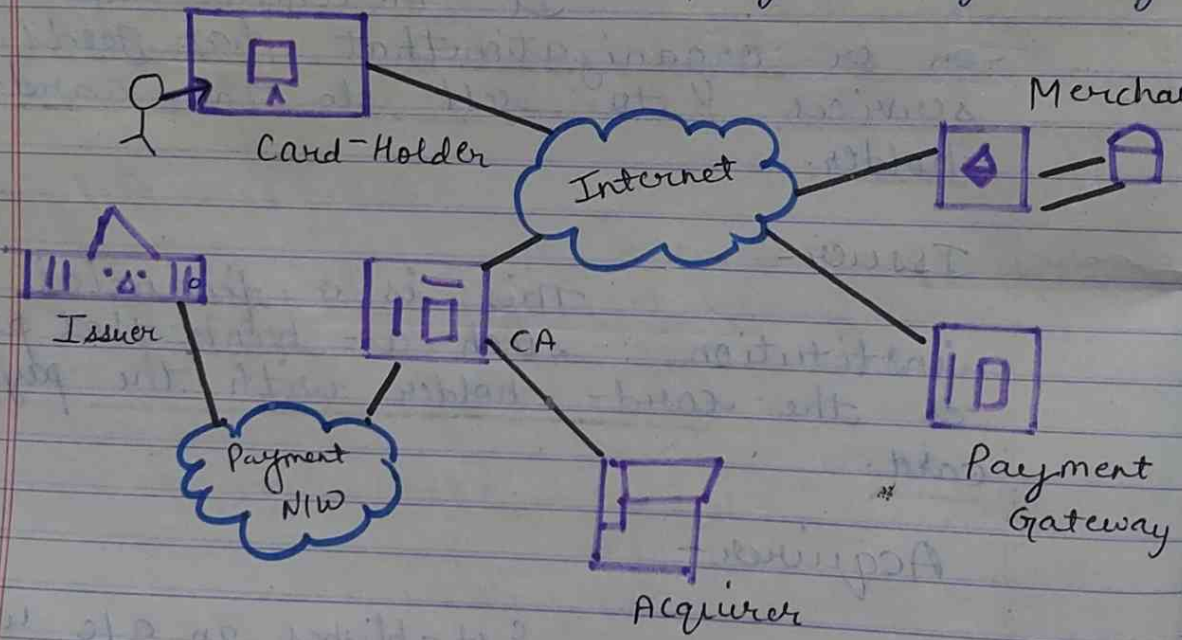
(7) The merchant requests payment authorization
(8) The merchant confirms the order & provide goods & services
(9)
(10) The merchant requests payment

(1) The customer opens an account
(2) The customer receives a certificate
(3) Merchant have their own certificates
(4) The customer places an order
(5) The merchant is verified
(6) The order & payment are sent

3 party designated merchant payment that processes messages.

Certification Authority -

This is an entity i.e. trusted to issues X.509 version 3 public key certificates for card-holders, merchants & payment gateways.



Secure Electronic commerce components -

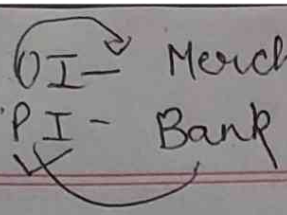
Date: 16/11/18

Day: - Friday

imp

Dual Signature.

The purpose of the dual signature is to link two messages that



are intended for two different recipients. In this case, the customer wants to send the order information (OI) to the merchant & the payment information PI to the bank. The merchant does not need to know the customers credit card no. & the bank does not need to know the details of the customer's order.

To see the need for the link suppose that the customer send the merchant two messages a signed OI & PI & the merchant passes PI to the bank.

If the merchant can capture another OI from this customer, the merchant could claim that this OI goes to the PI rather than the original OI.

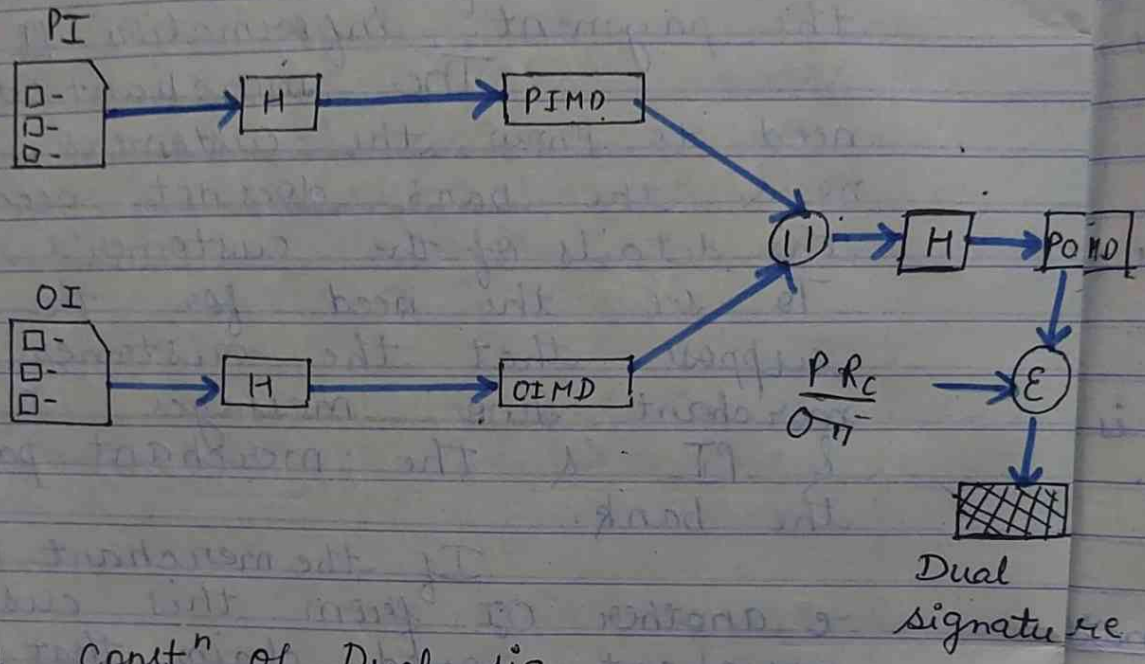
The linkage prevent this.

Creation of Dual Signature-

$$D.S = E(PR_c, [H(H(PI) || H(OI))])$$

The customer takes the hash of the P.I. & O.I. These two hashes are then concatenated & the hash of the result is taken. Finally the customer encrypts the final hash with his/her private signature key. Thus, creating the dual signature.

PR_c = customer's private signature



eg Const^n of Dual sign

where - H = Hash function (SHA1)

|| = concatenation

PIMD = Payment Information message digest

OIMD = Order info. message digest

POMD = Payment Order Message digest

ε = Encryption (R.S.A)

H(PIMD || H(OI)) ?2
D(PU_c, DS)

The merchant is in possession of dual-signature, OI & the message digest for the PI.

The merchant also has the public-key of the customer taken from the customer certificate then the merchant can compute the following -

H(PIMD || H(PI))
D(PU_c, DS)

PU_c = Customer's public signature key

If these two quantities are equal then the merchant has verified the signature.

The bank can compute -

H(H(PI) || OIMD),
D(PU_c, DS)

If these two equations are equal, the bank has verified the signature.

Intrusion Detection -

Unauthorized intrusion into a computer system or n/w

is one of the most crucial threat to computer security. Intrusion detection system to provide early warning of an intrusion, it involves detecting unusual pattern of activity or patterns of activity that are known to co-relate with intrusion. There are 3 classes of intruder's -

1. Masquerader -

An individual who is not authorized to use the computer.

2. Misfeasor -

A designate legitimate user to accesses data, programmes or resources for which such access is not authorized.

3. Clandestine User -

An individual who seizes supervisely control of the system & uses this control to evade auditing & access controls or to suppress audit collection.

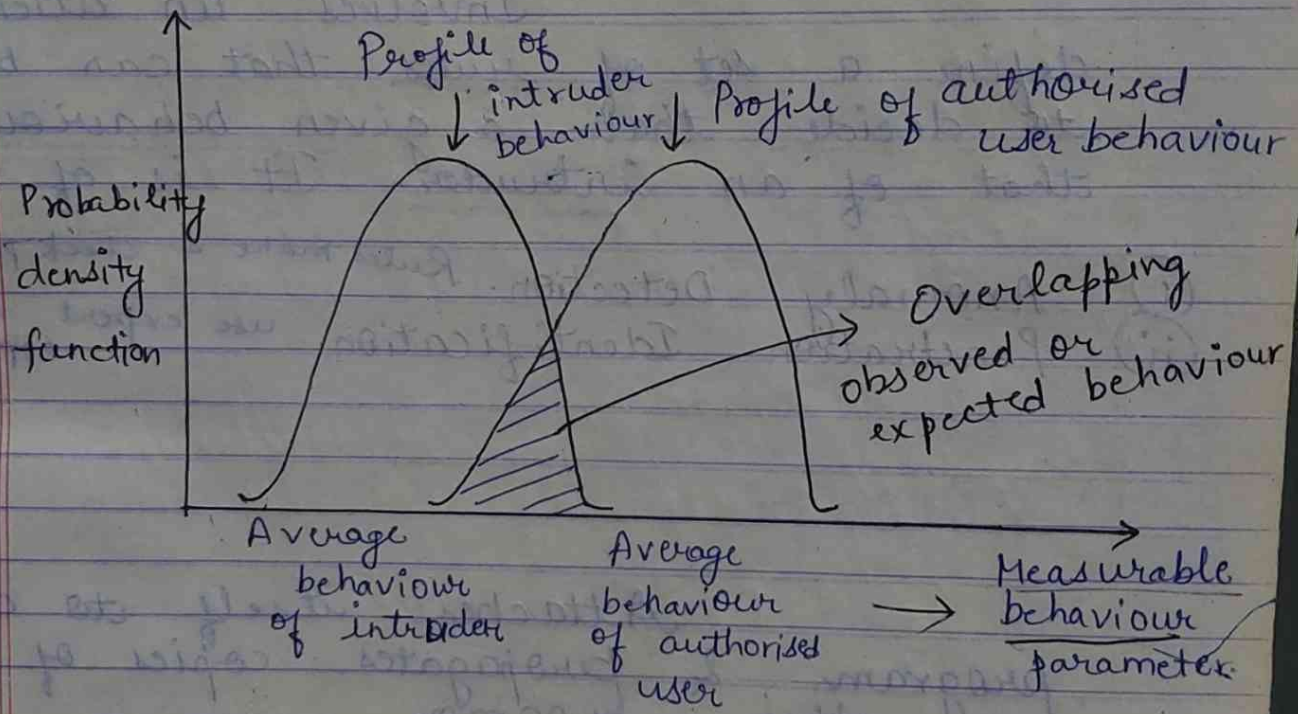
Intrusion Techniques -

1. One way function -

The system stores

only the value of function based on the user's password.

2. Access Control- Access to the password file is limited to one or a very few accounts



imp Approaches to Intrusion-Detection-

1. Statistical Anomaly Detection-

It involves the collection of data relative to the behaviour of legitimated over a period of time.
It is of 2 types-

(2) Threshold detection - at record frequency of event occuring
Profile Based Profile identify activity

(2i) Rule Based Detection -

Involves an attempt to define a set of rules that can be used to decide that a given behaviour is that of an intruder. It is of 2 types -

(i) Anomaly Detection. Rules make & check pattern
(ii) Penetration Identification. use expert system approach.

Virus -

Attaches itself to a program & propagates copies of itself to other program.

During its life-time a typical virus goes to the following 4 phases.

1. Dormant - Phase - idle

The virus is idle. It will eventually be activated by some event, the presence of another program or file.

2. Propagation Phase -

The virus places an identical copy of itself into other programs or into certain system areas on the disk.

3. Triggering Phase -

The virus is activated to perform the function for which it was intended.

4. Execution Phase -

The function is performed. The function may be harmless such as a message on the screen. Or damaging such as distraction of program & data files.

Types of Virus :-

1. Parasitic, Memory resident virus, boot
* sector virus.
2. Stealth virus,
3. Polymorphic virus
4. Metamorphic virus

Firewalls -

It can be an effective

A firewall protects networked computers from intentional hostile intrusion that could compromise confidentiality or result in data corruption

means of protecting a normal system from network based security thrust while at the same time efforting access to the outside world via WAN & the Internet.

Characteristic -

All traffic from inside to outside & vice-versa. must pass to the firewall.

Only authorized traffic as defined by the local security policy will be allow to pass further.

It itself is immune to penet-eration.

It focuses on service control more but also provide best controls -

1. Service control - It may filter traffic on the basis of IP address & TCP portal.

2. Direction Control - Determines

or denial of service.

~~n/w of~~

the direction in which particular service request may be initiated to the firewall.

3. User Control- Controls access to a service according to which user is attempting to access it.

4. Behaviour Control-

Controls how particular services control.

Scope of Firewall-

(1) It can serves as the platform for IPsec.

(2) It defines a single choke point that keeps unauthorized user out of the protected n/w.

(3) It provides a location for monitoring security related events. Audits & Alarms can be implemented of the firewall system.

(4) It is a convenient platform for several internal functions that are not security related.

Types of Firewall -

1. Application level
2. Circuit level
3. Packet - filtering Gateway.

THE END

* **Explain the transport & tunnel modes of IPsec**

Transport mode	Tunnel mode
* IPsec protects what is delivered from the transport layer to the network layer.	IP sec protects the entire IP Packet.
* It does not protects the ~~networ~~ IP header.	* It is normally used b/w two routers, b/w a host & a router or b/w router & a host.
* IPSec header are added to the information coming from transport layer, etc.	* It is used when either the sender or the receiver is not a host & protected from intrusion
* It is used, when we need host - to host protection of data.	
* The receiving host uses IPsec to check the authentication & / or decrypt the IP packet & deliver it to the transport layer.