CRYPTOGRAPHY & NETWORK SECURITY

6TH SEMESTER

LECTURE NOTES

Prepared By:- KRUPAMAYEE MAHAPATRA

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEEERING

SWAMI VIVEKANANDA SCHOOL OF ENGINEERING & TECHNOLOGY

MADANPUR, BHUBANESWAR, PIN-752054

Ch-1

Cryptography & Network Security

Cryptography :- Art of codifying messages so that they become Un-readable.

Need for security :-

2 typical examples of such security mechanisms

i. Provide a user id & password to AB user & use that information to authenticate a user.

ii) Encode information stored in the database in some fashion so, that it is not visible to users who do not have the right permissions.

organizations employed their own mechanisms in order to provide for there ~~kin~~ type of basic security mechanisms. As technology improved the communication infrastructure became extremely mature & newer applications began develops for various user demands & needs. people realized that the basic security measures were not quite enough.

Cause of Security :

- Most critical comp. application had no or care based. very little security ~~this~~ this continue for a no. of years until the importants of data cause truely realised. until when comp. data was considered to be useful but not something to be protected.
- When comp. applications where develop to handle financial & personal data the real need for security was failed like never before.

- people realise that data on comp.s was an extremely imp. asset part of organisation life. Therefore various areas in security began to gain prominence.

Security approaches

3 security approaches are there:

i. Trusted system
ii. Security Model
iii. Security Management practices

i) Trusted system :

2 - A trusted system that can be trusted to a specify ~~exchanged~~ to extent to enforce a specified security policy.
- However these days the concept has spanned across various areas, most prominently in the banking and financial community, but the concept never caught on.

2 - Trusted system often use the term reference monitor this is an entity that is at the logical heart of the comput system. It is mainly responsible for all the decisions related to access controls.

Imp. approaches

1 - The expected's from the reference monitor are also called trusted system it should be tamper proof.
- It should always be enbld
- It should be small enough so that it can be independently tested.

ii) Security Model : An organizat^n can take several approaches to implement its security model, let us summerize these approaches, are :-

a) No security :- In this simplest case, the approach could be a decision to implement no security at all

b) Security through obscurity :- In this model a system is secure simply because no body knows about its existence & contents. This approch can not work for too luck. As their are many ways an attacker can come to know about it.

c) Host security : In this scheme the security for each host is enforced individually. This is a very safe approach but the trouble is that it can not scale well. The complexity & diversity of modern sites organizat^{n}s makes the task even harder.

d) Network security : Host security is tough the achieve as organizat^{n}s grow & become more diverse In this technique, the focus is to control net. access to various post & their services. Rather than individual host security.

- This is a very efficient scalable model.

iii) Security Management practices :

Good security management practices always talk of a security policy being in place. puting a security policy in place is actually quiet top.

- A Good security policy & its proper implementation when a long way in ensuring adequate security management practices.

- A good security policy generally taked care of 4 key aspects.

a. Affordability :- cost & effort in security implem

b. Functionality :- Mechanism of providing security.

c. Cultural issues :- Whether the policy gels well with people expectat°, working style & believes.

d. Legality :- ~~Checks~~ whether the policy needs the legal requirement once a security policy is in place some following point should be ensure.

- Explanat° of the policy to all concerned
- outline every bodies responsibilities.
- use simple language in all communicat°.
- Establishment of accountability.
- provision for exept° & periodic reviews.

L.Q. ## Principle of security

D-31-03-022

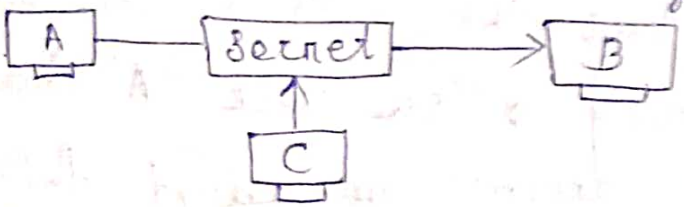
- Net. security is any activity desig°n to protect the usability & integrety of our net-s data.
- It is a stategy of organizat° which guarantees of net. traffic.
- It includes both s/w & h/w technology.
- It is a multiple layer of defence in the net.
- Only otherized user can access the net. & block the malicious attacks executing threads or virus.

Goal of security :

There are 6 goal / principle for security.

1. Confidentiality :-

- The principle of confidentially specifies that only the sender & the intended recipent (s) should be able to acess the contents of a message.
- Confidentiality gets compromised if an unathorised person able to access a message.

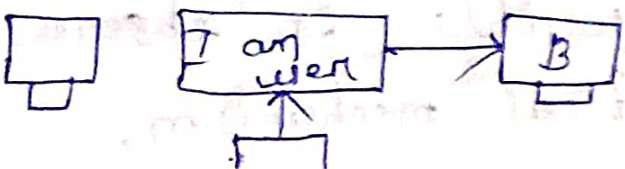


- protect our imp. confidential informat° e.g.- Here the user of comp. 'A' send a message to user of comp. 'B' another user 'C' gets access to the message which is not desired & therefore defeates the purpose of confidentiality if the confidential E-mail say back 'A' to 'B' which is acess by 'C' without the permission or knowledge of 'A' & 'B' this type of attack is called as intercept°.
- Intercept° causes loss of message confidentiality.

2. Integrity :-

- It means change of informat° only by authorized person & mechanisms.
- It avoides unwanted changes in the informat°.

E.g. - Customer bankbalance may changed after deposit or withdraw under the supervision of authorize mechanism



Here,
user 'c' tampers a message originally send by user 'A' which is actually destined for user 'B'. user 'c' somehow manage to view it. Change its contents & send the changed message to user 'B'. User 'B' has no way of knowing that the content the message where changed after user 'A' had send it. user 'A' also doesn't no about the changes.

- These type of attack is called as modification. Modificat° causes loss of message intigrety.

3. Authentication:

Authenticat° mechanism help establish proof of identities. The authenticat° ensures that the origin of electronic msg or document is correctly identify.

E.g. Suppose that user 'c' sends an electronic document over the internet user 'B' however the trouble is that user 'c' had posed as user 'A'. When 'c' send these document to user 'B'. How would user 'B' know that the msg has come from user 'c' who is posing as user 'A'.

- These type of attack is called fabricat°
- Fabricat° is possible in absence of proper authenticat° mechanism.

4. Non-Repudiation :

Non-repudiation does not allow the sender of a message to refute the claim of not sending that message.

e.g. - There are situations where a user sends a message & later on refuses that he/she had send that message. for e.g. user 'A' sends a fund transfer a request to bank 'B' over the internet. After the bank performs the fund transfer as per A's instruction, A could claim that he never send the fund transfer request to the bank. This A repudiation or denise, her funds transfer instruction. The principle of non-repudiation's defeats such possibilities of denying something, having done it.

5. Access Control :

The principle of access control determines who should be able to access what.

- For instance we should able to specify that user 'A' can view the records in a database but can not update them.
- Can access control mechanism can be set of to ensure these access control specify and control who can access what.

6. Availability :

The principle of availability states that resources or information should be available to authorised parties at all times.

- for e.g. due to intentional acts of unauthorized users 'C' an authorized user 'A' may not be able to contact 'A' server comp. 'B'.
- Interrupt^{n} could the availability of resources in dangerous.

7. Ethical & Legal Issues :-

Many ethical & legal issues in comp. security system seem to be in the areas of the individual right to privacy versus the great good of a larger entity. (e.g. company, society, for e.g. - Tracking how employees use comp.s crowd surveillance, managing customer profile. Tracking a person's travel with a passport, locat^{n} tracking so as to spam cell phone with text message advertisement & soon. A key concept in resolving the issues is to find out a person's expectat^{n} of privacy.
- Classically, the ethical issue in security systems are classified into the following four categories:

a) Privacy :- This deals with the right of an individual to control personal informat^{n}.

b) Accuracy :- This take about the responsibility for the authenticity, fidelity & accuracy of informat^{n}.

c) Property :- Here we find out the owner of the informat^{n}. We also talk about who controls access.

d) Accessibility :- This deals with the issue of the type of informat^{n} an organizat^{n} has the right to collect. And on that situat^{n}

it also expects to know the measures which will safe guarded against any unforeseen eventualities

ID-05.04.022

1.Q. ATTACK :

We can classify attack with respect to 2 views : a) A general view / A common person view
b) A technical view

a) A general view :- Form a common person's point of view, we can classify attacks on to 3 categories.

i) Criminal attack :- Criminal attacks are the simplest to understand. Here, the sole aim of the attackers is to maximize financial gain by attacking comp. system.

ii) Publicity attack :- publicity attacker attacks ~~the comp. system & the attacked party~~ because the attacker wants to see their name appears on television news channels & news paper. History suggest that these types of attackers are usually not hardcore criminals. They are people such as University & employees in large organizat°, who seek publicity by adopting a novel approach of attacking comp. system.

iii) Legal attack :-

The attacker attacks the comp. systems & the attacked party manages to take the attackers to the court. While the case is being fought the attacker tries to convince the judge & the jury that

there is inherent weakness in the comp. syst. & that she has done nothing wrong. The aim of the attacker is to exploit the weakness of the judge & jury in technology matters.

b. Technical view :-

From the technical point of view, we can classify the types of attacks that manages to take the attacker to the court while the on comp. & network system into 2 categories for better understanding.

i. Theoretical concepts behind these attacks.
ii) practical approaches used by the attacker.

- These attacks can also be into 2 types: Passive attack & Active attack.

Passive attack :-

In other words, the attacker aims to obtain information that is intransit. The term passive indicates that the attacker does not attempt to perform any modification to the data. This is also passive attacks are harder to detect.

- Thus general approach to be dealt with passive attack is to things about prevention rather than detection or corrective act.
- Passive attack do not involve any modification in content of an original message.
- These categories, namely release of

message content & traffic analysis.

Active attack :-

- The active attack are based on modificat° of the original msg in some manner or the creat° of a false message.
- In active attack the contents of the original message are modified in some way.

∴ Trying to pose as another entity involves masquerade attack.

∴ Modificat° attacks can be classified further in to replay attacks & alterat° of messages.

iii) Fabricat° causes denial of services (DOS) attacks

3

06.04.022

Masquerade is caused when an unauthorized entity pretends to be another entity. e.g. user C might pose as user A and send a message to user B. User B might be led to believe that the message indeed came from user A. In masquerade attacks, an entity poses as another entity.

Replay attack :

a user captures a sequence of events or some data units & re-sends them.

For instance. e.g. A user A wants to transfer some amount to user C's bank account. Both users A & C have accounts with bank B. User A might send an electronic message to

bank B, requesting for the funds transfer. User 'C' could capture this message and send a second copy of the same to bank B. Bank B would have no idea that this is an unauthorized message & would treat this a second and different, funds transfer request from user A.

Alteration :-

Alternat° of messages involves some change to the original message.

Denial of service (DOS) :-

In this attack, may/ can attempt to prevent legitimate users from accessing some services, which they are eligible for.

Cryptography : Concept & Techniques

Cryptography is the art of science of achieving security by encoding messages to make them non-readable.

Cryptanalysis :- Cryptanalysis is the technique of decoding messages from a non-readable format back to readable format without knowing how they were initially converted from readable format to non-readable format.

- Cryptology is a combination of cryptography & cryptanalysis.

Plain text & cipher text :

Plaintext :- Any communication in the language that we speak that is the human language, takes the form of plain text or clear text.

- Clear text or plain text signifies a message that can be understood by the sender, the recipient also by any else who gets on ones to that message.

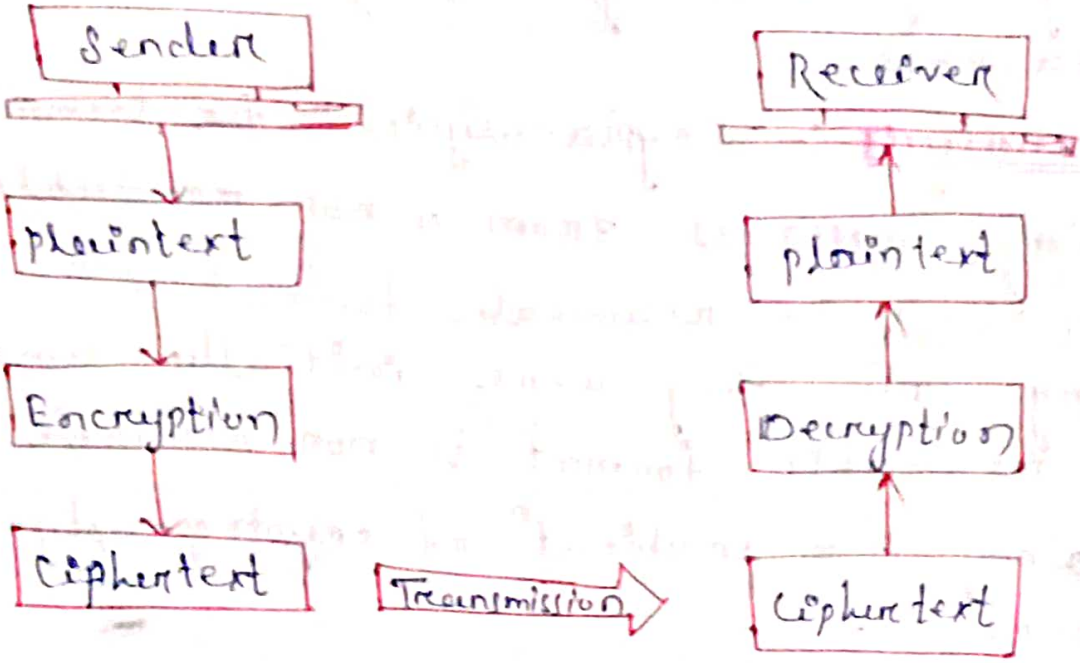
  e.g. My name is Indiree.

Ciphertext :- When a plain text message is codified using any suitable scheme, the resulting message is called cipher text.

e.g. Let us see A scheme for codifying message by replacing each alphabet three places down the line.

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

eg. plain text : I like to play
cipher text : L OLNH WR SODB



Encryption :- process of transforming plaintext into ciphertext.

Decrypt^{n} :- process of transforming ciphertext into plaintext.

There are 2 ~~type~~ primary ways in which a plaintext message can be modified to obtain the corresponding ciphertext:

i) Substitution
ii) Transposition.

i) Substitut^{n} Techniques

a) Caesar cipher :- This scheme (of replacing an alphabet with the one 3 places down the line) was first proposed by Julius C & termed as Caesar cipher.
- It was the 1st e.g. of substitut^{n} cipher.

In the cipher substitution cipher technique, the characters of a plaintext message are replaced by other characters, numbers or symbols.

- Caesar cipher is a special case of substitution technique where in each alphabet in a msg is replaced by an alphabet 3 places down the line.

e.g. A T U L
D W X O

b. Modified version of caesar cipher :

Caesar cipher is good in theory, but not so good in pratice. An alphabet 'A' in plaintext would not necessarily be replaced by 'D'. It can be replaced by any valid alphabet, i.e. by 'E' or by, for by 'h' & so on. once the replacement scheme is decided, it would be constant & will be used for all other alphabets in that msg. As we know, the english language contains 26 alphabets. Thus an alphabet by the english alphabet set, (i.e. B through z). Thus, for each alphabet, we have 25 possibilities of replacement. Hence, to break a msg in the modified version of caesar cipher, even earlier algorithm would not work.

D-08.04.022

Q. original A B C ... X Y Z
changed to X Y Z - ... U B A

If Alice send a msg HSLDN VHSVNLMVB
what should Bob infer from this

Ans :- SHOW ME THE MONEY

Algorithm of Modifying

1. Let 'k' be a no. equal to 1.
2. Read the complete cipher text message.
3. Replace each alphabet in the cipher text msg. with an alphabet.
4. Increment k by 1
5. If k is less than 26, then go to step 2. otherwise stop process.
6. The original text msg corresponding to the ciphertext msg is one of the 25 possibilities by the above steps.

Cryptanalysis is a person who attempts to break a cipher text message. The process itself is called as cryptanalysis.

A cryptanalyst attempting a Brute-force attack tries all possibilities to derive the original plaintext messages from a give cipher text message.

c. Mono-alphabetic cipher

The major weakness of the caesar cipher is its predictability. once we decide to replace an alphabet in a plaintext msg with an alphabet that is 'k' posits up or down the order, we replace all other alphabets in the plaintext msg with the same technique. Then the cryptanalyst has to try out a max^m 25 possible attacks & she is assured of success.

- Mono alphabetic ciphers pose a difficult problem for a cryptanalyst because it can be very difficult to crack them due to the high no. of possible combinat^n & communicat^n

Ciphertext K Ω U M P M Z M

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

4) Homophonic substitution cipher:

- The homophonic substitution cipher is very similar to monoalphabetic cipher like a plain text substitution cipher technique.
- We replace one alphabet with another in this scheme. However, the difference between the

i.e. 2 techniques. Technique is that where as the replacement alphabet set in case of the simple substitution techniques is fixed on the case of homophonic substitution cipher.

- One plain text alphabet can map to more than one cipher also involved that alphabet.
- Homophonic substitution cipher also involves substitution of one plain text character with a cipher text character at a time. however the cipher text character can be any one of the chosen set.

e) Polygram substitution cipher :-

In polygram substitution cipher technique, rather than replacing one plaintext alphabet with one cipher text alphabet at a time, a block of alphabets is replaced with another block. For instance, 'Hello' could be replaced by YUUOW, but (HELLO ⇒ YUOOW HELL could be replaced by a totally different cipher text block TEUI.

(HELL ⇒ TEUI)

- Polygram sub cipher technique replaced one block of plain text with a block of cipher text. It does not work on a character by character basis.

4) Polyalphabetic substitution cipher :

This cipher uses multiple one character keys. Each of the keys encrypts one plaintext char. The 1st key encrypts the 1st plaintext character; the second key encrypts the 2nd plaintext char. & soon. After all the keys are used, they are recycled. Thus, if we have 30 one-letter keys, every 30th character in the plaintext would be replaced with the same key. This no. is called as the period of the cipher.

- The main features of polyalphabetic substitution cipher are :
  a) It uses a set of related monoalphabetic substitution rules.
  b) It uses a key that determines which rule is used for which transformation.

ID - 11.04.022

Manual encryption of data :

(a) Play fair cipher :-

The play fair cipher also called as the play fair square is a cryptographic technic i.e. used for manual encrypt^{n} of data.

E.g. - We want to use the phrase "hello world" as our key. The 1st character (going from left to right) In the table will be the phrase duplicate letters removed. The rest of the table will be filled with the

remaining letters of the alphabet. In order, now our key table will look like this.

Plaintext → Hide the gold
Key → Hello world

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

5 x 5

In playfair cipher we a few simple rules relating to where the letters of each diagraph are in relate to each other. The rules are -

1. If both the letters are on the same column take the letter below each (going back to the top if at the bottom)
2. If both the letters are in the same row, take the letter to the right of each one (going back to the left)
3. If either of the preceding two rules are true, then form a rectangle with the two letters & take the letters on the horizontal opposite corner of the rectangle

E.g. 1. Plaintext — Hide the gold
Key — Hello world

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

HI - LF
DF - hD
TH - WN
EG - DP
OL - WO
DZ - CV

Ciphertext - LFhDWNDPWOCV

Key word - playfair

Plaintext - My name is Indira

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

MY → XF
NA → OP
ME → EG
IS → CN
IN → EU
DI → IR
RA → BL

Cipher text - XFOPEGCNEUIRBLZ

ID - 13.04.022

Hill cipher :-

Hill cipher works on multiple letters at the same time. The hill cipher ~~is~~ vulnerable to the known plaintext attack. This is because it is linear (i.e. It is possible to computer smaller factors of individually the matrix works on them individually & then join them back as & when they are ready.

Transposition Techniques

- In this cryptography technique involving the re arrangement of plaintext arrangement in some other form.

- Transposition techniques differ from substitution techniques in the way that they do not simply replace one alphabet with another, they also perform some permutations over the playing text alphabet.

a) Railfence Techniques :

Railfence technique involves writing plaintext as a sequence of diagonals & then reading it row by row to produce the ciphertext.

1. Treat every letter in the plaintext message as a no. so that A = 0, B = 1, C = 2 ... Z = 25

2. plaintext message = cat
so plaintext matrix = $\begin{bmatrix} 2 \\ 0 \\ 19 \end{bmatrix}$

3. Multiply the plaintext matrix by a matrix of randomly chosen keys of size n×n where 'n' is the no. of characters in the plain text message.

$$\text{key matrix} = \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 5 \end{bmatrix} = \begin{matrix} 31 \\ 216 \\ 325 \end{matrix}$$

4. ~~Log into the~~ Now multiply the 2 matrices

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 5 \end{bmatrix} \begin{bmatrix} 2 \\ 0 \\ 19 \end{bmatrix}$$

5. Now Compute a mod 26 value of the resultant matrix.

$$\begin{bmatrix} 3 & 1 \\ 1 & 16 \\ 3 & 25 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 5 \\ 8 \\ 13 \end{bmatrix}$$

6. Now translate these number to their corresponding alphabet i.e. 5 = F
8 = I
13 = N

7. Therefore our cipher text is FIN.

ID - 15.04.022

b) Book cipher or Running key cipher :-

The idea used in book cipher or running key cipher is quite simple & is similard to the principle of vernam cipher. For producing the cipher text some portion of text from a book is used which solves the purpose of one time pad. Then the characters from a book are used as the one time pad & they are added to the input plaging text message.

c) Vernam cipher :-

Vernam cipher use a one-time pad which is discarded after a single use & therefore suitable for only short messages.

e.g. 1. plain text — MY Name
12 24 13 0 12 4

2. key pad — no Ad ex
13 14 0 3 4 23

Initial total - 25 38 13 3 16 27

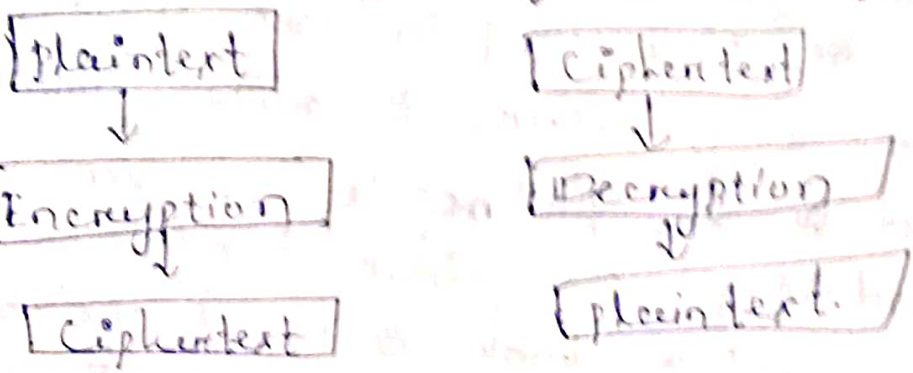
4. subtract 26 if greater > 25

5. cipher text 38 - 26 = 12
27 - 26 = 1

Y O E X

Encryption & Decryption ?

- In technical term the process of encoding plaintext message into ciphertext message is called as encryption.
- The process of transforming a ciphertext message back to plaintext message is called as decryption.



ID-19-04-022

In computer to computer communication the computer at the senders end usually transforms a plaintext message into cipher text by performing encryption. The encrypted cipher text message is then sent to the receiver over a network. The receivers comp. then takes the encrypted message & perform decryption process to obtain the plain text message. Every encryption & decrypt° process has 2 aspects that is the algorithm & the key used for encryption & decryption.

Input to encryption & decryption process

- Algorithm
- Key

- In general the algorithm used for encrypt & decryption process is usually known to every body. However it is the key used for encryption & decrypt^n that makes the process of cryptography secure
- Broadly their are 2 cryptographic mechanic depending on what key & are used.

1. If the same key is used for encryption & decryption then it is called as symentric key cryptography.
2. If the different keys is used ~~for encrypt^n & decrypt^n then it is called a symentric key~~ in cryptography mechanism i.e. one key is used for encryption & another different key is used for decrypt^n then it is called as asymmentric key cryptography.

Cryptography techniques

- Symentric key cryptography
- Asymentric key cryptography

Symentric key cryptography :—

~~This~~ This is the shortened kind of that involves only one secret key to cipher & Decipher information. Symentric key cryptography is an old & best known technique.

It uses a secret key that can either be a number, word or a string of random letters.
- It is blended with the plain text message to change the contents in a particular way. The sender & the receiver should no the secret key. i.e. used to encrypt & decrypt all the messages. Blowfish, AES, DES are e.g. of symmetric encrypt^{n}.

Asymmetric key cryptography :-

- This is also known as public key Cryptography.
- This encrypt^{n} uses 2 keys to encrypt & decrypt a message.
- Secret key are exchanged over the internet or a large net. A public key is made freely available to anyone who might want to send you a message. The 2nd key is the private key is kept a secret. So that only you can know. Security of the public key is not required because it is publicity available & can be passed over the internet.
- Popular asymmetric key encrypt^{n} algorithm include RAS, DAS, PKCS etc.

Ch-3

ID - 20-04-022

1.0 Symmetric & Asymmetric Algorithm

There are 2 key aspect of a algorithm i.e. algorithm types & algorithm modes. An algorithm type defines what size of plaintext should be encrypted in each step of an algorithm. The algorithm modes defines the details of the cryptographic algorithm

Algorithm Types :

Regarded as used at broad level generation of ciphertext from plaintext can be done in to basic ways.

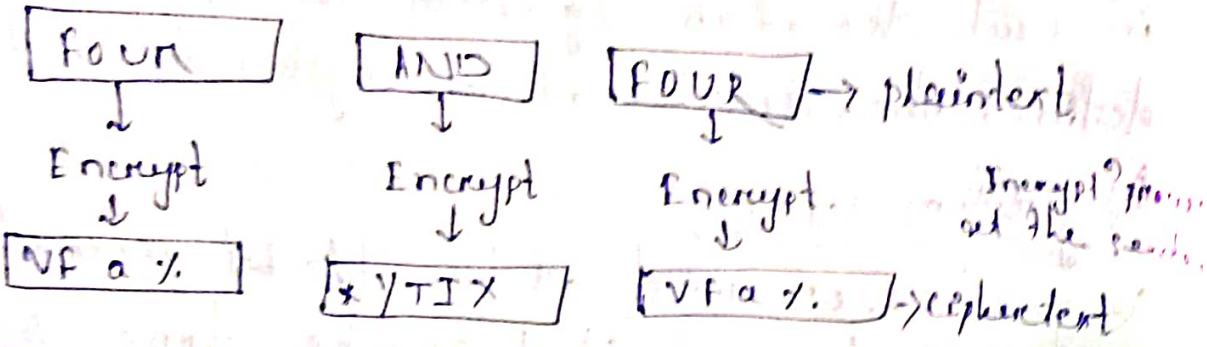
i) Stream cipher
ii) Block cipher

i) Stream cipher :- The plaintext is encrypted one by at a time suppose the original message is pay loo in ASCII character to there binary value let us assume that it is translated to 01011100 suppose the key to be applied is 10010101 in binary. Let us assume that De apply the XOR logic as the encryption algorithm.

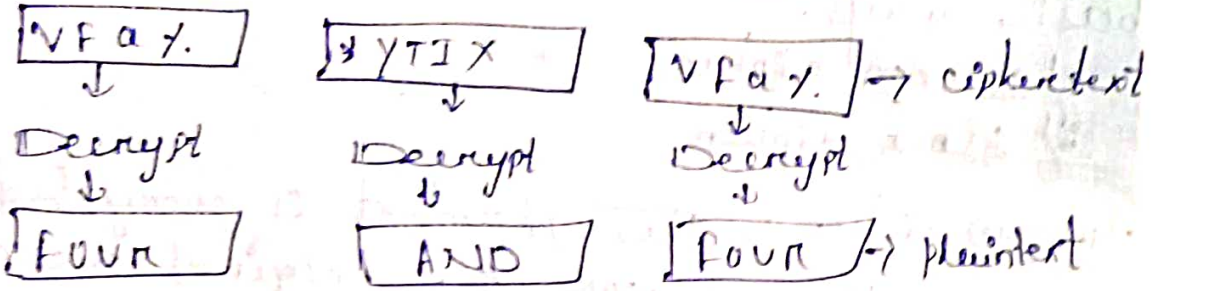
Text format - pay loo
Binary " - 01011100
Key - 10010101
XOR operation with key) - 11001001 (ciphertext)
Plaintext - ZTU91^ % D

Stream cipher techniques involve encryption of plaintext byte at a time. Decryption also happen 1 byte at a time.

ii) Block cipher :- Block cipher techniques involves encryption of 1 block of text at a time. Decryption also takes 1 block of encrypted text at a time.



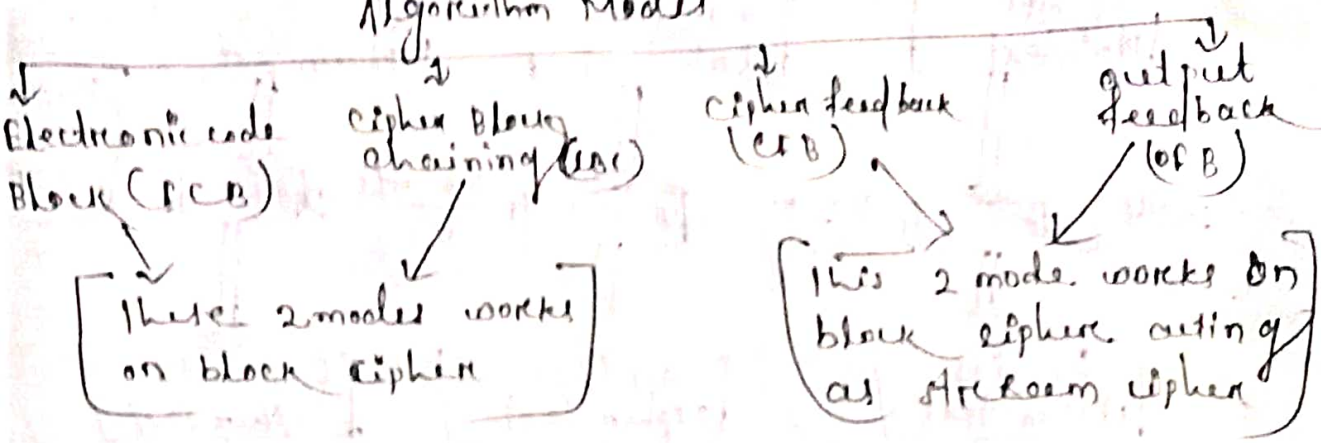
Decryption process at the sender



Algorithm Modes :-

- An Algorithm modes is a combination of service the basic algorithm steps on the block cipher.
- There are four important algorithm modes mainly electronic code booked (ECB).

Cipher block chaining :- cipher feedback, output feed back.



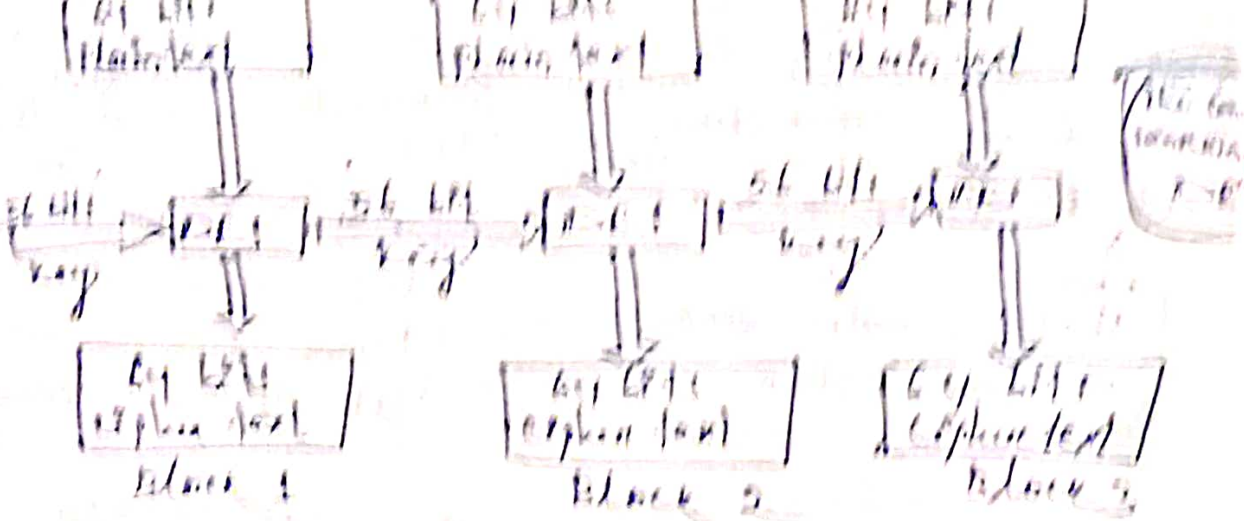
ID - 21.04.022

L.Q **Data encryption standard (DES) :-**

- The data encryption standard also called as the data DEA-1 by ISO (DEA) by ANSI & DEA-1 by ISO has been a cryptographic algorithm used for over 3 decades of plate DES has been found vulnerable against very powerful attack & therefore the popularity of DES has been slightly on the declining.
- However no book on security is complete without DES. As it has been a benchmark on crypto algorithm.

How DES Work :

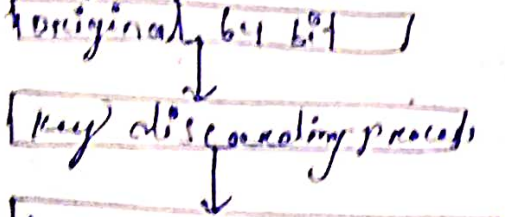
- DES is a block cipher it encrypts data block of size 64 bits each i.e. 64 bits of plaintext those are the input to do DES. Which produces 64 bit of ciphertext. The same algorithm an ER used for encryption & decryption with minor differences. The key length is 56 bits.



We have mentioned that key uses a 56 bit key. Actually the initially concept of key is 64 bit. However, before the next process even bit every 8 bits of the key is discarded, i.e. produce a 56 bit key i.e. bit position 8, 16, 24, 32, 40, 48, 56 of 64 bit are discarded. Before discarding these bits can be used for parity checking to ensure that the key data is not corrupt.

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

Thus the discarding the every 8 bit key produces a 56 bit key from the original 64 bit key.



The process of DES key

- DES is based on the 2 fundamental attribute of cryptography.

Substitution (confusion) &
Transposition (Diffusion)

DES consist of 16 steps each of which is called as a round. Each round performs the steps of substitut^n & transposit^n. The steps involves in the process of DES are:

Step. 1 :- In the 1st step 64 bit plaintext is handed over to an initial permutation function i.e. called IP.

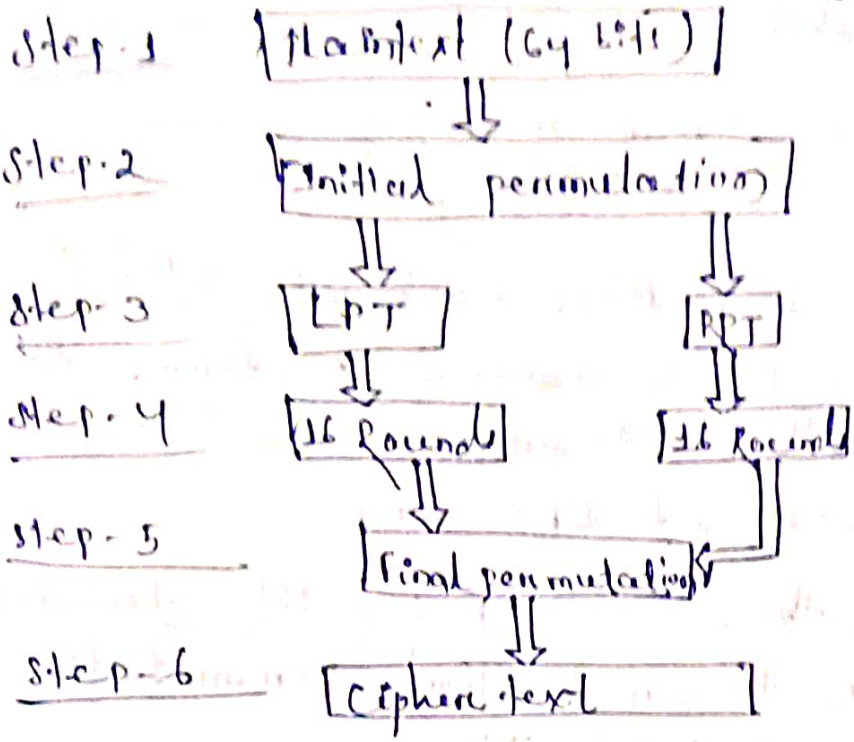
Step-2 :- The initial permutat^n is perm^d on plaintext.

Step-3 :- Now the initial permutat^n vertices to half of the permuted block i.e. left plaintext & right plaintext architecture.

Step-4 :- Now each of the entity & goes through 16 rounds of encrypt^n process.

Step-5 :- Finally entity & entity were rejoined & a final permutat^n is perform on the compile block.

Step 6 :- The result of these process produces a 64 bit ciphertext



Brocad labeled steps in DES :

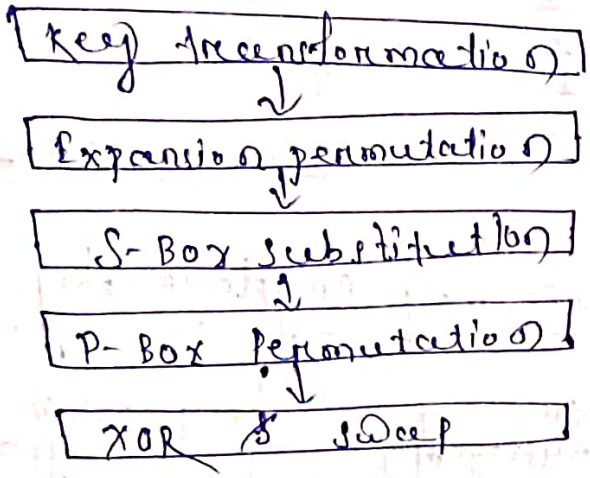
i) Initial permutation IP :-

IP happens only one & it happen before the 1st round. It suggest how to transposit in IP should proceed.

Bit posit^{n} in plaintext Block	To be over written with the contents of the 64 posit^{n}
1	58
2	50
3	42
⋮	⋮
64	7

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

After the initial permutation IP is done the resulting 64 bit permutation is divided into 2 half block. each half block consist of 32 bits. The left block is called as LPT & right block is called as RPT Now 16 rounds are perform on these 2 blocks. Each of the 16 round consist of the broad level steps out line below.



Details of one round in DES

Key transformation : We know that the initial 64 bit key is transformed into a 56 bit key. Then for each round a 56 bit key is available. From this 56-bit key a different 48 bit sub key is generated during each round using a process called as key transformation. For these the 56-bit key is devided into 2 half each of 28 bits. These are circularly shifted left by one or 2 positions depending on the round.

Round	No. of key bits shifted
1	1, 2
2	1
3	2
4	2
5	2

6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

ID - 09.03.022

Symetric vs Asymetric key cryptography

Characteristic	Symetric key cryptography	Asymetric key cryptography
1. key used for encrypt & decryption.	Some key is used for encrypt & decryption	one key is used for encrypt & another used for decryption.
2. Speed of encryption & decryption size of resulting encrypted text	Very fast usually same as or less than original the clean text size	slower More than the original text
3. Speed of encryption & decrypt size of resulting encrypted text. key agriment on exchange	A big problem	No problem at all
4. No. of keys required as Compaired to the participent in the messg exchange.	Equals is about the square of the no. of participent so. scalebility is an issue.	Same as no. of participents so scales of quite well.

3. RSA	Mainly for encrypt^{n}/decrypt^{n} (confidentiality) can't be used for digital signature (Integrity & non-repudiat^{n})	Can be used for encrypt^{n} & decrypt^{n} (confidentiality) as well as for digital signature. (Integrity & non-repudiat^{n} check)

Digital Signature :-

- Digital signature has assumed great significance in modern world of wave commerce.
- Most countries have already made provision for recognizing a digital signature as a valid authorization mechanism. Just like paper based signature.

Digital signature have legal status too. e.g. suppose you send a message to a bank over the internet to transfer some amount of your account in bank paper & digital signature the message these transaction has the same status have the one where in field in & sign the bank paper base money transfer.

RSA Algorithm :-

- The RSA algorithm is the most popular & proven asymetric key cryptography algorithm
- The RSA algo. is based on the mathematical fact that it is easy to find & multiply large prime number together, but of is extremely difficult to factor their product.

- Its private & public keys are RSA are based on very large prime numbers. It algorithm is very simple however the real challenge in case of RSA is the collection of primes of public & private

Algo

1. Choose two large prime number P & Q.
2. Calculate $n = P \times Q$
3. Select the public key (i.e. encryption key) E such that it is not a factor of $(P-1) \times (Q-1)$
4. Select the private key (i.e. decrypt key) D such that the following eq. is true $(D \times E) \bmod (P-1) \times (Q-1) = 1$
5. For encrypt calculate the cypher text CT from the plain text PT as follows
   $CT = PT^E \bmod N$
6. Send the CT as the cipher text to the receiver.
7. For decryption calculate the plaintext PT from the ciphertext CT as follows
   $PT = CT^D \bmod N$

$P = 7, Q = 17$

1. $P = 7, Q = 17$
2. $N = P \times Q = 7 \times 17 = 119$
3. $E = 5$
4. $(D \times E) \bmod (P-1) \times (Q-1) = 1$
   $D = 77$
   $(77 \times 5) \bmod 96$

$(P-1) \times (Q-1)$
$= (7-1) \times (17-1)$
$= 6 \times 16$
$= 96$
factors of 96
$= 1, 2, 3, 4, 6, 8, 12, 16, 24, 32$

$= 38^5 \bmod 91$

$=$

5. Let us assume that $pt = 10$ so $CT = (PT)^E \bmod N$

$= (10)^5 \bmod 119$

$= 40$

* Now the CT i.e 40 is send to the receiver

$PT = (CT)^D \bmod N$

$= (40)^{77} \bmod 119$

$= 10$

Ch-11 Digital Certificate & Public Key Infrastructure

The problem of key exchange or key agreement is quite severe & indeed one of the most difficult challenges in design any comp. based cryptography solutions.

This problem was resolve with a revolutionary idea of using digital certificate conceptually we can compare digital certificate to the documents such as our passport, driving license. A passport or a driving license helps in establishing, our identity. For instance our passport proofs provide important information regarding us like our full name, our nationality, our date & place of birth, our photograph & signature.

The Concept of digital certificate :

A digital certificate is simply a small computer file. For e.g. my digital certificate could actually be a computer file with the file name such as Rachita (where dot certificate signifies the 1st key character of the word certificate). But in actually practice the file extension can be different. Just as our passport signifies the association between our us our characteristics name, nationality, DOB, signature etc. The digital certificate simply signifies the association

betⁿ ~~or w our cha~~ our public key) our us.
A digital certificate establishing relation betⁿ a user & publicky. Therefore a digital certificate contain user name & user publickey given will prove that A perticular public key belongs to a perticular user.

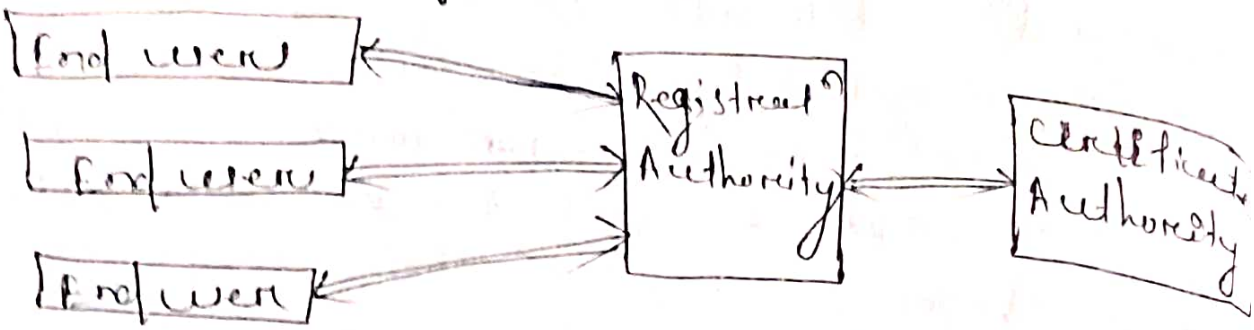
Certificate authority (CA) :-

A CA trusted ~~agency~~ that can issue digital certificate. The authoribory of acting as a CA has to be with some one who every body trust. Consicuently the Govt. of various contry decide who can & who can not be a CA. usually a CA is a repetate organizatⁿ such as post office, financial institutⁿ, s/w companies etc. 2 of the worl most famous CA are veriring, entrust self screen limitted a substaty of ~~sat~~ SATYAM info way) limitted become the 1st Indian CA in feb. 2013.

Registraction Authority :-

Since CA can be over loades with the verity of task issuing new certificate meaning old once, revoking the once that have become invalid for whatever is can etc. The CA can be daily date. Some of its task to a third party called are the resistraction auding. Lien called carray from an end user perspective there is a little different between CA & RA. Terminally the carray is an intermediate entity betⁿ the end user & CA. To access the CA

request to deny to deny activity.



RA commonly provides the following services

- Accepting & verifying registration information about users.
- Generating keys on we have the end user.
- Accepting & authorizing request for key backup & recovery.
- Accepting & authorizing the request for certificate revocation.

ID-12.05.022

Digital certificate creation steps :

There happens in case the user is not aware of the technique involve in generation of a keypad. A major disadvantage of this approach is the possibility of the agency knowing the private key of the user.

Registration :-

This step is required only if the generate the key pad in the 1st stage. If the agency generate the keypad on we have on the user step will be a part of the 1st step of self.

- Assuming that the user has generate the

The keypad the user now sent the public key & other information & evidences about himself or herself to the array. For this the RA provide website on which the user entered data & when all the data is correct submit it. This data on travels over the internet to the array.

- The format for certificate request has been standardized & its called as certificate signing request (CSR). This is one of the public key cryptography standards (PKCS)

Verification user :-

After the registration process is complete the array is to be verify the user credentials. This verification is done in 2 steps.

1. 1st key the array needs verify the user credential such as the evidence provided as correct & are acceptable. e.g. If the user is an organization the array would business character, historical documents, creditability tools.

- If the user is an individual then verify the postal address, E mail id, phone no., driving licence can be soficient.

2. The second check is to ensure that user who is requesting the certificate which is cause private key corresponding the public key that send to be array. Where important as this can create legal profiles. If the user change that he/she never poses past the private

key for the corresponding public key that was send to the carrey. Then this can create legal problem to verify this a cheat, is done i.e. called as cheating the proof of position (pop) this can be done in following case:

i) The carrey demands the user to digitaly sign his/her CR (Certificate signing request) by using his/her private key. If the carrey can verify the signature using the public of that user then the carrey believe that the user.

ii) Alternatively the carrey can create a random no. challenge, encrypts it using the public key & send this challenge to the user. If the user can decrypt it using his/her private key then the carrey verify do the user exam.

iii) The carrey can generate a dumy certificate encrypt it using the users public key & sends to the use the user can decrypt it only he/she decrypt & obtain the plaintext certificate.

ID. 13.05.02?

Certificate creation: Assuming that all the step has been successful so far the carrey pass on all the details of the user to the CA. The CA does not own verification & create a digital certificate for the user.

Private key Management :

Protecting private key :- A user must field the private key secretly it must not be possible for another user to guess some ones private key. In many situation of the private key of the user might be required to be transported from one location to another. For instance suppose that the user wants to change for PCs to handle these situation there is a cryptography standard by the name PKCS #12. This allows user to export her digital certificate & private key on the form of a computer file.

Multiple key pairs :-

The public key Infrastructure (PKI) approach also recommends that in serious business applications user should posses, multiple digital certificate which also means multiple key pairs. The needs for this is that one certificate would be strictly used for signing & another for encrypt this ensures that the loss of one of the private keys does not affect the complete operations of the user.

Password protection :-

This is the simplest & most common mechanism to protect a private key. The private key is stored on the harddisk of the users use comp. as a disk file. This file can be accessed only with the help of password or personal identification no. (PIN) since any one who can guess the password correctly can

access the private key. This is considered as the last source method of protecting a private key.

Token :-

A token store a private key in an encrypted format to encrypt & access it the user must provide a one type of password which means that the password is valid only for that particular access. Next time these password becomes invalid & another must be used.
e.g. Biometrics, fingerprints.

The private key is associated with a unique characteristics of an individual (such as fingerprint, rectina scan & voice comparision) This is similar in concept to the token but here the user need not carry anything with him unlike the token.

Key update :-

Good security practice demand that the key pair should be updated ~~periods~~ periodically. This is because over time keys becomes susceptible to cryptanalysis attacks. Causing a digital certificate to expaires after a certain data ensures this. This requires an update to the key pair. The expiry of a certificate can be dealt with in one of the 2 following ways

i) The CA resource a new certificate based on the original key pair. This is not recombed, unless there is an all round confidence in the strength of the original key pair. A fresh key generated is issues as new certificate based on that a new key pair.

ii) The key update process itself can be handle

in the 2 days.

a) In the 1st approach the end user has to detect that the certificates is about to expire & request the CA to issue a new one.

b) In the other approach the expire date on the certificate is automatically change the every time it is used & as soon as it is about to expire. It's renewal request is send to the CA for this special system is to be imple.

Key Archival:-

The CA must plan for & maintain for the history of the certificate & the key of the user. For instance, suppose that some one approach the CA of alice requesting the CA to make alice digital certificate to available who used 8 year back to sign a legal document for verification purposes. If the CA has not archived the certificate how can the CA provide this information. This can cause serious legal problem therefore a key archival is very significan aceptes of any PKI services.

PKIX Model :-

The digital certificate structure format & fields. It also specifies the procedure for distributing the public key in order to extend such standards & make them universal. The internet engineering task for form the public key infrastructure. X.509 working ghead. This extends the basic phylosophy of the x.509 standard & specifies how the digital

certificate can be deployed in world of the internet.

ID-16.05.022

PKIX Services:-

PKIX identifies the primary goals of a PKI infrastructure. In the form of the following broad label services.

i) Registration :- It is the process where a end entity makes it self known into a CA. usually this is a via an agency.

ii) Initialization :- It deals with the basic problems such as how the end entity is sure that it is talking to the right CA. They have seen how this can be talked.

iii) Certificate :- In this step the CA creates a digital certificate for the end entity & returns it to the end entity. Maintenance a copy for its own records & also copies it public directories, if require.

iv) Key pair Recovery :- Key is used for encrypt may be required to be recovered at later date for decrypting some old document. key archival & recovery services can be provided by a CA or by an independent key recovery system.

v) Key Generation :- PKIX specifies that the end entity should be able to generate private & public key pairs or the CA or RA should be

able to do this for the end entities & then distribute the key securely to the end entities)

vi) Key update :- This allows a smooth transition from one expiring key pair to a fresh pair. By the automatic renewal of digital certificate. However there is a provission for manual digital certificate renewal request & response

vii) Cross certificate :- Helps in establishing trust model. So that end entities that are ~~not~~ certified by different CA can cross verify each other.

viii) Revocation :- PKIX provides support for the checking of the certificate status in 2 modes. one is online, other one is offline.

Public key cryptography standards (PKCS) :

PKCS model is an initially developed by RSA laboratory with help of respective of the host industry & academy. The main purpose of PKCS is to standardize public key infrastructure. The standardized is many respects such as formating, algorithms & APIs. This would have to develope & implement interoperable PKI solutions. Rather than every one choosing their own standards.

10.12.05.022

PKCS standards :-

Standard	purpose	Details
1. PKCS #1	RSA encryption Standard	This standard defines the basic formating rules for RSA public key function, more specifically the digital signature. It defines

			how digital signature to be calculated, structure of the structure of digital as well as format of the signature. This standard also defines the syntax for RSA private & public keys.
2.	PKCS #2	RSA encryption standard for message digest.	This standards outlines message digest calculation. However this is now merged into PKCS #1 & does not have independent existence.
3.	PKCS #3	Diffie-Hellman key agreement standard	It defines a mechanism to implement Diffie-Hellman key agreement protocol.
4.	PKCS #5	password based encryption (PBE)	It describes a methods for encrypting an octet string with a symmetric key. The symmetric key is derived from a password.
5.	PKCS #6	Extended certificate syntax standard.	It define syntax for extending the basic attributes of an X.509 digital certificate.
6.	PKCS #8	private key information standard	Describes the syntax for private key information (i.e. algorithm & an attribute used to generate the private key)
7.	PKCS #9	Selected attribute types.	It defines selected attribute types for use in PKCS #6 extended certificates (i.e. Email address, unstructured name & address).

Ch-5

Internet Security protocols

i) Static web pages :-

The main players in my internet based communication are standard of the web browser (client) & the web server (server).

Hypertext Transfer protocol :- (HTTP)

- HTTP is used for the communication between the browser & server. This is of a request response form. i.e. the browser sends a HTTP request & the server sent an HTTP response & communicated b/t them etc. These types of web pages are called as static web pages.
- A web page is created by an applicated developer or designer & it is stored on a web server. When ever any user request for that page the web server sends back that page without performing any additional processing. Here the content of the web pages donot change depending on the changes. They are always same. Hence the name is static.
- Static web pages follow a simple HTTP request request response flow.

ii) Dynamic Webpages :-

- Static web pages are not always useful they are suitable for contents that do not change often.
- For information that changes quite often stop prices whether information news & sports updates, Static web pages could not serve the purpose.

- A dynamic web pages often a call to such a program. The contents of a dynamic web pages can vary all day depending on a no. of parameters.
- Dynamic web pages are more complex than static web pages. In fact dynamic web pages are much more than HTML. Executing dynamic web pages involve server side programming.

Active Web pages:

- With the arrival of the popular to the Java Active web pages becomes quite popular. The idea behind the active web pages is actually quite symbol. When a client send an HTTP request for an active web page.
- The web server sends back the HTTP response that contents an HTML page as usual. In addition the HTML page also contains a small program that executes on the client comp. inside the web browser. usually the small program send to the browser along with the HTML page is called Java applet. An applet is a client side program written in Java programming language that can be executed by a web browser.
- Applets can be used to perform a variety of task such as painting, images graphs, charts & other drawing objects on the client browser screen.

ID. 19.03.022

Protocols & TCP/IP :-

The transmission control protocol or internet protocol S/W is the translator that makes the magic work on the internet. TCP/IP is a combinat of many protocol that facilitate the communicat bet computers over the internet.

TCP/IP layer

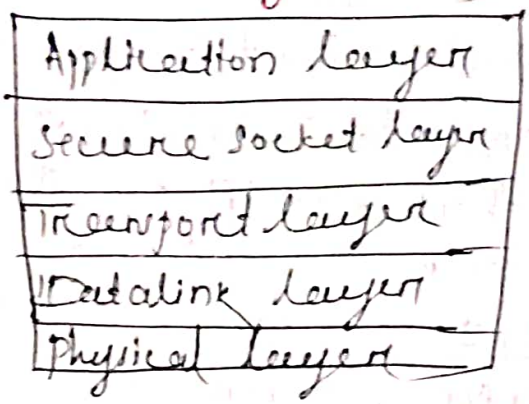
Application layer
Transport layer
Internet layer
Data link layer
physical layer

Each of these layer performs a specific routine task for instance all the application programs such as HTTP, E mail, etc are a part of the applicat layer. This when a web browser comunicates with a web server using the HTTP protocol.

The application layer comes in 2 layer the applicat layer on the client comp. ~~interact~~ interact with the transport layer of the same comp. Which in term interact with the internet layer on ther same comp. Which in term interact with the data link layer of the same comp. Which finaly interact with the physical layer of the same comp. At this stage the bits are send are voltage or current pulse via the physical transmit layer. On the server the physical layer in the form of voltage or current the direction of voltage is the

reverse physical layer to application layer.

Secure Socket layer (SSL):



Secure socket layer protocol is an Internet protocol for secure exchange of information bet^n a web browser & a webserver. It provides 2 basic secure socket.

i) Authentication
ii) Confidentiality

Logically, it provides a secure pipe line bet^n web browser & web server. Netscape operation developed in 1994. Since then SSL has become the most popular Web security mechanism. All the web browser supports SSL. Currently SSL called version 2, 3 & 3.1. The most popular of them is version 3 which was resided in 1996.

ID-20.05.022

Transport layer security (TLS) :-

It is an IETF standardization initiative whose goal is to common with an internet standard version of SSL net scale wanted

to standardize of SSL. Hence standard the protocol over to TLS there are visible difference bet SSL & TLS. The core idea & implimentation are quite similar.

Secure hypertext Transfer protocol (SHTTP):

- The SHTTP protocol is a set of security mechanism define for protecting the internet traffic. There include the data entry, forms & internet based transaction.
- The services offered by SHTTP are quite similar to those of SSL. e.g. gmail.com.
- However SSL has becomes highly successful but STTP have not the SHTTP work at the applicat° layer & is therefore tightly coupled with HTTP online essery (which seeds bet° the application transport layer)
- SHTTP support both authentication & encrypt° of HTTP traffic bet° the client & the server.
- The key difference bet° the SSL & HTTP is that SHTTP works at the label of individual message it can encrypt & sign individual message & other hand SSL does not difference bet° different message instead it aims at making the connect° bet° a client & the server, regardless of the message that they are exchanging. also SSL can not perform digital signatures. So HTTP is very readily used.

Secure Electronic Transaction (SET):

The SET is an open encryption & security specification i.e. designed for protecting credit card transactions on the internet.
SET is not a payment system it set of security protocols & format that enables the employee the existing credit card payment infrastructure in a secure manner.

- SET services can be summerise as an follow.
- It provide secure communicate channel among all the party's envolve on an e-commerce transaction.
- It provides authentication by the use of digital certificates.
- Ensures confidentiality because the information is only available to the party's available to the transaction that to when & where necessary.

SET participends:

i) Card holder
ii) Merchand
iii) Issuer
iv) Acquirer
v) payment gateway.

ID-24.05.022

i) Card holder:

- Using the internet, consumer & corporate purchasers interact with merchant for buying good/services.