Chapter-4
Cryptography.
[30 Marks]

Symmetric Encryption Principles :-

Symmetric Encryption Principles has five ingredients (fig-1).

1) Plaintext :- This is the original message or data that is feed into algorithm as I/P.

2) Encryption Algorithm :-
The Encryption algorithm performs various substitutions & transformations on the plain text.

3) ~~Secret Key~~ Cipher text :-
The scrambled message produced as o/p of Encryption algorithm. It depends on plaintext & secret key.

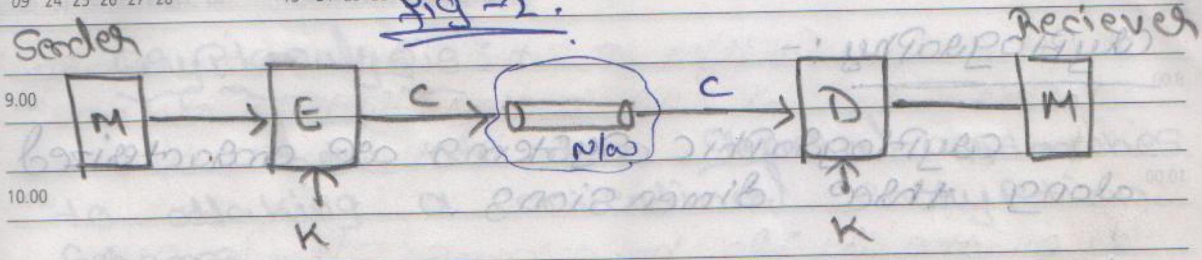
~~4) cipher text :-~~
~~The scrambled message produced as o/p of Encryption algorithm.~~

4) Secret Key :-
The secret key is also I/P to the algorithm. The substitution & transformations performed by algorithm depend on the key.

NOTES

5) Decryption Algorithm :-
This is essentially the encryption algorithm runs in reverse. It takes ciphertext & same secret key & produces the original plaintext.

fig-2.



where.
M:- Plaintext
K: - Secret key
E: Encryption
C: cipher text
D: Decryption.

Cryptography :-

It is defined as scheme for enciphering for Plain text is cryptography

Cryptanalysis :-

Techniques used for deciphering a message without knowledge of encryption details is termed as Process of cryptanalysis.

NOTES

Cryptography :-

Cryptographic systems are characterized along three dimensions.

1) The type of operation used for transforming Plaintext to ciphertext :-

All the Encryption algorithms are based on two general Principles — Substitution, in which each element in Plaintext is mapped to another element and transformation, in which elements of plaintext are re-arranged.

2) The number of keys :-

If both sender & reciever use the same key, the system is reffered as Symmetric/single key/conventional encryption.

If both sender & reciever uses the different keys, the system is reffered as asymmetric/two keys/Public key encryption.

3) The way in which Plaintext is Processed.

The Block-cipher Processes the I/P elements one Block at a time.

The Stream-cipher, Processes the I/P elements continuously Producing one o/p element at a time.

Cryptanalysis :-

There are two general approaches to attaking a conventional encryption schemes.

1) cryptanalysis :-

Cryptanalysis relies on the nature of algorithm plus key used. If intruder gets to know these then all future & past messages encrypted with that key are compromised.

2) Brute Force Attack :-

The Attacker tries every possible key on a piece of cipher-text until it is translated into plaintext.

Imp Feistel Cipher Structure :-

Many symmetric block encryption algorithms have structure described by Horst Feistel as shown fig-②. ⊛ The I/P to encryption algorithm are a plaintext block of 2w bits & key a K.

⊛ The plaintext block is divided into two halves, LE0 & RE_0.

* The two halves of the data pass through 'n' rounds of processing & then combine to produce the cipher text block.

* All the rounds have same structure. A substitution is performed on the left half of the data. This is done by applying a Round function F to the right half of the data. & then taking Exclusive-OR (XOR) of the O/P of that function & the left half of the data. ~~The round~~

* Following this substitution, a permutation is performed that consists of the interchange of two halves of the data.

33

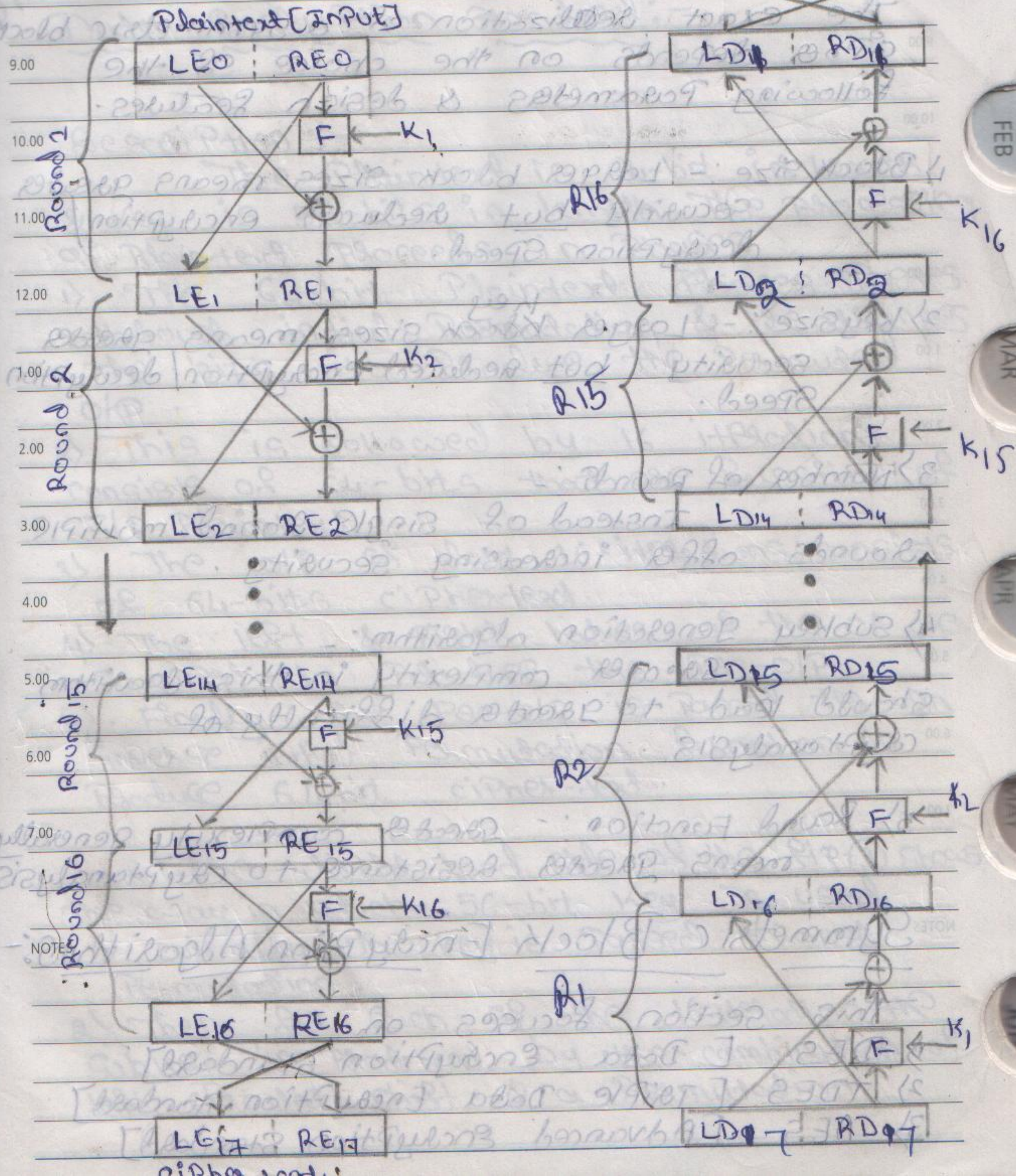
Reciever.

02						February 2014
wk	M	T	W	T	F	S	S

February 2014: wk 05: 1 2; 06: 3 4 5 6 7 8 9; 07: 10 11 12 13 14 15 16; 08: 17 18 19 20 21 22 23; 09: 24 25 26 27 28

March 2014: wk 09: 31, 1 2; 10: 3 4 5 6 7 8 9; 11: 10 11 12 13 14 15 16; 12: 17 18 19 20 21 22 23; 13: 24 25 26 27 28 29 30

2014 Wednesday 08 January 008-357 • WK 02



9.00 10.00 11.00 12.00 1.00 2.00 3.00 4.00 5.00 6.00 7.00 NOTES

The exact realization of a symmetric block cipher depends on the choice of the following parameters & design features.

1) Block size :- Larger block sizes means greater security but reduced encryption/decryption speed.

2) Keysize :- Larger Key sizes means greater security but reduced encryption/decryption speed.

3) Number of Rounds :-
Instead of single round, multiple rounds offer increasing security.

4) Subkey generation algorithm :-
Greater complexity in this algorithm should lead to greater difficulty of cryptanalysis.

5) Round Function :- Greater complexity generally means greater resistance to cryptanalysis.

Symmetric Block Encryption Algorithms:-

This section focuses on
1) DES [Data Encryption Standard]
2) TDES [Triple Data Encryption Standard]
3) AES [Advanced Encryption Standard].

IMP ***

Data Encryption Standard:-

Description:-

The plaintext is 64-bit in length & key is 56-bits in length. The processing of plaintext proceeds in phases.

1) The 64-bit plaintext ~~phases~~ passes through intial permutation & rearranges the bits to produce the permuted O/P.

2) This is followed by 16 iteration consists of 64-bits that are function of I/P plaintext

3) The O/P of last 16-iterations consists of 64-bits ciphertext.

4) The left & right halves of the O/P are swapped to produce the pre-O/P.

5). Finally the pre-O/P is passed through inverse initial permutation function to produce 64-bit cipher-text.

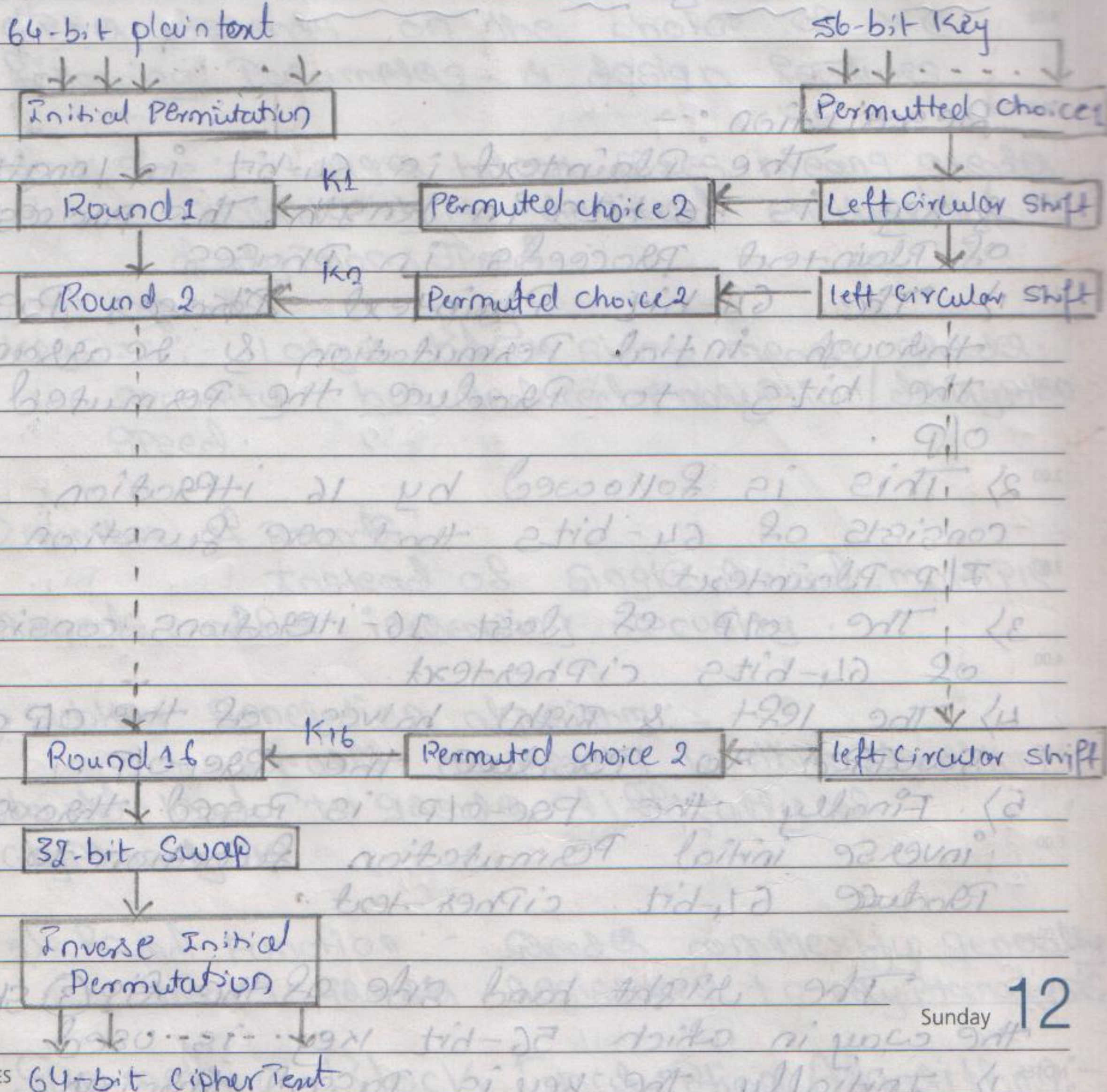
The right hand side of the fig-(3) shows the way in which 56-bit key is used

1) Initially the key is passed through permutation.

2) Then for each of the 16-iteration the subkey is produced by the combination of left circular shift & a permutation.

fig-③

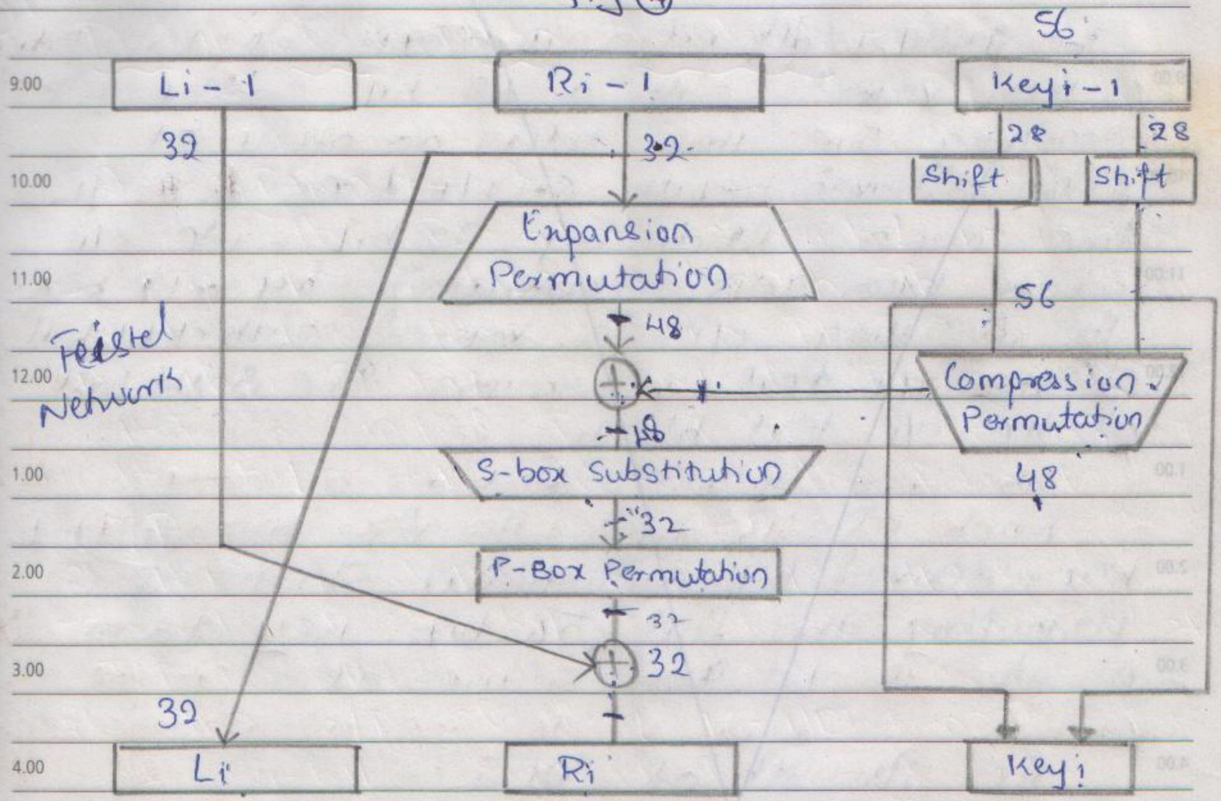
9.00
10.00
11.00
12.00
1.00
2.00
3.00
4.00
5.00
6.00
7.00



Sunday 12

NOTES

fig (4)



The Heart of DES Algorithm is Feistel network shown in fig (4).

The 64-bit block of incoming Plaintext is split into right & left half of 32-bits each. whereas the right half becomes the left becomes the left half of the o/p text block at the end of the round.

The right half enters the expansion permutation & then XORed with a 48-bit wide key. The resulting sum then enters an array of eight S-boxes with 6-I/P lines & 4-O/P line each producing 32-bit wide O/P. which then gets permutted by a P-box. The resulting O/P is XOR-ed with left half of the I/P text & becomes the right half of the O/P text block.

Each of 16-DES Rounds has 48-bit key derived by continually shifting & permuting the full 56-bit key from round to round.

The strength of DES :-

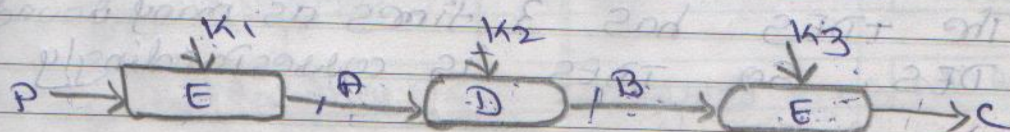
⇒ Larger block sizes means greater security
⇒ " key " " " "
⇒ multiple rounds offer increasing security.
Greater complexity leads to greater difficulty of cryptography.

NOTES

Triple Data Encryption Standard [TDES]

TDES in which DES is applied three times if we consider a triple length key to consist 56-bit keys K_1, K_2, K_3 & block size is 64-bits.

Encryption as follows:

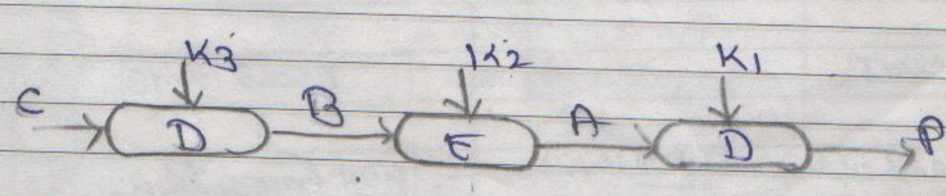


$C = E_{K_3}[D_{K_2}[E_{K_1}[P]]]$

where:

- C = cipher text
- P = Plain text
- E = Encryption
- D = Decryption
- $E_K[x]$ = Encryption of 'x' using key 'K'
- $D_K[y]$ = Decryption of 'y' using key 'K'.

Decryption as follows: It is reverse process of encryption.



$P = DK_1[EK_2[DK_3[C]]]$.

*** Imp

Advanced Encryption Standard : [AES]

The principle drawback of TDES is that Algorithm is sluggish [slow & complex] in S/w & H/w implementation.

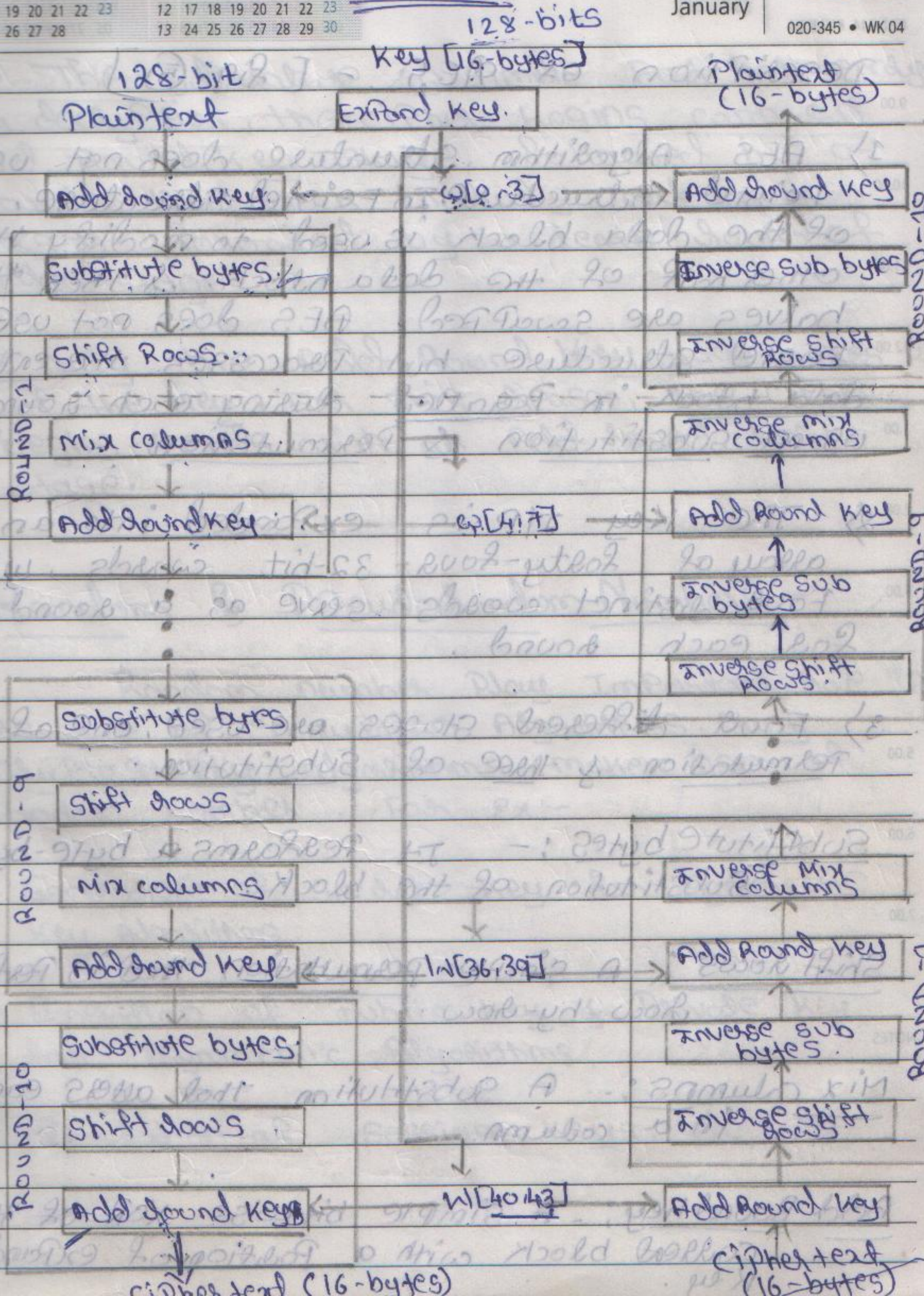
The TDES has 3 times as many rounds as DES, so TDES is correspondingly slow.

The DES & TDES uses Block size of 64-bit. So larger block size adds more security

AES Algorithm uses a Symmetric block encryption. AES support a block size of 128-bits & Key sizes of 128, 192 & 256 bits.

NOTES

fig (5)


128-bits
Key [16-bytes]
128-bit
Plaintext
Expand key.
Plaintext
(16-bytes)
Add Round key.
w[0,3]
Add Round key
Substitute bytes.
Inverse sub bytes
Shift Rows.
Inverse shift Rows
ROUND-1
ROUND-10
Mix columns.
Inverse mix columns
Add Round key
w[4,7]
Add Round key
ROUND-9
Inverse sub bytes
Inverse shift Rows
Substitute bytes
Shift Rows
ROUND-9
Mix columns
Inverse Mix columns
Add Round key
w[36,39]
Add Round key
Substitute bytes
Inverse sub bytes
ROUND-1
ROUND-10
Shift Rows
Inverse shift Rows
Add Round keys
w[40,43]
Add Round key
Ciphertext
(16-bytes)
Ciphertext (16-bytes)

Description of AES :- [fig-⑤]

1) AES Algorithm structure does not use Feistel structure. In Feistel structure, half of the data block is used to modify the other half of the data block, & then the halves are swapped. AES does not use a Feistel structure but processes the entire data block in parallel during each round using substitution & permutation.

2) The key I/P is expanded into an array of forty-four 32-bit words, w[i]. Four distinct words serve as a round key for each round.

3) Four different stages are used, one of permutation & three of substitution:

Substitute bytes :- It performs a byte-by-byte substitution of the block.

Shift rows : A simple permutation that is performed row-by-row.

Mix columns :- A substitution that alters each byte in a column.

Add Round key :- A simple bit-wise XOR of the current block with a portion of expanded key.

4) The structure is simple. For both encryption & decryption, the cipher begins with an Add Round Key stage, followed by 9-rounds that each includes all four stages, followed by a tenth round of three stages.

5) only the Add Round Key stage makes use of the key. For this reason, the cipher begins & ends with an Add round key stage.

Random & Pseudorandom Numbers:-

Random number play important role in the use of encryption Algorithms. Many cryptography algorithms makes use of Random number. For Ex:-

1) Generation of secret key for Symmetric key Algorithms.

2) Generation of Public key & Private key for Asymmetric Algorithms.

3) Generation of session keys. etc.

The Random number can have uniform distribution of bits or Independence

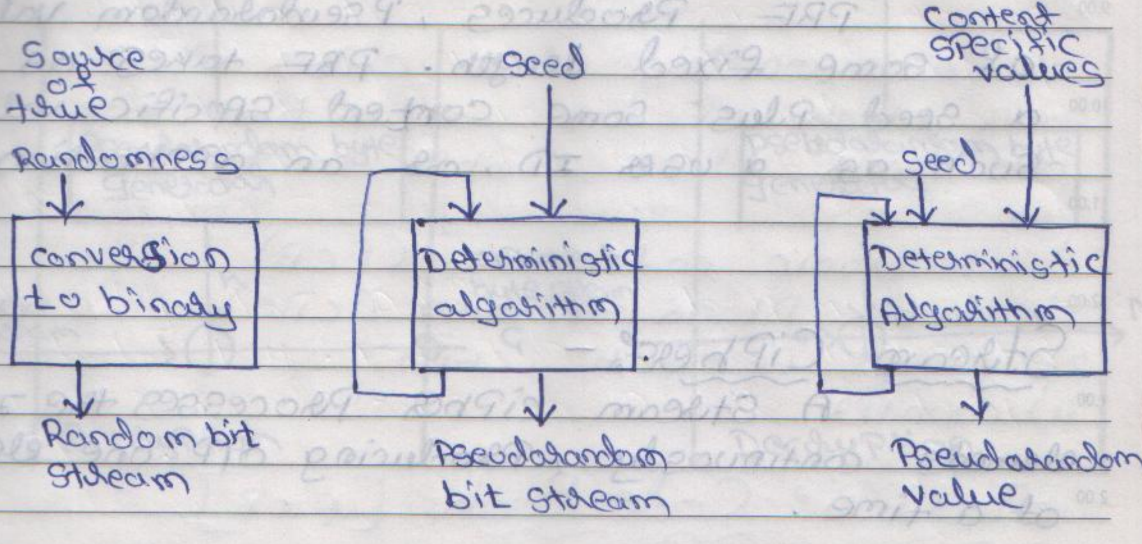
Uniform distribution:-
The distribution of bits in the sequence should be uniform; that is the frequency of occurrence of ones & zeros should be approximately the same.

Independence:
There is no dependence between the occurrence of ones & zeros.

The Random numbers are generated using the following algorithm.

1) TRNG's [True Random number Generator]
2) PRNG's [Pseudorandom number generator]
3) PRF's [Pseudorandom Function]

TRNG: [reffer fig (a)]
TRNG takes a I/P a source that is effectively random. The source could be timming Pattern, mouse movements, & instantaneous values of the system clock.
The source, serves as I/P to an Algorithm that Produces random binary O/P.



[a] TRNG [b] PRNG [c] PRF

TRNG involve conversion of an anlog source to a binary o/p.

PRNG [reffer - fig(b)]

PRNG takes I/P a fixed value called seed. & Produces a sequence of o/p bits using deterministic algorithm. There is some feedback path by which results of algorithm are fed back as I/P as additional o/p bits are produced.

PRF : [reffer - fig(c)]

PRF Produces, Pseudorandom value of some fixed length. PRF takes as I/P a seed plus some content specific values such as a user ID, or an application ID.

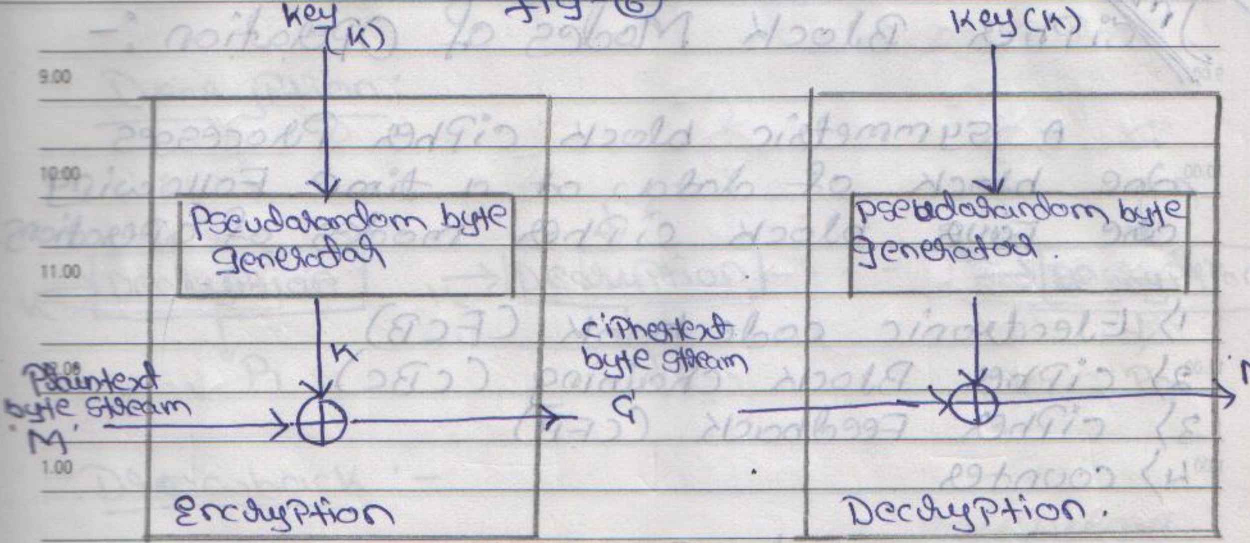
Stream Ciphers:-

A stream cipher processes the I/P elements continuosly, producing O/P one element at a time.

Stream [2] cipher structure:-

The fig-6 shows the stream cipher structure. In this structure, a key is I/P to a pseudorandom bit generator that produces a stream of 8-bit numbers that are random. The O/P of the generator, called a keystream is combined one byte at a time with the plain text stream using the bitwise exclusive-OR [XOR] operation. For example, if the keystream generated by generator is 01101100, & the plaintext byte is 11001100 then the resulting ciphertext byte is.

fig-⑥



11001100 → Plaintext
⊕ 01101100 → Key stream
10100000 → cipher text.

Decryption requires the use of the same pseudorandom sequence.

10100000 → ~~Plaintext~~ cipher text
⊕ 01101100 → key stream
11001100 → Plaintext.

NOTES

Imp

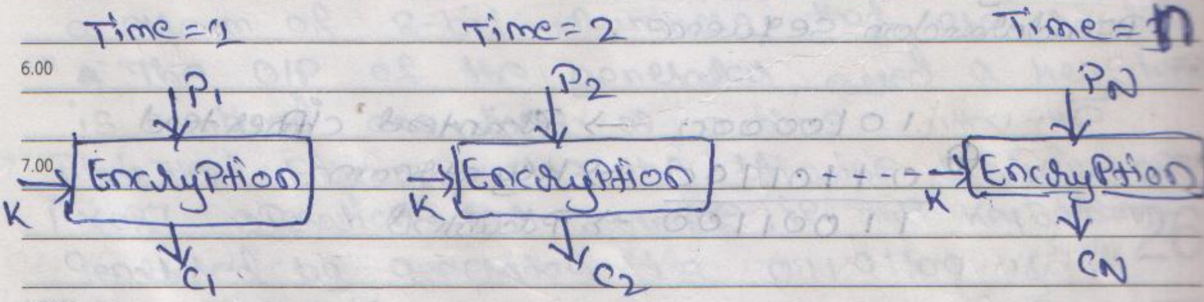
Cipher Block Modes of Operation :-

A symmetric block cipher Processes one block of data at a time. Following are Four block cipher modes of operation

1) Electronic code book (ECB)
2) cipher Block chaining (CBC)
3) cipher Feedback (CFB)
4) counter.

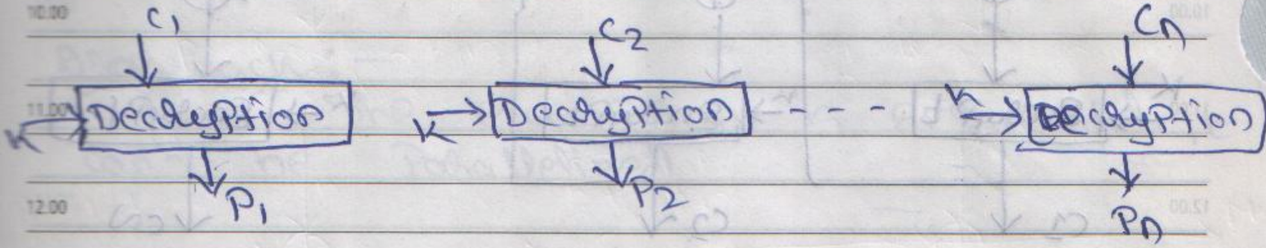
Electronic Code Book [ECB]

In ECB the Plaintext is handled one block at a time and each block of Plaintext is encrypted using the same key.



Encryption

Decryption:



Drawback :-

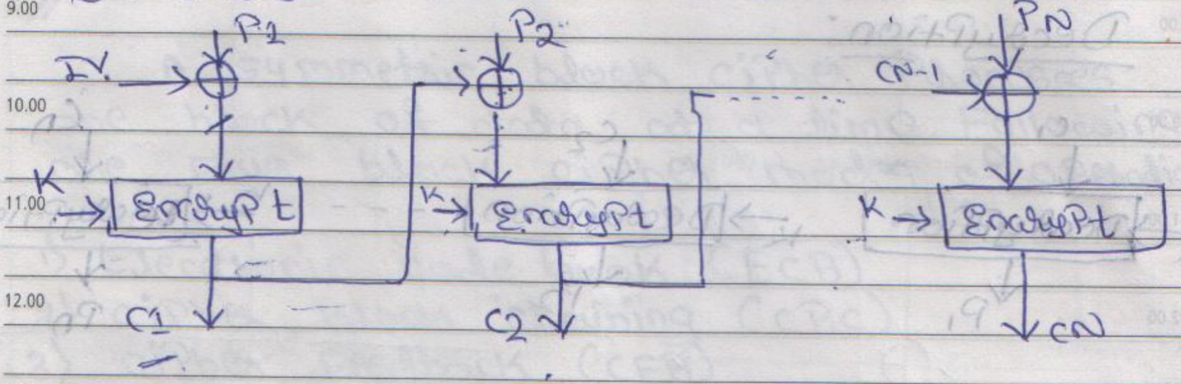
If same 'b'-bit block of Plaintext appears more than once in the message, it always produces the same ciphertext for lengthy messages, the ECB mode may not be secure.

Cipher Block Chaining [CBC]

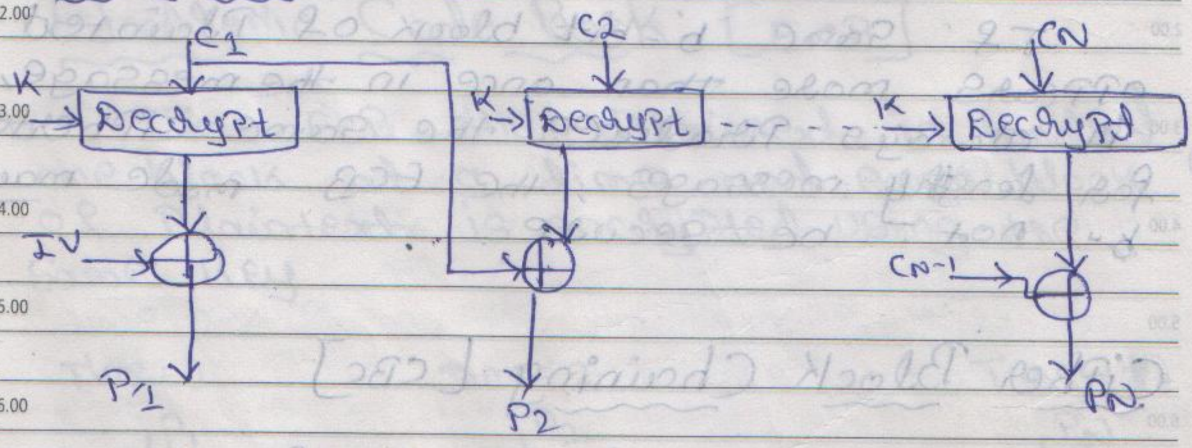
To over come drawback of ECB, CBC is introduced. In this CBC, the I/P to Encryption algorithm is XOR of the current Plaintext block & the preceding ciphertext Block, the same key is used for each block.

For Decryption, each cipher block is passed through the decryption algorithm the result is XOR-ed with the preceding cipherblock to produce to Plaintext

Encryption :-



Decryption :-



To Produce the first block of ciphertext an initialization vector (IV) is XOR-ed with first block of Plaintext. On decryption the IV is XOR-ed with O/P of the decryption algorithm to recover the first block of Plaintext

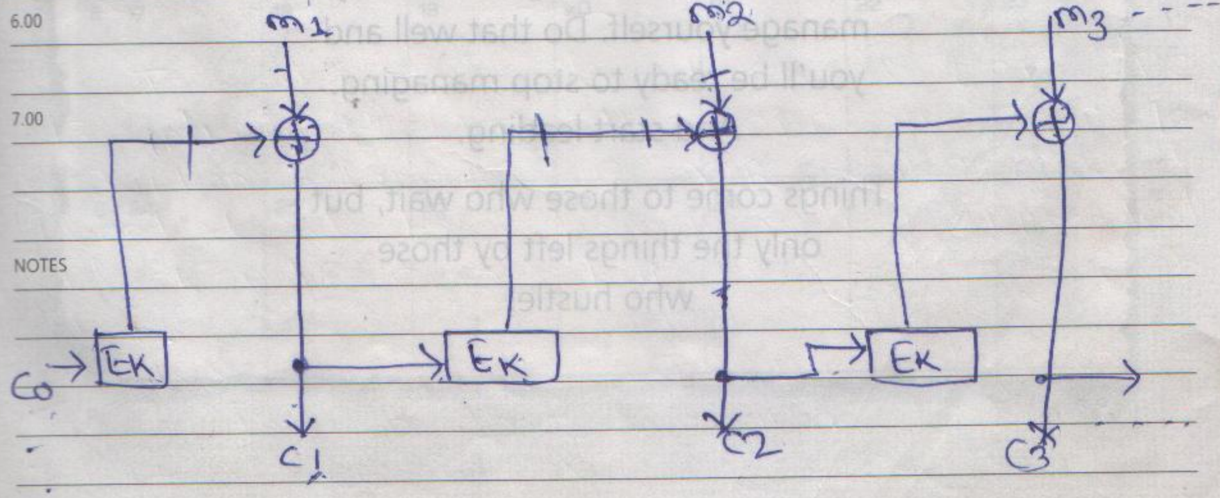
$E_K(P)$

NOTE :- The IV must be known to both the sender & reciever but unpredictable by third party.

Drawback :-
The encryption is sequential it can't be parallelized.

Cipher Feedback Mode :- [CFB]

In CFB the previous ciphertext block is encrypted & O/P produced is combined with the plaintext block using XOR to produce the current ciphertext block.
An initilization vector "C_0" is used as "seed" for the process.



Counter Mode :-

For encryption, the counter is encrypted & then XORed with plaintext block to produce the ciphertext block; there is no chaining. For decryption, the same sequence of counter values is used, with each encrypted counter XOR-ed with a ciphertext block to recover the corresponding plaintext block.

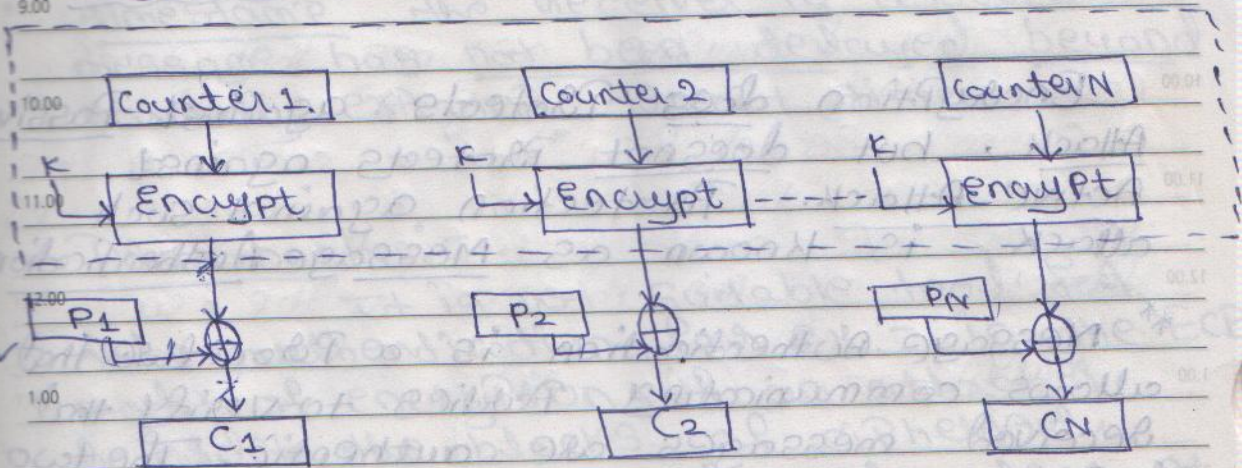
The following are the advantages of CTR mode.

1) H/w efficiency
2) S/w efficiency
3) Random Access
4) Provable security
5) Simplicity.

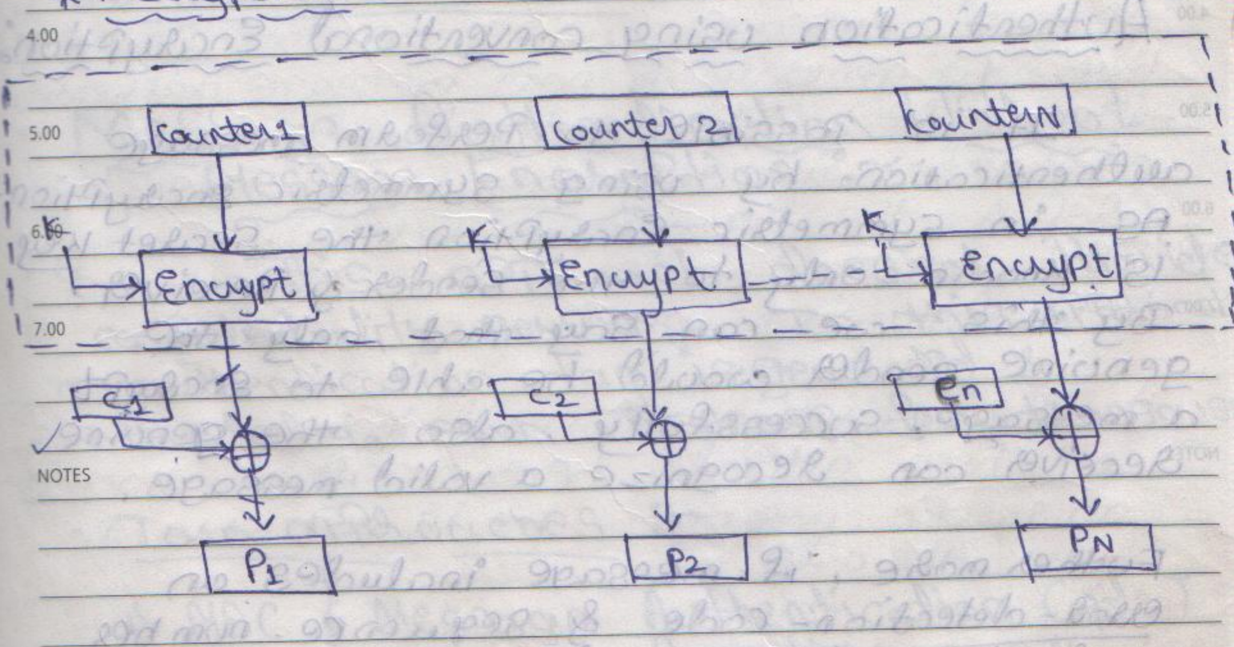
Encryption

NOTES

*Encryption:



*Decryption:



Approaches to Message Authentication.

Encryption does protects against Passive Attack, but doesnot protects against Active Attack. Protection against such attack is known as Message Authentication

** Message Authentication : is a Procedure that allows communicating Parties to verify that received messages are authentic. The two important aspects are to verify that the contents of the message have not been altered and that the source is authentic.

Authentication using conventional Encryption:-

It is Possible to Perform message authentication by using symmetric encryption. As in symmetric Encryption the secret key is known only to the sender & Receiver. By this we can say that, only the genuine sender would be able to encrypt a message successfully, also the genuine receiver can recognize a valid message.

Futhermore, if message includes an error-detection-code & sequence number the receiver is assured that no alteration have made.

Further if the message includes a timestamp, the receiver is assured that message has not been delayed beyond normally expected transit time.

Drawback:-
It is not suitable tool for data authentication for ex:- in the ECB mode of encryption, if an attacker re-orders the blocks of ciphertext, then each block will still decrypt successfully, but the re-ordering has altered the meaning of the overall data sequence.

Message Authentication Without Message Encryption:-

This approach does not provide confidentiality service. In this approach a authentication tag is generated & appended to each message for transmiss

Two approaches :-

1) MAC (Message Authentication Code)
2) one-way hash function.

Imp ***

Message Authentication Code :-

This technique assumes that two communicating Parties, say 'A' & 'B', share a common secret key "K_{AB}". when 'A' has a message to send to 'B', it calculates the message authentication code as a function of the message & the key

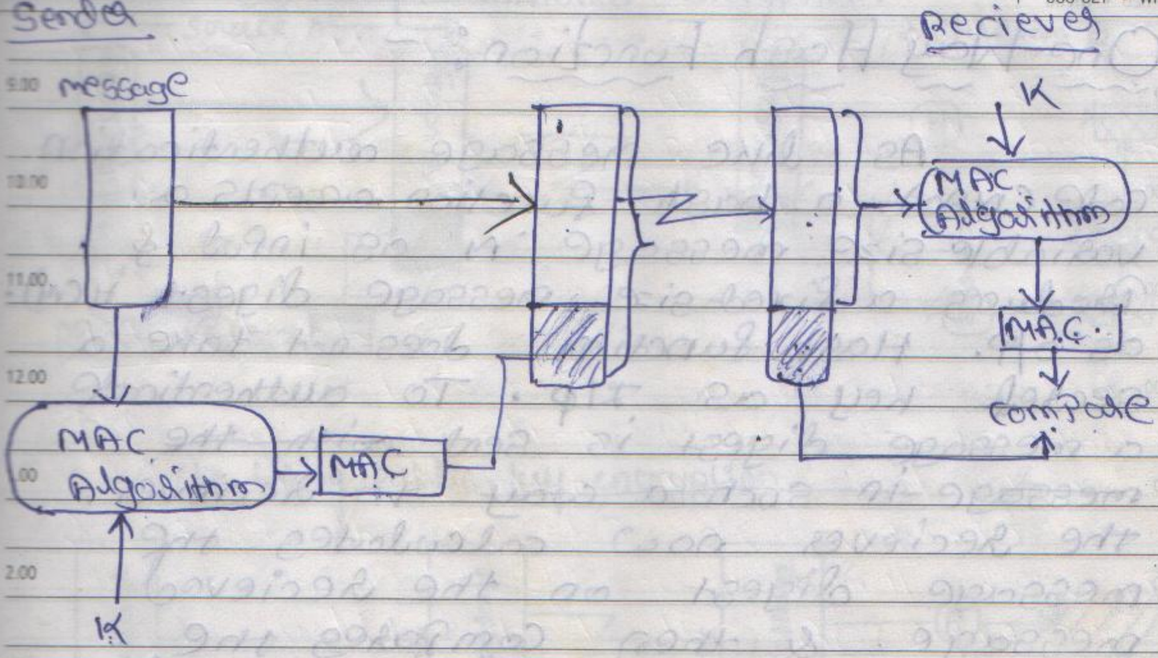
$$MAC_M = F(K_{AB}, M).$$

The message plus code are transmitted to the intended recipent. The recipent performs the same calculation on the recieved message, using the same secret key, to generate a new message authentication code. The recieved code is compared with the calculated code (reffer the fig - shown below).

If the recieved code matches the calculated then following statements apply:-

1) The receiver is assured that message has not been altered. because if an attacker alters the message, he is not able to alter the code.

2) The receiver is assured that message is from the alleged sender.



Because no one else knows the secret key.

3) If the message includes sequence number, then the receiver can be assured of the proper sequence.

NOTES

One-Way Hash Function: -

9.00

As like message authentication
10.00 code (MAC), a hash function accepts a variable-size message 'M' as input &
11.00 produces a fixed-size message digest H(M). as o/p. Hash function does-not take a
12.00 secret key as I/p. To authenticate a message digest is send ~~with the~~
1.00 ~~message in such a way~~ to reciever. the reciever now calculates the
2.00 message digest on the recieved message. & then compares the
3.00 calculated & recieved message digest.

4.00 Imp

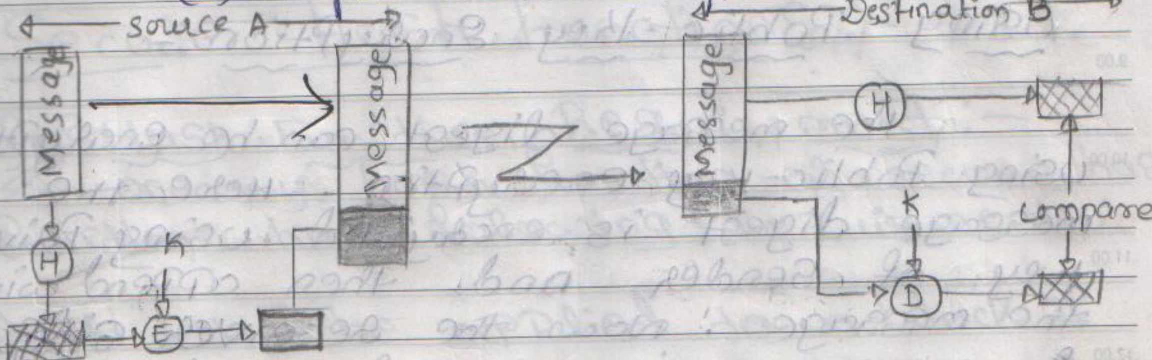
There are three ways in which the
5.00 message can be authenticated.
1) using conventional encryption
6.00 2) using Public-key Encryption
3) using secret value.
7.00

NOTES

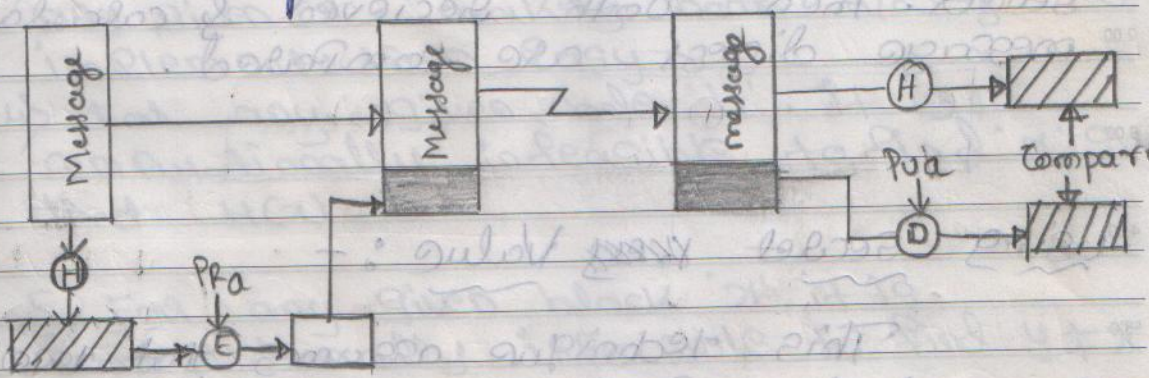
using conventional Encryption: -

The message digest can be encrypted using using conventional Encryption, if it's assumed that only sender & receiver share the encryption key, the authenticity is assured. as shown in fig-(a)

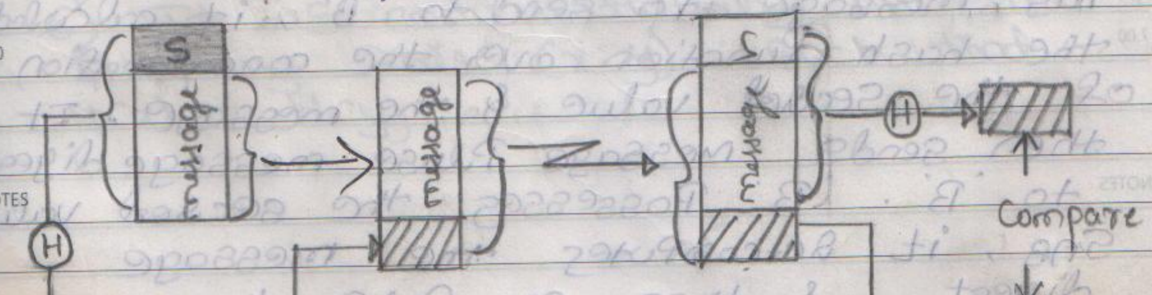
(a) Using conventional encryption:



(b) Using public-key encryption



(C) Using Secret value



Using Public-Key Encryption :-

The message digest can be encrypted using Public-Key encryption. Here the message digest is encrypted using Private Key of Sender and then append with the message. Now the receiver side, message is calcuded on recieved message and also recieved message is decrypted using Public Key of the sender. Then both recieved & calculated message digest are compared.

Using Secret Value :-

This technique assumes that two communicating Parties say 'A' & 'B', share a common secret value S_{AB}. when 'A' has message to send to 'B', it calculates the hash function over the concatenation of the secret value & the message. It then sends message Pluse message digest to 'B'. 'B' Possesses the secret value S_{AB}, it re-computes the message digest, & then compares the received & calculated message digest.

Secure - Hash Functions :-

*** Imp Hash - Function Requirement :-

Oneway hash function or secure hash function has following requirements:

1) 'H' can be applied to a block of data of any size.
2) 'H' Produce a fixed-length output.
3) H(x) is relatively easy to compute for any given 'x'. making both H/w & S/w implementation easy.
4) For any given code 'h', it is computationally infeasible to find 'x' such that H(x) = h.

5) For any given block 'x', it is computationally infeasible to find $y \neq x$ with H(y) = H(x).

6) It is computationally infeasible to find any pair (x, y), such that H(x) = H(y).

NOTES

Simple-Hash Function

The I/P is viewed as a sequence of n-bid blocks. The I/P is processed one block at a time in an iterative fashion to produce an n-bit hash function.

One of simplest hash function is the bit-by-bit exclusive-OR (XOR) of every block. This can be expressed as

$$C_i = b_{i1} \oplus b_{i2} \oplus \cdots \oplus b_{im}$$

where

c_i = i^{th} bit of hash code, $1 \leq i \leq n$

m = number of n-bit blocks in the I/P

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

$\oplus$ = XOR operation.

NOTES

	bit 1	bit 2	. . . . . .	bit n
Block 1	b_{11}	b_{21}		b_{n1}
Block 2	b_{12}	b_{22}		b_{n2}
Block 3	b_{13}	b_{23}		b_{n3}
⋮	⋮	⋮	⋮	⋮
Block m	b_{1m}	b_{2m}	. . .	b_{nm}
Hashcode	C_1	C_2	. . .	C_n

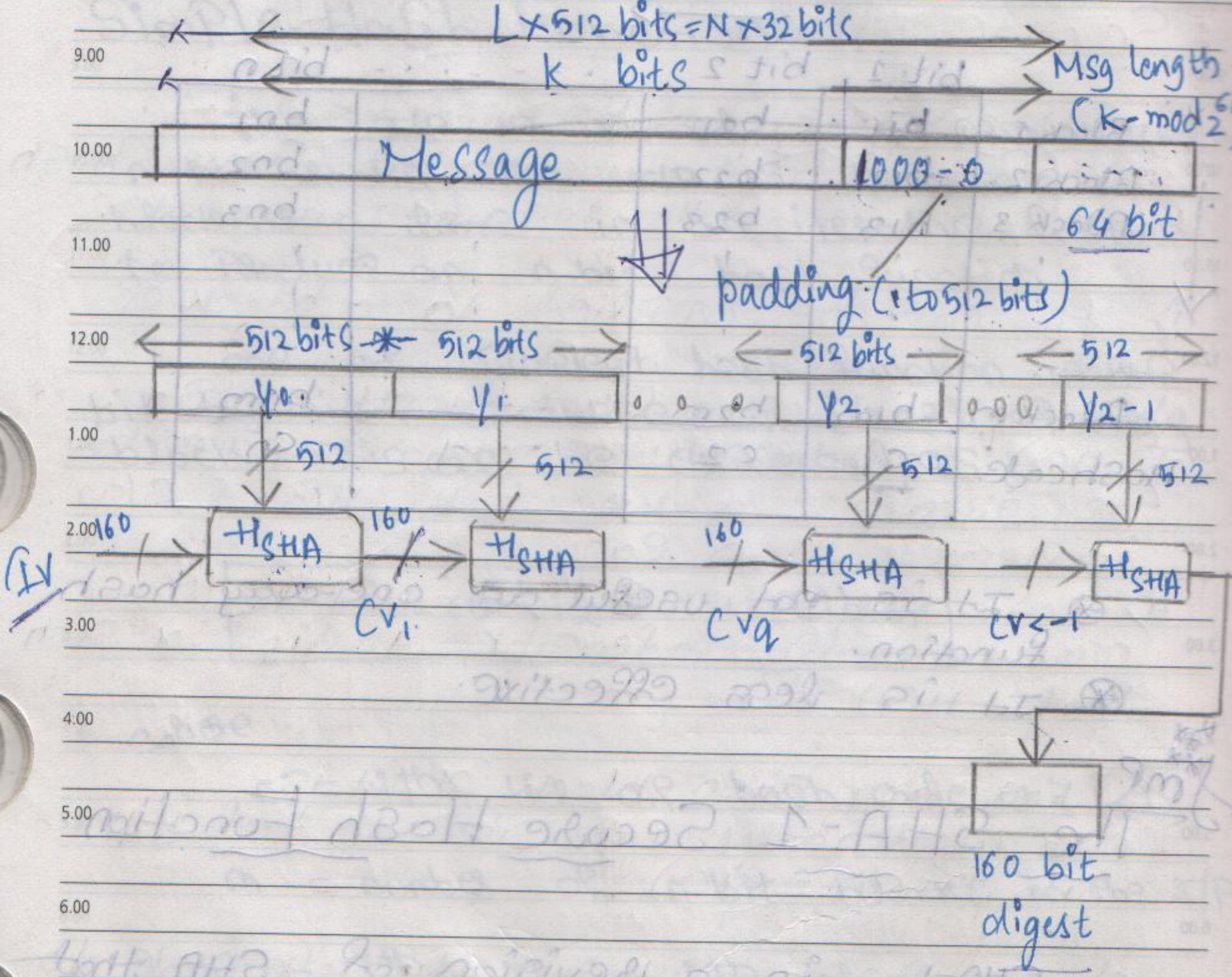
* It is not useful as one-way hash function.
* It is less effective

IMP

The SHA-1 Secure Hash Function

SHA-1 is a revision of SHA that was established in the year 1995. The algorithm takes a message of less than 2^{64} in length & Produces a 160-bit message digest.

9.00
10.00
11.00
12.00
1.00
2.00
3.00
4.00
5.00
6.00
7.00



Sunday 16

NOTES

MD - Message digest.

wk	M	T	W	T	F	S	S
09	31					1	2
10	3	4	5	6	7	8	9
11	10	11	12	13	14	15	16
12	17	18	19	20	21	22	23
13	24	25	26	27	28	29	30

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

Processing a message to Produce a ~~[illegible]~~ digest consists of the following steps.

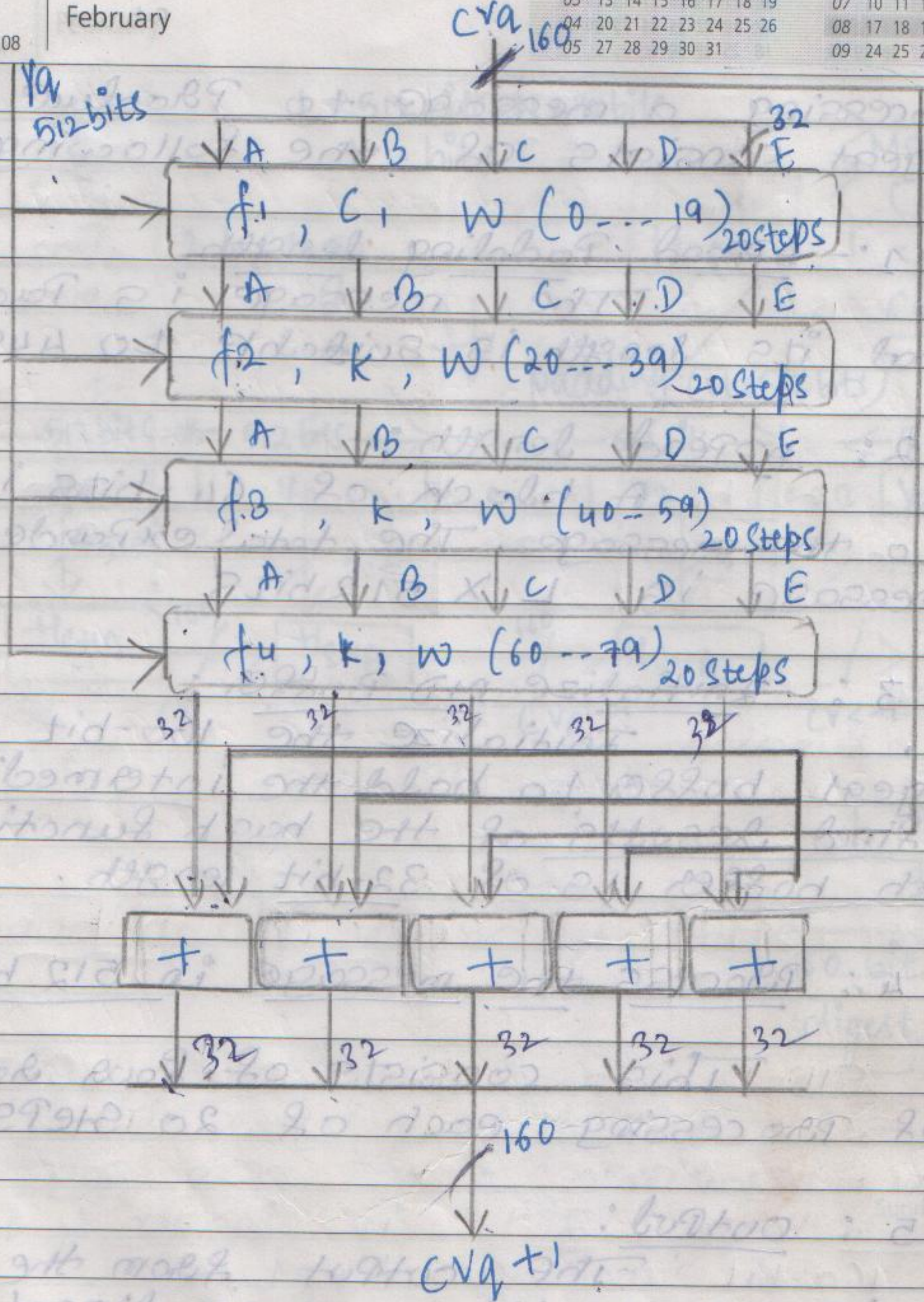
Step 1:- Append Padding length
The message is Padded so that its length is suitable to 448 mod 512.

Step 2: Append length:-
A block of 64-bits is appended to the message. The total expanded message is L X 512 bits.

Step 3: Initialize MD Buffer:
Initialize the 160-bit message digest buffer to hold the intermediate & final results of the hash function. Each buffer is of 32-bit length.

Step 4: Process the message in 512 bit blocks:
This consists of four rounds of processing each of 20 steps.

Step 5: Output:
The output from the L^{th} stage is the 160-bit message digest which is obtained after all L X 512 bit block have been Processed.


CVq
160
Yq
512 bits
32
A B C D E
f1, C, W (0 ... 19) 20 steps
A B C D E
f2, K, W (20 ... 39) 20 Steps
A B C D E
f3, K, W (40 .. 59) 20 Steps
A B C D E
f4, K, W (60 .. 79) 20 Steps
32 32 32 32 32
+ + + + +
32 32 32 32 32
160
CVq+1

Process the message in 512-bit blocks:

This consists of 4 rounds of processing of 20-steps each. The four rounds we refer to as $f_1, f_2, f_3, \& f_4$. Each round takes as I/P the current 512-bits block processed & 160 bit buffer value ABCDE & update the contents of buffer.

Public Key Cryptography Principles:-

Public key cryptography is asymmetric which uses two ~~seprate~~ separate keys in contrast to the symmetric conventional encryption, which uses only one key

A Public-key encryption scheme has six ingredients

① Plaintext - This is readable message or data that is fed into the algorithm as I/P.

② Encryption Algorithm: The encryption algorithm performs various transformation on the Plaintex.

(3) Public and Private Key :-

This is a Pair of keys that have been selected so that if one is used for encryption, the other is used for decryption.

(4) ciphertext :- This a scrambled message Produced as o/P. It depends on the Plaintext and the key.

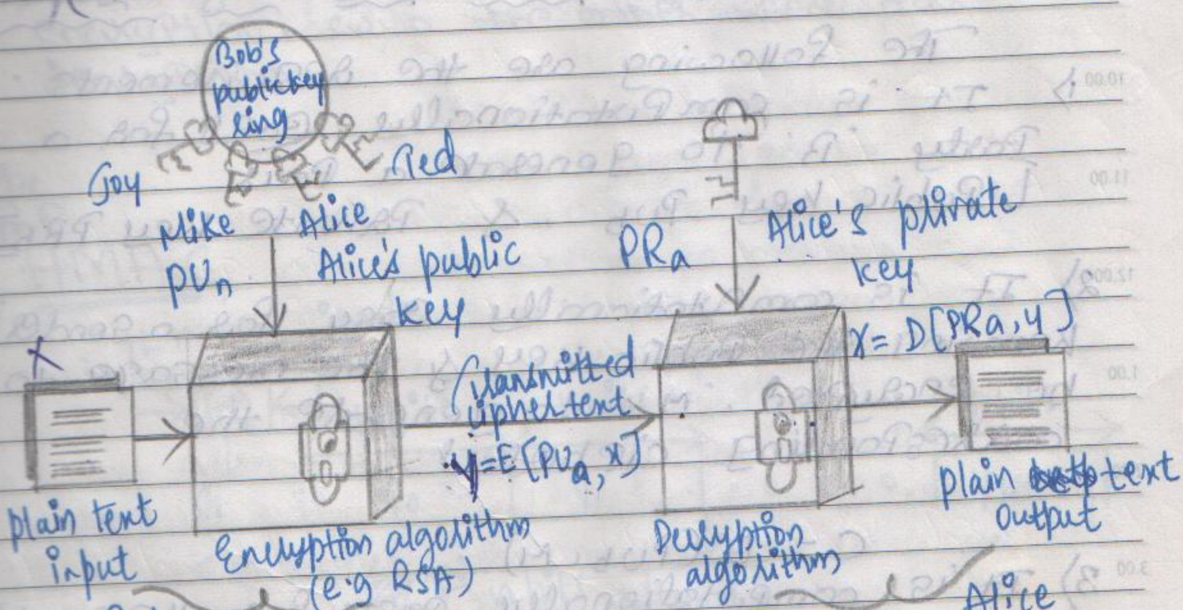
(5) Decryption Algorithm :-

This algorithm accepts the ciphertext & the matching key & Produces the original Plaintext.

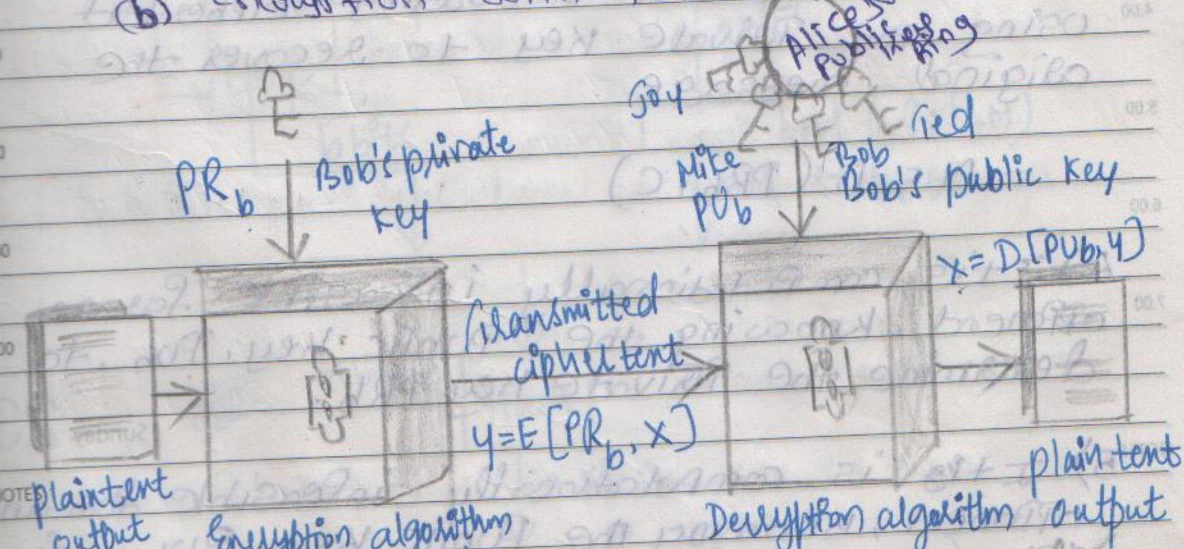
The following are the essential steps for Encryption with Public key.

1. Each user generates a Pair of keys to be used for Encryption & decryption of messages.
2. Each user Places one of the two keys in a Public register or, other accessible file. The companion key is kept private.
3. If Bob wishes to send a Private message to Alice. Bob encrypts the message using Alice's Public key.

(a) Encryption with Public Key.



(b) Encryption with Private Key.



4. When Alice receives the message, she decrypts it using her Private Key. Because only Alice knows the Private Key.

***Imp**

Requirements for Public-Key Cryptography:-

The following are the requirements:

1) It is computationally easy for a Party 'B' to generate a pair [Public key PU_b & Private key PR_b]

2) It is computationally easy for a sender knowing the public key & the message to be encrypted 'M' to generate the corresponding ciphertext

$$C = E(PU_b, M)$$

3) It is computationally easy for the receiver 'B' to decrypt the resulting ciphertext using the private key to recover the original message.

$$M = D(PR_b, C)$$

4) It is computationally infeasible for an opponent, knowing the public key PU_b to determine the private key PR_b.

5) It is computationally infeasible for an opponent, knowing the public key PU_b, & ciphertext 'C', to recover the original message 'M'.

6) Either of the two related keys can be used for encryption, with the other used for decryption.

Imp

HMAC

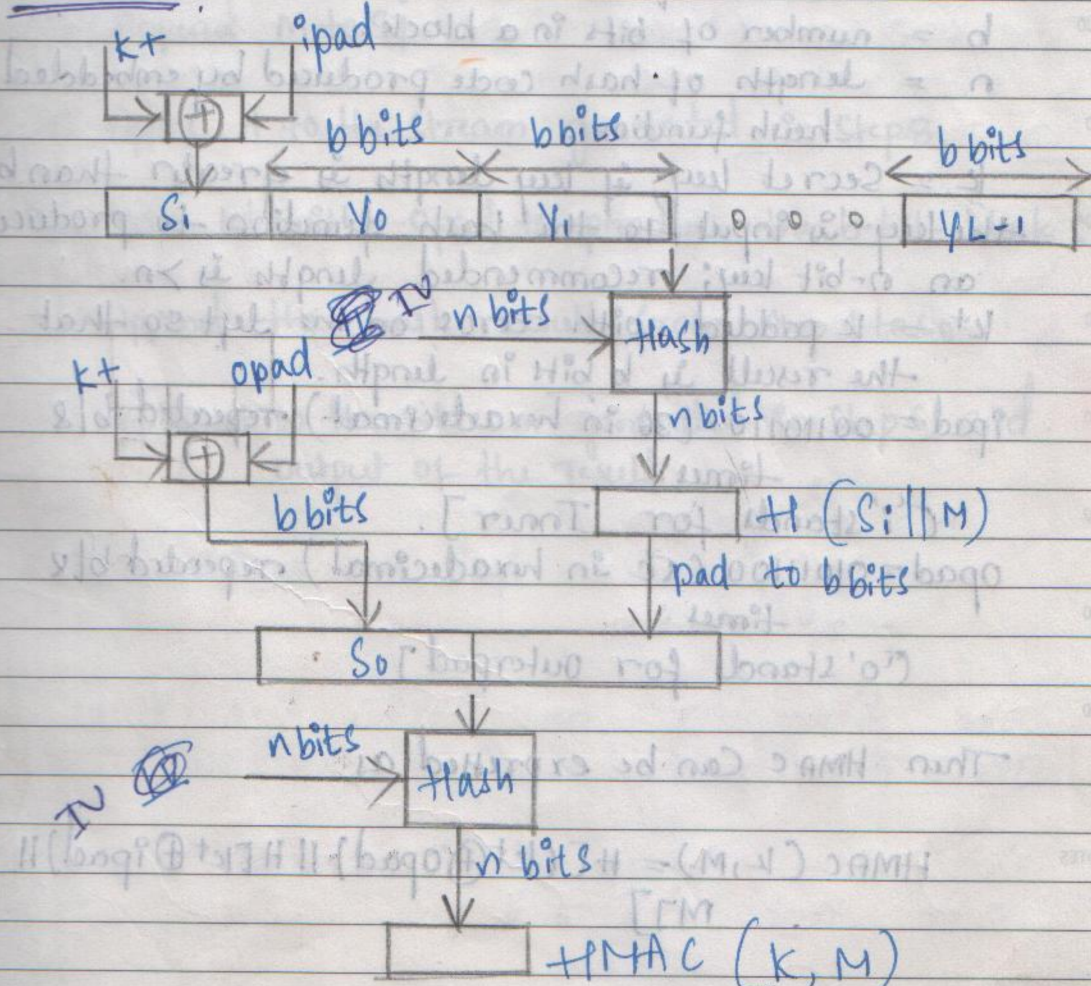


figure illustrates the Overall operation of HMAC. the following terms are defined:

H = embedded hash function.
M = message input to HMAC
Y_i = ith block of M, $0 \leq i \leq (L-1)$
L = number of blocks in M.
b = number of bits in a block.
n = length of hash code produced by embedded hash function.
K = Secret key; if key length is greater than b, the key is input to the hash function to produce an n-bit key; recommended length is $\geq n$.
K^+ = K padded with zeros on the left so that the result is b bits in length.
ipad = 00110110 (36 in hexadecimal) repeated b/8 times.
('i' stands for Inner].
opad = 01011100 (5C in hexadecimal) repeated b/8 times.
['o' stands for Outerpad]

Then HMAC Can be expressed as.

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

Steps for HMAC :

1) Append zeros to the left end of k to create a b-bit string k^+.

2) XOR k^+ with ipad to produce the b-bit block S_i.

3) Append M to S_i.

4) Apply H to the stream generated in step 3.

5) XOR k^+ with opad to produce the b-bit block S_o.

6) Append the hash result from step 4 to S_o.

7) Apply H to the stream generated in step 6 and output of the result.

Public Key Cryptography Algorithms

*** Imp

The RSA Public-Key Encryption Algorithm

It was developed in 1977 by Ron Rivest, Shamir & Adleman at MIT. The RSA is block cipher, in which plaintext & cipher text are integers between '0' and 'n-1' for some 'n'.

Encryption & decryption are of the following form, for some plaintext 'M' & ciphertext 'C':

$$C = M^e \bmod n \quad \text{[Encryption]}$$

$$\left.\begin{aligned} M &= C^d \bmod n \\ &= (M^e)^d \bmod n \\ &= M^{ed} \bmod n \end{aligned}\right\} \text{[Decryption]}$$

The following are steps for keys generation :-

1) Select two prime number 'p' & 'q' such that $p \neq q$

2) calculate $n = p * q$
3) calculate $\phi(n) = (p-1) * (q-1)$
4) Select an integer 'e' such that

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

5) calculate 'd', such that
$de \bmod \phi(n) = 1$

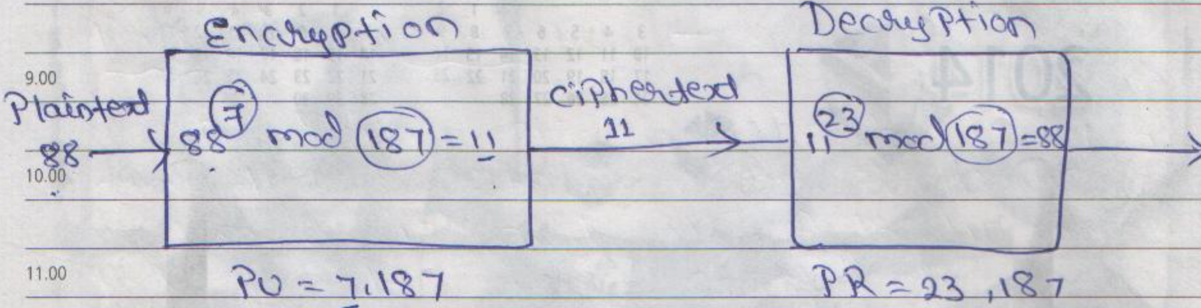
∴ Public Key = $KU = \{e, n\}$

∴ Private Key = $KR = \{d, n\}$

Ex:

Suppose M = 88, the following steps

1) Select two prime number $P = 17$ & $q = 11$
2) Calculate $n = pq = 17 \times 11 = 187$
3) Calculate $\phi(n) = (p-1)(q-1)$
$= 16 * 10 = 160$
4) select 'e' ~~such that~~ 'e' is, $e = 7$
5) Determine 'd' such that $de \bmod 160 = 1$.
The correct value is $d = 23$.



Diffie-Hellman Key Exchange :-

For this scheme, there are two publicly known numbers: a prime number 'q' & an integer 'α' that is primitive root of 'q'. Suppose the user 'A' & 'B' wish to exchange a key. User 'A' selects a random integer $X_A < q$, & computes $Y_A = \alpha^{X_A} \bmod q$. Similarly, user 'B' selects a random integer $X_B < q$ & computes $Y_B = \alpha^{X_B} \bmod q$. Each side keeps the 'X' value private & makes the 'Y' value available publicly to the other side.

User A computes the key as $K = (Y_B)^{X_A} \bmod q$, & user 'B' computes key as $K = (Y_A)^{X_B} \bmod q$.

These two calculation produce identical results:

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

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

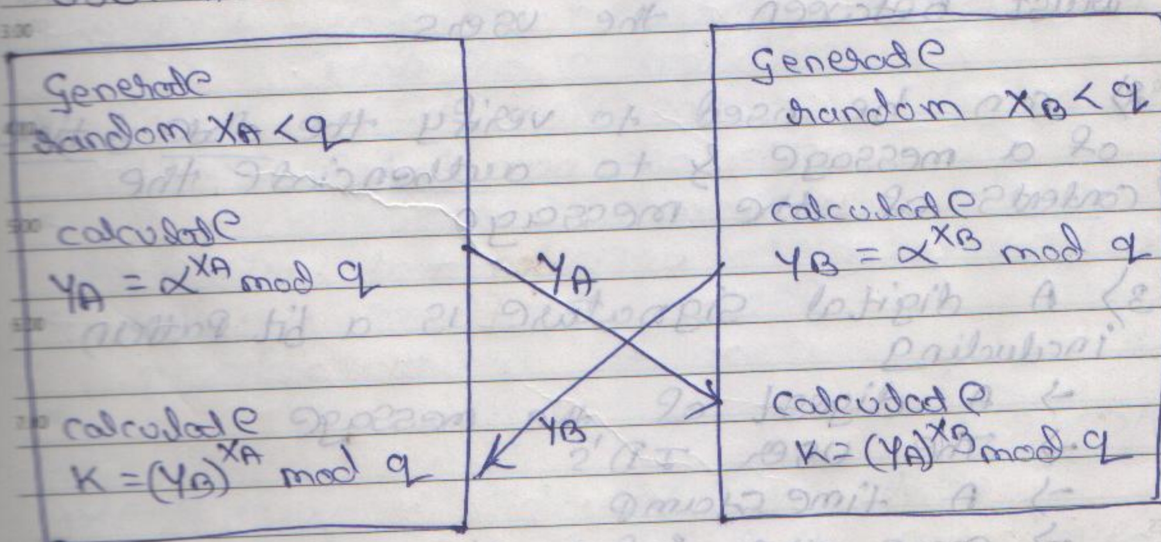
$$= (\alpha^{X_B})^{X_A} \bmod q$$

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

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

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

User 'A' — User 'B'



NOTES

Digital signature :-

A digital signature is basically a way to ensure that an electronic document is authentic. Authentic means that you know who created the document & you know that it has not been altered in any way.

Features of digital signature :

1) can be used to provide nonrepudiation service when there is a lack of complete trust between the users

2) can be used to verify the date & time of a message & to authenciate the contents of the message

3) A digital signature is a bit pattern including
   - → A digest of the message
   - → The user ID's
   - → A time stamp
   - → some other information.

30 marks

Network Security

Fundamental Concepts:

Here we will discuss objectives, assets, threats, vulnerable, safeguards & potential attacks.

Objectives:-

Information security has four major objectives as given below:

i) Confidentiality :- Ensuring that information is not ~~disclo~~ disclosed to unauthorized persons.

ii) Integrity :- Preventing unauthorized creation or modification of data.

iii) Availability :- Ensuring that authorized users are not denied access to information & resources.

iv) Legitimate use:- Ensuring that authorized persons don't use the information in an ~~an~~ unauthorized way.

Assets :

Assets are valuable resources of the organization that need to be protected. The loss of an asset represents the significant loss of the organization.

Ex:- users, application, servers, N/w, documents, Reputations .... etc.

Threads :-
Threads are an event that poses some danger to an asset. The four major threads are as follows:
i) Information Leakage — Information is leaked to unauthorized users which is thread to secrecy.
ii) Integrity violation :- Altering or creating false data that results in inconsistency of data.
iii) Denial of service :- using legitimate access rights to

iv) Illegitimate use :- Exploitation of privileges by legitimate users.

The above threads can be realized in different ways as given below:
1) Authorization violation :- A person authorized to use resource uses it in an unauthorized manner.
2) Bypassing control :-

3) Eavesdropping :- Leakage of Information by monitoring communication channel.
4) Interception :- Extracting Information from radio frequency.

5) malicious Programs :- Programs that are specially written to damage other Programs.

6) masquerade :- Person / entity Pretends to be different.

7) Traffic Analysis :- Leakage of information by analyzing traffic Pattern.

8) Re Pudiation :- A Person Participating in an exchange of information denies having Participated.

Vulnerability :-

Vulnerability is weakness or absence of Safeguards.

The categories of vulnerability is

-> Security Policy
-> Procedures
-> Administration.
-> Implemenation.
-> Apathy.

Example of vulnerability are

i) Granting higher rates to users than required.
ii) Initializing insecure System.
iii) Failure of Protection mechanism, etc.

Safeguards :-

Safeguards are Physical controls, Security Policies, security mechanism & Procedure that Protect assets from threads.

Physical controls are Physical security, administrative security etc.

Security Policy :- is a set of rules establish by organization to apply to all security related activities.

Security services are :
-> Identification & authentication service
-> Access Control Service
-> confidentiality service.
-> Data Integrity Service.

Attacks :-
An attack is realization of threats

Tools :- Tools used fall into 4 categories
-> Physical Attack
-> information exchange
-> user commands
-> Programs etc.

Actions:-

9.00 Depending on the vulnerability, the attacker can perform different actions such

10.00 as scan, flood, bypass, steal, read/copy/modify.

11.00

Target:- The targets of attack are generally

12.00 account, process, data, system components & network.

1.00

Imp

2.00 *** Identification & Authentication:-

3.00 Identification & authentication are measures to prevent unauthorized people from

4.00 entering the system.

There are 3 ways of authenticating a

5.00 user identity.

6.00 1) Proof by knowledge. Eg (Password)
2) Proof by possession. Eg (Pin card)
7.00 3) Proof by property Eg. [Finger Print]
4) Strong authentication.

NOTES

Proof by Knowledge:-

A Password is associated with each user. Passwords are shared between user & system. To gain the access to the system, the user enters a user ID & password. The system authenticates the user if the Password matches with that stored in the system.

There are different ways to store Passwords in the system

- → clear Passwords
- → Encrypted Passwords.

Clear Passwords:- The system stores Passwords in clear text in Password file, which is "read" & "write" Protected from users. It Provides no Security from system administrators or super user.

Encrypted Passwords:- A one-way hash function of Passwords are stored instead of clear Passwords. It Provides Security.

Threats on Passwords:-

The Threats include replay, Brute force Attack, Password guessing, Dictionary attacks etc.

Safeguards :-

9.00 Password rules are imposed to prevent use of weak passwords such as:-

10.00 → Minimum length of passwords and allowable set of characters, uppercase, numeric,

11.00 non-alphanumeric are specified.

→ The password ageing time frames are

12.00 specified to enforce change in passwords.

1.00

Proof by Possession :-

2.00

A user presents physical token that

3.00 the system can recognize as belonging to him such as a Banking card or ATM card.

4.00 Personal Identification Numbers (PINS) are often used along with physical token to

5.00 Identify the user. To prevent the brute force attack on PIN, the ATM

6.00 card will be blocked/deactivated if three unsuccessful attempts are made to

7.00 enter the PIN.

Proof by Property :-

NOTES

Biometric techniques relay on reliable unique characteristics of users such as finger-prints, voice patterns, retina scans, face geometry & hand geometry.

when the system needs to authenticate the user, the system obtains a biometric measure of the user & then compares it against that stored in the database.

<u>Strong Authentication</u> :-

1) <u>PassKeys</u> :- user password is mapped to a one-way hash-function to generate a cryptographic key. Such password-derived keys are known as PassKeys. The PassKey is used to secure communication link between user & the system.

2) <u>one-time passwords</u> :- A special equipment generates a Random number which is used as password. The password is changed every minute & is time synchronized to the database stored in the computer.

3) <u>Challenge Response Protocol</u> :- Here user provides his/her identity by responding correctly to the challenge (question) asked by verifier. For ex:- the user & system agree on function $f = x^2 + 5$. when the user logs in, the system randomly selects a number say 10 & send it to user, the user has to reply with number 105 for valid Authentication.

Access Control:-

Access control is defined as prohibiting the user from accessing resources not authorized to it.

Subject:- A subject is an entity wishing to access & perform operation on object. The subject may be users or process

Object:- An object is an entity to which access must be controlled. Ex:- file, database, CPU, memory, printer, N/w etc.

Operation:- Each object is associated with a set of operations that may be performed on it. for ex:- For file object, the operations could be open, close, create, delete, read or write.

Protection Rules:- Protection rules govern rules for subjects access to the object.

Identity Based Polices :-

It is classified into individual-based Policy, group-based Policy, and role-based Policy.

An Individual-base Policy is expresed in terms of list for each subject stating which subjects may perform which actions on the objects.

In group-based Policy, several subjects are granted the same Permissions for one object.

In role-based Policy, rights are granted to groups of people based on this role in the organization.

Rule Based Policy :-

Rule Base Policy are categorized into two categories : Multilevel Policy & comparment based Policy

Multilevel Policy operates by assiging to each object a security level from the hierarchy of levels.

compartment-Base Policy, a set of objects is associated with a named security compartment or category, which isolates them from other sets of objects.

⊛ Security Requirements :-

The Hierachial levels are defined such as top-secret, confidential & unclassified.

⊛ Mandatory Access Control :-

Important Relations have been defined for granting read-only access & write-only access as discussed below :-

⇒ Read only access states that a subject 'S' has read access to object 'X' if security level of 'S' is greater than or equal to security level of 'X'

⇒ Write only access states that a subject 'S' has write access to object 'X' if security level of 'X' is greater than that of 'S'.

⊛ Discretionary Access Control

Here once a subject has obtained information from the object, it can pass on that information to anyone else without the knowledge of object's owner.

Labeling :-

A Labeling requirements ensure that all human readable outputs Produced by the system is labelled with the security levels of the information attached to the visible o/P.

Auditing :-

The activities of the system are recorded. The records can be analyzed in case the security of the system is compromised.

NOTES

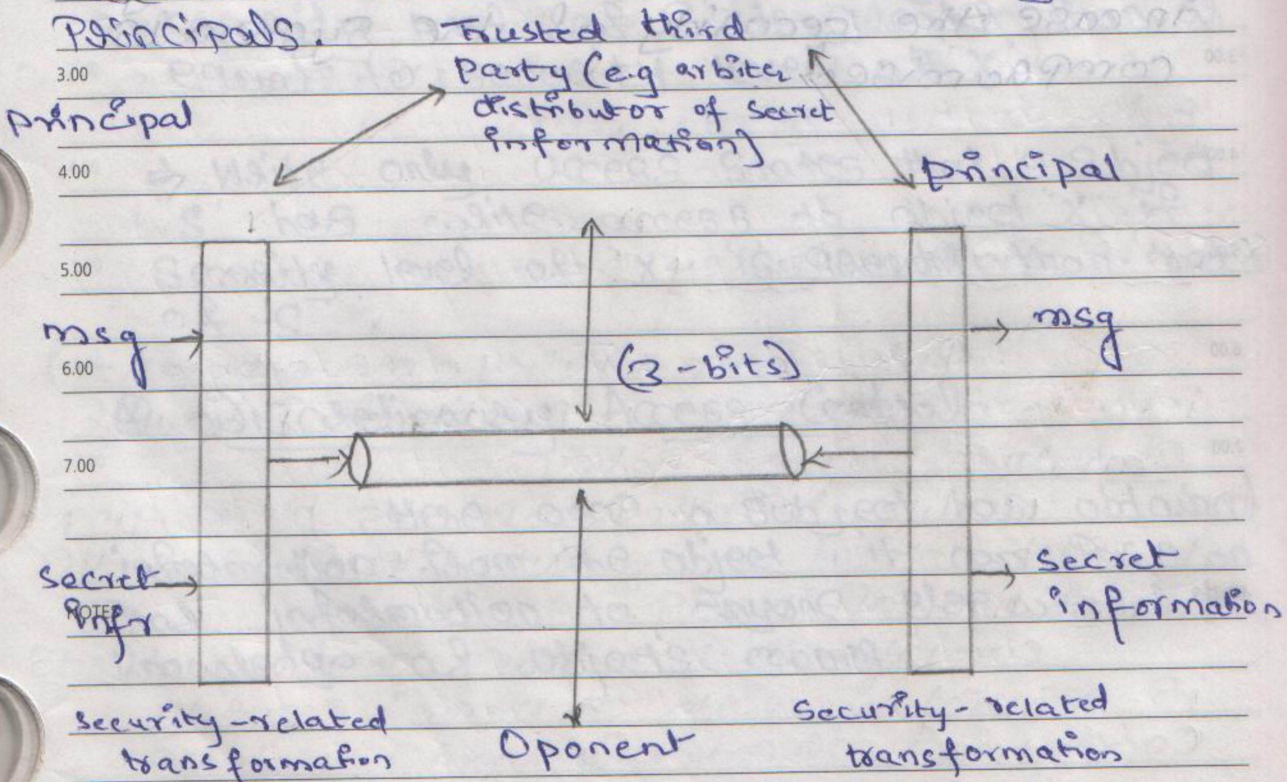
wk	M	T	W	T	F	S	S
05						1	2
06	3	4	5	6	7	8	9
07	10	11	12	13	14	15	16
08	17	18	19	20	21	22	23
09	24	25	26	27	28		

wk	M	T	W	T	F	S	S
09	31					1	2
10	3	4	5	6	7	8	9
11	10	11	12	13	14	15	16
12	17	18	19	20	21	22	23
13	24	25	26	27	28	29	30

Imp

A Model For Network Security :-

The below fig shows the model for N/w security. A message is to be transferred from one party to another across some sort of Internet. The two Parties, who are the Principals in this transaction, must co-operate for the exchange to take place. A logical information channel is established by defining a route through the Internet from source to destination & by co-operative use of communication Protocols by two Principals.



The techniques for Providing security have two components:

1) A security related tranformation on the information to be sent.

2) Some secret information should be shared by the two Principals. & it is hoped unknown to the opponent.

This general model shows that there are four basic tasks in designing a Particular security service.

1) Design an algorithm for Performing the security related transformation.
2) Generate the secret information to be used with the algorithm.
3) Develop methods for the distribution & sharing of the secret information.
4) specify a Protocol to be used by the two Principals that makes use of the security algorithm & secret information to achieve a Particular security service.

V.V. Imp

Malicious Software.

malicious S/w are programs that corrupts other program or pose severe security threads to the system. It is classified into two categories.

1) Host Dependent
2) Host Independent.

1) Host-dependent programs:-

Trapdoor:- It is a secret entry point into a computer program that allows someone who is aware of the trapdoor to gain access without going through normal methods of authentication.

Logic bomb:- The logic bomb is code embedded in some legitimate program that checks for certain conditions to be met.

NOTES

Trojan horse:- A program that appears to be useful but contains a hidden code which when executed performs some unwanted functions.

Virus :- A self-replicating program that infects other programs, either by modifying them directly or by modifying the environment in which they operate.

Boot Sector virus :- Infect, the master boot recorded by overwriting the original boot code with an infected version. A boot virus is spread to the disk drive when the system is booted with an infected floppy disk.

File infecting virus :- Infects executable files with com, exe, & OV1 extensions. O.S files are targeted.

Macro virus :- includes executable ~~files~~ programs that attach themselves to documents created in microsoft world & Excel. The virus executes & does its damage when the user receives a word or Excel document & executes a macro.

multipart virus :- Infect boot sectors as well as executable files. They are a real problem because they use

Stealth & polymorphism to prevent detection.

polymorphic virus :- changes its appearance to avoid detection by antivirus s/w. It encrypts itself with a special algorithm that changes every time an infection occurs.

Steath virus :- Attempts to hide itself from the O.S & antivirus s/w. They stay in memory to intercept attempt to use the O.S & hide changes made to file sizes.

2) Host-independent Programs :-

Bacteria :- program that consume system resources by replicating itself. The program do not explicitly damage any file.

worms :- N/w worm prgm replicates itself & sends copies from one computer to another across n/w connections.

Safeguards :-

Scanners :- Every virus is constructed from number of bytes. A unique Sequence of these bytes can be Selected which can used to identify the virus. The sequence is known as virus Signature. A Scanner Searches files locking for Signature. most antivirus s/w are Scanners which scans for known signatures.

Integrity Checkers :- An integrity checker can be used to identify viruses with known Signatures. This utility calculates checksum for every file that the user chooses & stores the checksums in a file. periodically, the integrity checker is run again on files & checksums are re-cal-culated to detect discrepanies.

Behavior blocker :- This utility remains in memory & alerts the user of any suspecious activity.

Firewalls :-

⇒ A firewall is a device that filters all traffic betⁿ a protected or "inside" n/w & a less trustworthy or "outside" n/w. usually, a firewall runs on a dedicated device, because it is a single point through which traffic is channeled.

⇒ The purpose of a firewall is to keep "bad" things outside a protected environment.

⇒ A firewall is a n/w access control device that is designed to deny all traffic except that which is explicitly allowed.

⇒ Firewalls have a wide range of capabilities. The Types of firewalls include.

* packet filtering firewalls
* Stateful inspection firewall.
* Proxy firewall
* Guards.
* personal firewalls.

Packet filtering firewalls :- packet filtering firewalls or packet-filtering gateway applies a set of rules to each incoming IP packet & then forwards or discards the packets.
Filtering rules are based on infr contained in a n/w packet.

→ Source IP address :- The IP address of the system that originated the IP packet.

→ Destination IP address :- The IP address of the system the IP packet is trying to reach.

→ Source & destination transport level address :- The transport-level (e.g TCP or UDP) port no, which defines applications such as SNMP or TELNET.

→ IP protocol field :- Defines the transport protocol.

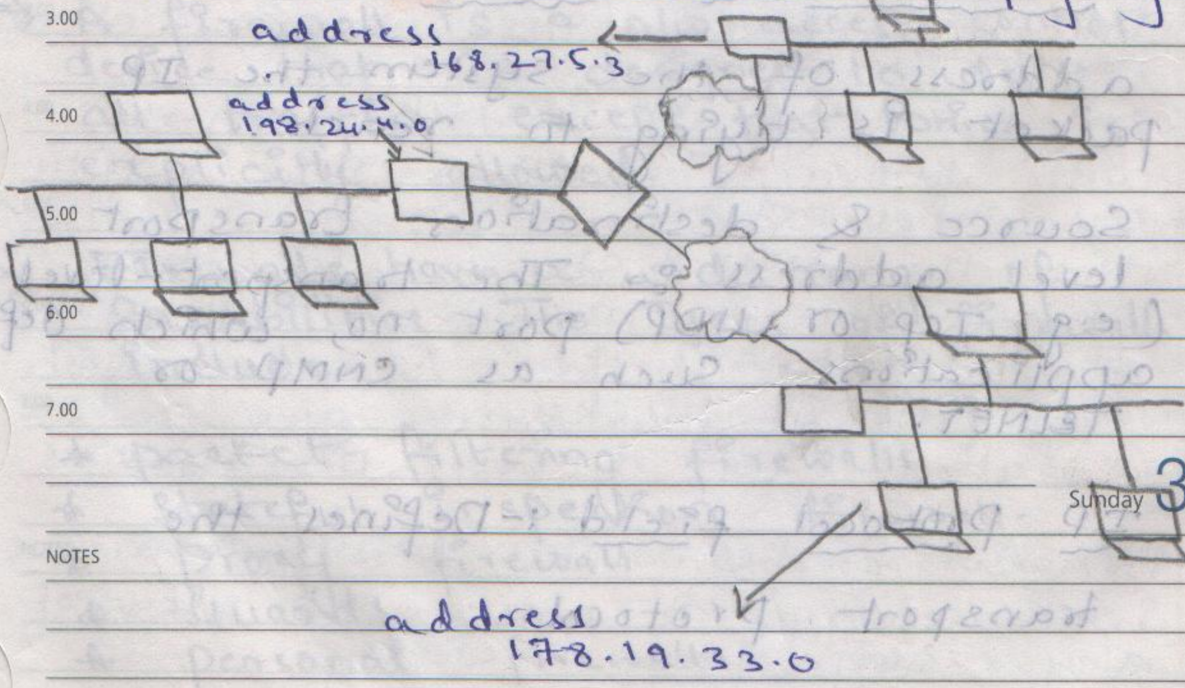
02							February 2014
wk	M	T	W	T	F	S	S
05						1	2
06	3	4	5	6	7	8	9
07	10	11	12	13	14	15	16
08	17	18	19	20	21	22	23
09	24	25	26	27	28		

03							March 2014
wk	M	T	W	T	F	S	S
09	31					1	2
10	3	4	5	6	7	8	9
11	10	11	12	13	14	15	16
12	17	18	19	20	21	22	23
13	24	25	26	27	28	29	30

→ interface:- for a router with three or more parts, which interface of the router the packet came from or which inter-face of the router the packet is destined for.

⇒ If there is no match to any rules, then a default action is taken,

For Example:- suppose a company has 3 LAN's at three locations throughout the nation, as shown in fig.



Sunday 30

NOTES

In this example, the router has two sides: inside & outside. we say that local LAN is on the inside of the router, & two connections to distant LANs through the wide area n/w are on the outside. It could use a packet-filtering firewall on the LAN at 198.24.4.0 to allow in only communication designed to the host at 198.24.4.0 & to allow out only communications address either to address 168.27.5.3 or 178.19.33.0.

Stateful inspection firewalls :-

⇒ filtering firewall work on packets one at a time, accepting or rejecting each packet & moving on to the next. They have no concept of "state" or "context" from one packet to another in the input stream.

⇒ Policy rules are enforced through the use of packet infection filters. The filters examines the packets & deter-mine whether the traffic is allowed based on the policy rules & the state of the protocol, this is known as statefull inspection.

Guard :-

9.00

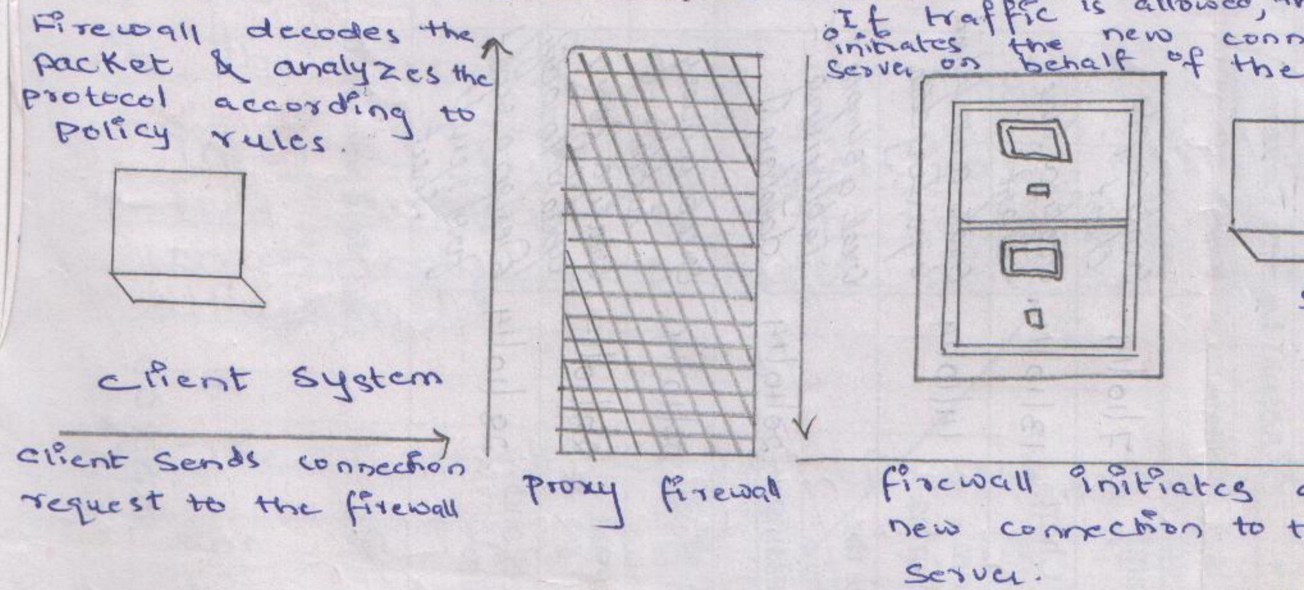
A guard is a sophisticated
10.00 firewall. ~~xxx~~ The guard decides
what services to perform on
11.00 the users behalf in accordance
with its available knowledge, such
12.00 as whatever it can reliably know
of the (outside) user's identity, previous
1.00 interactions & so forth.

2.00 ⇒ Guard activities can be quite
sophisticated : illustrated examples.
3.00

(i) A university wants to allow
4.00 its students to use email up to
a limit of so many msg or so
5.00 many characters of e-mail in the
last so many days.
6.00

(ii) A school wants its students to be
7.00 able to access the worldwide web,
but, because of slow speed of
its connection to the web, it will
NOTES allow only so many characters
per downloaded image.

where the location of the network is from packet information.



Personal Firewall

A personal firewall (sometimes called a desktop firewall) is a software application used to single Internet-connected computer from intruders. Personal firewall protection is especial for users with "always-on" connections such as DSL or cable modem.

Often compared to anti-virus applications, personal firewalls work in the background at th (link layer) level to protect the integrity of the system from malicious computer code by co Internet connections to and from a user's computer, filtering inbound and outbound traffic, alerting the user to attempted intrusions.

03							March 2014
wk	M	T	W	T	F	S	S
09	31					1	2
10	3	4	5	6	7	8	9
11	10	11	12	13	14	15	16
12	17	18	19	20	21	22	23
13	24	25	26	27	28	29	30

04							April 2014
wk	M	T	W	T	F	S	S
14		1	2	3	4	5	6
15	7	8	9	10	11	12	13
16	14	15	16	17	18	19	20
17	21	22	23	24	25	26	27
18	28	29	30				

Imp.

9.00 Limitations of fire walls.

10.00 1) The firewall does not Protect against internal threats such as disgruntled

11.00 employee.

12.00 2) The firewall cannot Protect against the transfer of virus infected programs or files.

1.00 3) The firewall cannot Protect against

2.00 attacks that bypass the firewall.

3.00

4) Firewalls can be "fooled" by source

4.00 routing or address spoofing.

5.00

6.00

7.00

NOTES