PNS SCHOOL OF ENGINEERING & TECHNOLOGY

Nishamani Vihar, Marshaghai, Kendrapara

LECTURE NOTES

ON

CRYPTOGRAPHY AND NETWORK SECURITY

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

6TH SEMESTER

PREPARED BY

MR. BISWARANJAN SWAIN

LECTURER IN COMPUTER SCIENCE & ENGINEERING

Syllabus

Unit 1. Possible attacks on Computers

1.1 The need for security

1.2 Security approach

1.3 Principles of security

1.4 Types of attacks

Unit 2: Cryptography Concepts

2.1 Plain text & Cipher Text

2.2 Substitution techniques

2.3 Transposition techniques

2.4 Encryption & Decryption

2.5 Symmetric & Asymmetric key cryptography

Unit 3: Symmetric & Asymmetric key algorithms

3.1 Symmetric key algorithm types

3.2 Overview of Symmetric key cryptography

3.3 Data encryption standards

3.4 Over view of Asymmetric key cryptography

3.5 The RSA algorithm

3.6 Symmetric & Asymmetric key cryptography

3.7 Digital signature

Unit 4: Digital certificate & Public key infrastructure

4.1 Digital certificates

4.2 Private key management

4.3 PKIX Model

4.4 Public key cryptography standards

Unit 5: Internet security protocols

5.1 Basic concept

5.2 Secure socket layer

5.3 Transport layer security

5.4 Secure Hyper text transfer protocol(SHTTP)

5.5 Time stamping protocol (TSP)

5.6 Secure electronic transaction (SET)

Unit 6: User authentication

6.1 Authentication basics

6.2 Password

6.3 Authentication Tokens

6.4 Certificate based authentication

6.5 Biometric authentication

Unit 7 . Network Security & VPN

7.1 Brief introduction of TCP/IP

7.2 Firewall

7.3 IP Security

7.4 Virtual Private Network (VPN)

UNIT-1

Possible Attacks on Computers

INTRODUCTION:

The computer security in the contemporary sense is that the security of the data over the network or stored in the computer. The different aspects of security are

➢ Computer Security - generic name for the collection of tools designed to protect data and to prevent hackers.

➢ Network Security - measures to protect data during their transmission.

➢ Internet Security - measures to protect data during their transmission over a collection of interconnected networks.

1.1 THE NEED FOR SECURITY :

The computer security specifically relates to network security.

It is the security against attackers and hackers.

Network Security includes two basic securities.

The first is the security of data information i.e. to protect the information from Unauthorized access and loss.

Second is computer security i.e. to protect your computer system from unwanted damages caused due to network. One of the major reason for such damages are the viruses and spywares that can wipe off all the information from your hard disk or sometimes they may be enough destructive and may cause hardware problems too.

So there is a need to protect data and to thwart(prevent) hackers.

The security is needed for the following given reasons.

➢ To protect the secret information of users on the net only. No other person should see or access it.

➢ To protect the information from unwanted editing, accidently or intentionally by unauthorized users.

➢ To protect the information from loss and make it to be delivered to its destination properly.

➢ To manage for acknowledgement of message received by any node in order to protect from denial by sender in specific situations.

➢ To restrict a user to send some message to another user with name of a third one. For example a user X for his own interest makes a message containing some favourable instructions and sends it to user Y in such a manner that Y accepts the message as coming from Z, the manager of the organization.

➢ To protect the message from unwanted delay in the transmission lines/route in order to deliver it to required destination in time, in case of urgency.

1.2 SECURITY APPROACH

An organization can take several approaches to implement security model, so these are

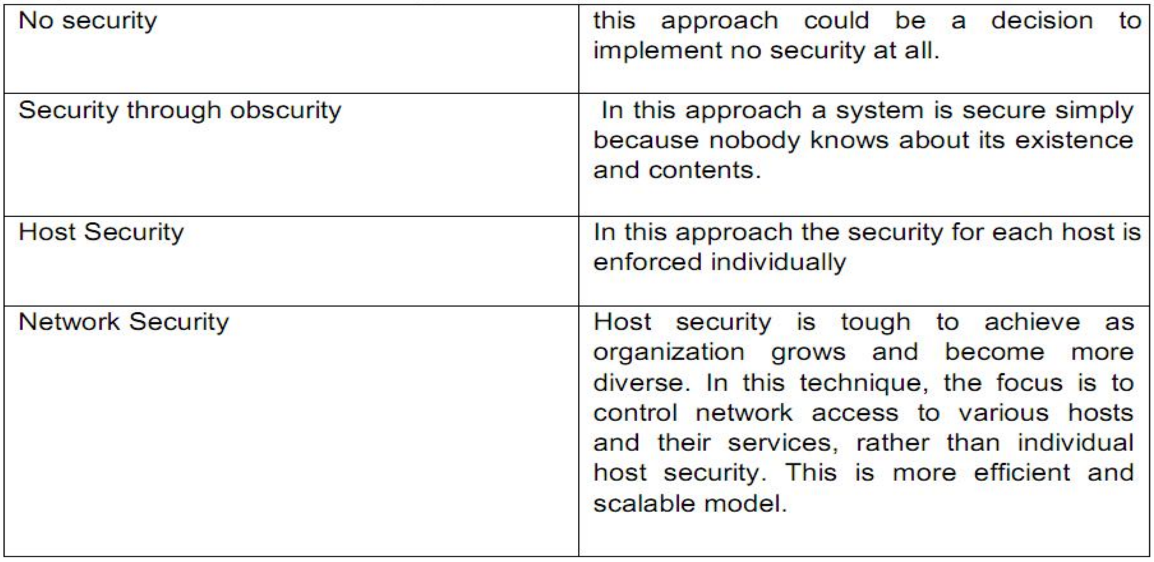
Trusted system

A trusted system is a system that is relied upon to a specified extent to enforce a specified security policy. As such, a trusted system is one whose failure may break a specified security policy.

Trusted systems are used for the processing, storage and retrieval of sensitive or classified information.

Security model

An organization can take several approaches to implements its security model.



No security	this approach could be a decision to implement no security at all.
Security through obscurity	In this approach a system is secure simply because nobody knows about its existence and contents.
Host Security	In this approach the security for each host is enforced individually
Network Security	Host security is tough to achieve as organization grows and become more diverse. In this technique, the focus is to control network access to various hosts and their services, rather than individual host security. This is more efficient and scalable model.

Security Management Practices

Good security management practices always talk of a security policy being in place.

A good security policy and its proper implementation ensures security management practices.

A good security policy generally takes care of four key aspects, as follows

Affordability : - Cost and effort in security implementation must be affordable (cost effective).

Functionality : - The mechanism of providing security must be simple.

Cultural issues: - The policy must withstand peoples' expectations, working style and beliefs.

Legality : - Policy must meet the legal requirements.

Once a security policy is in place, the following points should be ensured.

- The policy must be explained clearly to all the stake holders.
- Responsibility of everyone should be outlined.
- Simple language must be used in all the communications such that everybody could understand.
- Accountability must be fixed.
- There must be periodic reviews to verify that all the principles are being implemented or not. Also there should be provision for exception for smooth functioning of the system.

1.3 PRINCIPLES OF SECURITY

There are four chief principles of security. For a system to be secured these principles must be followed. Those are:

Confidentiality

Integrity

Authentication

Non- repudiation.

There are two more

access control

availability

Confidentiality :

- The principle of confidentiality specifies that only the sender and the intended recipients should be able to access the contents of a message.
- Confidentiality gets compromised if an unauthorized person is able to access a message.
- Example of compromising confidentiality is if user of computer A sends message to user of computer B, another user C get access to this message which is not desired .
- This type of attack is called interception.
- Interception causes loss of message confidentiality.

Integrity :

➢ When the contents of a message are changed after the sender sends it, but before it reaches the intended recipient, we say that the integrity of the message is lost. It is shown in figure.

➢ For example, consider that user A sends message to user B. User C tampers with a message originally sent by user A, which is actually meant for user B. User C change its contents and send the changed message to user B. User B has no way of knowing that the contents of the message changed after user A had sent it. User A also does not know about this change. This type of attack is called modification.

➢ Modification causes of loss of message integrity.

Authentication :

- Authentication is the process of determining the true identity of someone.
- Authentication is also used in other ways -- not just for identifying users, but also for identifying devices and data messages.
- For example suppose user C send an electronic documents to user B ,the trouble is that user C had posed as user A .
- How would user B know that the message has come from user C who is posing user A.
  This type of attack is called Fabrication.
- Fabrication is possible in absence of proper authentication mechanisms

Non-repudiation :

Non repudiation is the assurance that someone cannot deny something.

Typically, non repudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

You might send registered mail, for example, so the recipient cannot deny that a letter was delivered.

A legal document typically requires witnesses to signing so that the person who signs cannot deny having done so.

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

Access Control :

Access control is a security technique that can be used to determine who should be able to access what.

Physical access control limits access to campuses, buildings, rooms and physical IT assets.

Logical access limits connections to computer networks, system files and data.

Access control systems perform authorization identification, authentication, access approval, and accountability of entities through login credentials including passwords, personal identification numbers (PINs), biometric scans, and physical or electronic keys.

Access control specifies and control who can access what.

Availability :

Availability of information refers to ensuring that authorized parties are able to access the information when needed.

Information only has value if the right people can access it at the right times.

Denying access to information has become a very common attack nowadays, For example, due to the intentional actions of an unauthorized user C, an authorized user A may not be able to contact a server computer B.

This would defeat the principle of availability. Such an attack is called as **interruption.**

Interruption puts the availability of resources in danger.

1.4 TYPES OF ATTACK:

The attack on computer system are grouped into following two categories

1. Passive attacks
2. Active attacks

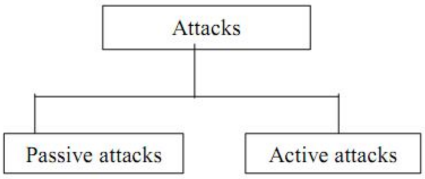


Fig. 1.1

a) Passive attacks:-

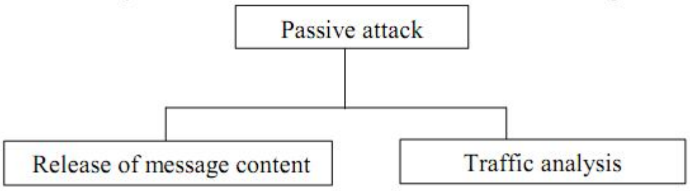
In passive attack, the attacker's goal is just to obtained information.

This means that the attack does not modify data or harm the system.

Passive attack do not involves any modifications to contents of an original message.

Passive attacks are difficult to detect.

Further the passive attacks are classified into two sub-categories.



(Types of passive attacks)

Fig. 1.2

Release of message content:-

Release of message content is quite simple to understand.

When we send a confidential email message to our friend, we desire that only she be able to access it.

Otherwise, the content of the message are released against our wishes to someone else.

Using certain security mechanisms, we can prevent release against contents.

Traffic analysis:-

If we had encryption protection, an attacker might still be able to observe the pattern of the messages . Such attempts of analyzing messages to come up with likely pattern are known as traffic analysis attacks.

Passive attacks are difficult to detect because they do not involves any alteration of the data.

b) Active attacks: -

Active attacks may change the data or harm the system. Attacks that threatens the integrity and availability are active attacks.

Active attacks are normally easier to detect than to prevent, because an attackers can launch them in a variety of ways.

In active attack, the content of the original message are modified in some way .

It is quite difficult to prevent active attacks absolutely, because to do so would require physical protection of all communication facilities and paths at all times. Instead, the goal is to detect them and to recover from any disruption or delays caused by them.

Active attacks are divided into three categories:

Masquerade –

One entity pretends to be a different entity.

In a masquerade attack, the intruder pretends to be a particular user of a system to gain access or to gain greater privileges than they are authorized for. A masquerade may be attempted through the use of stolen login IDs and passwords, through finding security gaps in programs or through bypassing the authentication mechanism.

Example user C might pose as user A and send a message to user B. User B might be led to believe that the message came from A.

Replay attack –

Involves passive capture of a data unit and its subsequent transmission to produce an unauthorized effect.

Example suppose user A wants to transfer some amount to user C .Both users A and C have accounts with bank B. User A might send an electronic message to bank B requesting for the fund transfer. User C could capture this message and send a second copy to bank B would have no idea that this is an unauthorised message and would treated as second and different. Therefore user C would get the benefit of the found transfer twice.

Alteration of messages–

Some portion of message is altered or the messages are delayed or recorded, to produce an unauthorized effect.

Suppose user A(Bob) send an electronic message transfer $1000 to D‟s account to bank B(alice). User C (Darth) might capture this message and change it to $10000.

Denial of service –

Denial of service (DOS) attacks make an attempt to prevent legitimate users from accessing some services, which they are eligible for. For instance, an unauthorized user send too many login requests to a sever using random user ids one after the other in quick succession, so as to flood the network and deny other legitimate users from using the network facilities.

Computer Security (Program that attacks):-

A few programs that attack computer system are:

Virus:-A virus is a computer program that attaches itself to another legitimate program and causes damage of the computer system or to the network. During the life time a virus goes through four phases

1. Dormant phases:-Here the virus is idle it gate activated on certain action or event
2. Propagation phase:-In this phase a virus copy itself and each copy start creating more copies of self .
3. Triggering phase:-A dormant virus move into this phase when the action event or event for which it was waiting is initiated.
4. Execution phase:-this is actual work of the virus.

Virus can be classified into

Parasitic virus

Memory resident virus

Boot sector virus

Stealth virus

Polymorphic virus

Metamorphic virus

Micro virus

Worm:- A worm does not perform any destructive action and instead only consumes system resources to bring it down. a virus modify a program but worm does not modify a program, it replicate itself again and again.

Trojan horse:-A Trojan horse allow an attacker to obtain some confidential information about a computer or network.

Applets and active AX:-Java applets and active AX control are small client side programs that might cause security problems , if used by attackers with a malicious intention .

Questions on Unit –I

1.Write down the principles of security and explain.

2. Explain the type of passive attacks.

3. Explain the type of active attacks.

4. What are the difference between active attack and passive attack.

UNIT-II

CRYPTOGRAPHY CONCEPTS

1.1 CRYPTOGRAPHY TECHNIQUES :

From the beginning any era, human being has two natural needs for communication:

(a) To communicate and share information and

(b) To communicate selectively.

- These two needs gave rise to the art of coding the messages in such a way that only the intended people could have access to the information. Unauthorized people could not extract any information.
- The word "cryptography‟ is the combination of two Greek words, "Krypto" meaning hidden or secret and "graphene" meaning writing.

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

✓ The art or science encompassing the principles and methods of transforming an intelligible/understandable message into one that is unintelligible/non-understandable form, and then retransforming that message back to its original form.

Cryptanalysis: It is the technique of decoding messages from a non-readable format back to a readable format.

✓ It is done without knowing how they were initially converted from readable format to non-readable format.

✓ Also called code breaking.

Cryptology: is a combination of cryptography and cryptanalysis.

✓ Cryptography + Cryptanalysis = Cryptology.

Some Keywords:

Plain Text : Clear text or plain text signifies a message that can be understood by the sender, the recipient and also by anyone else who gets an access to that message.

Example: Hi Amit.

Cipher Text : When a plain text message is codified using any suitable scheme, the resulting message is called as cipher text.

Example: Plain Text: Hi Amit.

Cipher Text: Ki Dplw.

Encryption/ Encipher/Encrypt:

- Converting plaintext to cipher text.
- Encryption is the process of encoding a message or plain text so that cipher text can be produced.
- Plaintext is converted into cipher text by using encryption algorithm.
- Converting cipher text into plaintext.
- Decryption is the reverse process, transforming an encrypted message back into its normal text/plaintext.
- This is done by using decryption algorithm.

Cipher:

- Encryption and Decryption algorithms are together known as cipher.

Key:

- It is a number or set of numbers on which the cipher operates. Encryption Technique/ transforming a Plaintext into Ciphertext:
- Clear text, or plain text, signifies a message that can be understood by the sender, the recipient, and also by anyone else who gets access to that message. When a plain-text message is codified using any suitable scheme, the resulting message is called cipher text.

2.2 ENCODING TECHNIQUES:

- There are two primary ways in which a plain-text message can be codified/ transform to obtain the corresponding cipher text:

– Substitution technique
– Transposition technique.

1) **Substitution-cipher technique:**

In the substitution-cipher technique, each character of a plain-text message is replaced by other character, number or symbol.

There are several techniques. They are:

– Caesar Cipher
– Modified version of Caesar Cipher
– Mono-alphabetic Cipher
– Homophonic Substitution Cipher
– Polygram Substitution Cipher
– Polyalphabetic Cipher

i) <u>Caesar Cipher</u>

- Proposed by Julius Caesar.
- Mechanism to make a plaintext message into cipher text message.
- It replacing each letter of the alphabet with the letter standing n places further down the alphabet.
- Example: Replace each A with D, B with E, etc.

ABCDEFGHIJKLMNOPQRSTUVWXYZ
DEFGHIJKLMNOPQRSTUVWXYZABC
PT: KIIT
CT: NLLW

ii) ***<u>Modified Version of Caesar Cipher :</u>***

Modified version Caesar cipher is Caesar cipher but an alphabet A in plain text would not necessarily be replaced by D.

It can be replaced by an any valid alphabet, i .e. by E or by F or by G and so on .

Once replacement scheme is decided, it would be constant and will be used for all other alphabets in that message.

The English language contains 26 alphabets thus an alphabet A can be replaced by any alphabet in the English alphabet set (i.e. b to z) of course. it does not make sense to replace an alphabet by itself(means A is replaced by A) that means each alphabet has 25 possible of replacement.

A mechanism of encoding the message so that they can send securely is called cryptography.

Few terms are used in cryptography:-

Brute force attack:-

An attacks on a cipher text message, where they attacker attempt to use all possible permutation and combination is called as a brute force attack.

Cryptanalysis:-

The process of trying to break any text message to obtain the original plain text message itself is called cryptanalysis.

Cryptanalyst:-

The person attempting a cryptanalysis is called cryptanalyst.

iii) ***Mono-alphabetic Cipher:***

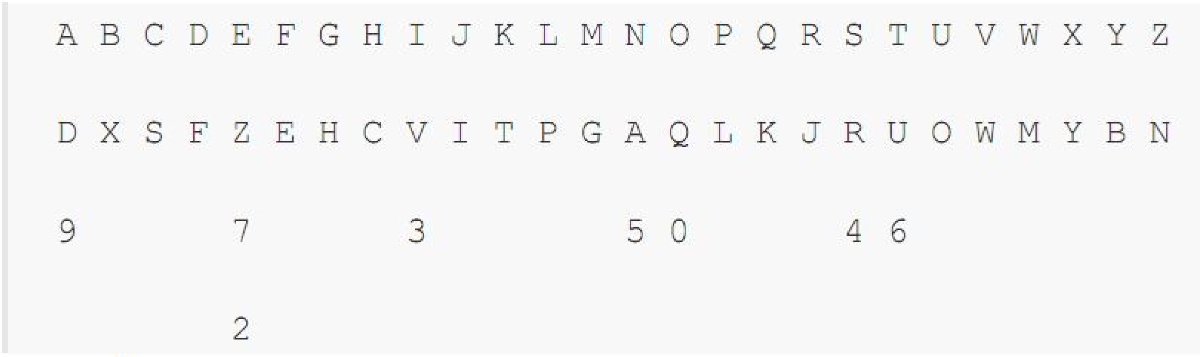
- A mono-alphabetic cipher is a substitution cipher where a symbol in the plaintext has a one-to-one relationship with a symbol in the cipher text.
- It means that a symbol in the plaintext is always replaced with the same symbol in the cipher text, irrespective of its position in the plaintext.
- It uses random substitution.
- This means that in a given plain-text message, each A can be replaced by any other alphabet (B through Z), each B can also be replaced by any other random alphabet (A or C through Z), and so on. The crucial difference being, there is no relation between the replacement of B and replacement of A. That is, if we have decided to replace each A with D, we need not necessarily replace each B with E—we can replace each B with any other character!
- To put it mathematically, we can now have any permutation or combination of the 26 alphabets, which means (26 x 25 x 24 x 23 x ... 2) or 4 x 1026

possibilities! This is extremely hard to crack.

iv) Homophonic Substitution Cipher

The Homophonic Substitution cipher is a substitution cipher in which single plaintext letters can be replaced by any of several different cipher text letters.

They are generally much more difficult to break than standard substitution ciphers. The number of characters each letter is replaced by is part of the key, e.g. the letter 'E' might be replaced by any of 4 different symbols(z,7,2,1), while the letter 'Q' may only be substituted by 1 symbol (k) as shown on Fig 2.4



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	X	S	F	Z	E	H	C	V	I	T	P	G	A	Q	L	K	J	R	U	O	W	M	Y	B	N
9				7				3					5	0				4	6						
				2																					

1

Example to encipher the message , DEFEND THE EAST WALL OF THE CASTLE, we find „D‟ in the top row, then replace it with the letter below it, „F‟. The second letter, „E‟ provides us with several choices; we could use any of „Z‟, „7‟, „2‟ or „1‟. We choose one of these at random, say „7‟. After continuing with this, we get the cipher text:

Plain text: DEFEND THE EAST WALL OF THE CASTLE

Cipher text: F7EZ5F UC2 1DR6 M9PP 0E 6CZ SD4UP1

v) *Polygram substitution :*

A simple substitution cipher substitutes for single plaintext letters. In contrast, polygram substitution ciphers involve groups of characters being substituted by other groups of characters.

In Polygram Substitution Cipher technique replaces one block of plain text with a block of cipher text-it does not work on character by character.

For example, HELLO can be replaced by YUQQW, but HELL could be replaced by a totally different cipher text block TEUI.

vi) *Poly-alphabetic Substitution Cipher :*

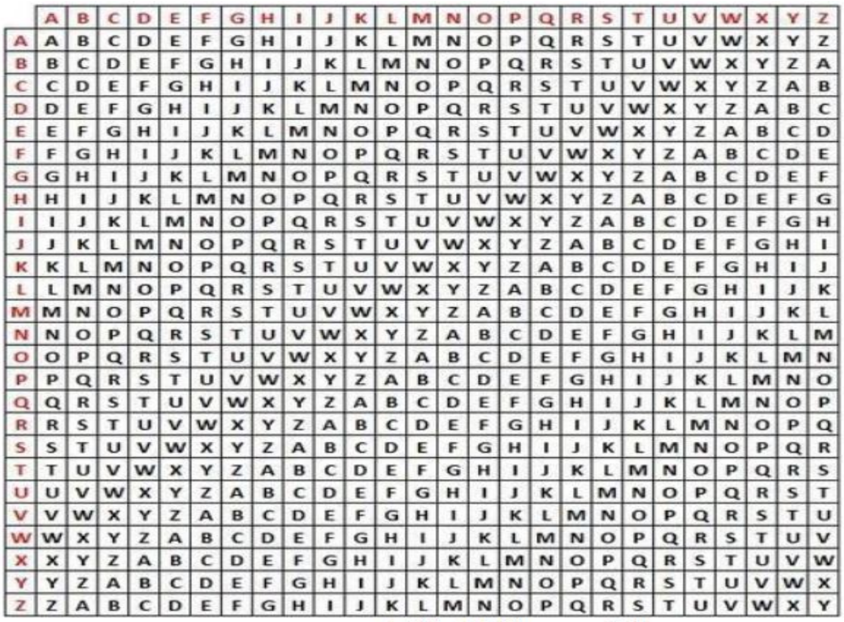
A poly-alphabetic substitution cipher involves the use of two or more cipher alphabets.

Instead of there being a one-to-one relationship between each letter and its substitute, there is a one-to-many relationship between each letter and its substitutes.

The Vigenere Cipher and Beaufort Cipher are example of Poly-alphabetic Substitution Cipher .

The Vigenere Table

The Vigenere Cipher, proposed by Blaise de Vigenere from the court of Henry III of France in the sixteenth century, is a poly-alphabetic substitution based on the following table.



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

Keyword:	RELAT IONSR ELATI ONSRE LATIO NSREL
Plaintext:	TOBEO RNOTT OBETH ATIST HEQUE STION
Cipher text:	KSMEH ZBBLK SMEMP OGAJX SEJCS FLZSY

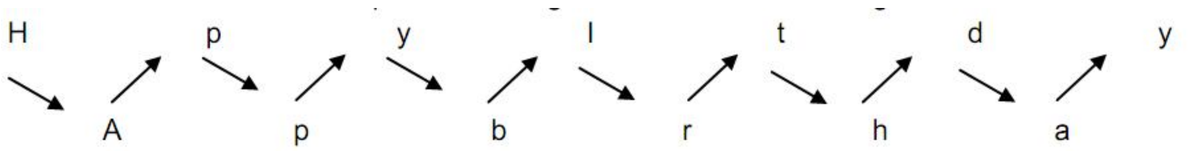
2.3 TRANSPOSITION TECHNIQUES :

As we have seen in substitution technique we replace each plain text with new alphabets in cipher text but in transposition, we don’t replace one alphabet with another alphabet. We just rearrange the positions of plain text and get the cipher text. Techniques used in transposition:

i) *Rail fence Technique:*

It is a type of transposition technique which rotates the position of plain text message.

Example, suppose that we have a plain text message HAPPY BIRTHDAY we can convert this text in cipher text using rail fence as shown in following figure.



text: HPYITDYAPBRHA

Algorithm :

Arrange the plain text message in sequence of diagonals as shown above .

Read the text row by row and write it in sequence and thus we will get the cipher text.

ii) ***Simple columnar transposition technique:***

It rotates the position of alphabets in plain text and then find out the cipher text.

Algorithm:

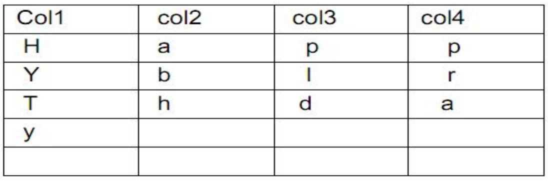
a) write the plain text message in a rectangle of pre defined size.

b) Read the message column by column in random order of columns.

c) The message obtained by doing so is the cipher text.

Example, suppose plain text that we have to encrypt is HAPPY BIRTHDAY. We can encrypt this as follows:

Consider a rectangle with four columns and write the plain text row by row.



Col1	col2	col3	col4
H	a	p	p
Y	b	I	r
T	h	d	a
y			

Now decide the order of columns as random order. Suppose order decided is 3,1,4,2 and read the text in this order.

Resulting text is the cipher text that is in this example cipher text is PIDHYTYPRAABH

iii) ***Simple columnar transposition technique with multiple rounds:***

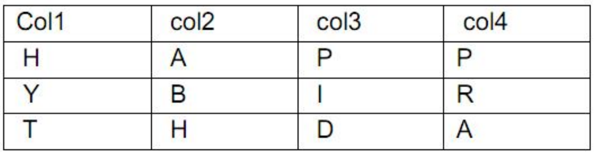
On improve the simple columnar transposition technique, we increase the complexity of this technique by implementing the same steps twice or thrice or depending upon the security of message.

Algorithm:

1. write the message row by row in a rectangle of pre defined size.
2. Read the message column by column in random order of columns.
3. The message thus obtained is cipher text.
4. Repeat steps a to c as many times as needed.

Example, consider the same PLAIN TEXT as above HAPPY BIRTHDAY.

a) Consider a rectangle with four columns and write the plain text row by row as shown in table

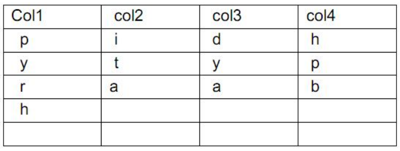


Col1	col2	col3	col4
H	A	P	P
Y	B	I	R
T	H	D	A

b) Now decide the order of columns as random order. Suppose order decided is 3,1,4,2 and read the text in this order.

c) Resulting text is the cipher text that is in this example cipher text is PIDHYTYPRAABH

d)Perform step a to c once more.



Col1	col2	col3	col4
p	i	d	h
y	t	y	p
r	a	a	b
h			

iv) <u>Vernam Cipher (One-Time-Pad)</u>

The vernam Cipher, also called as One-Time Pad, is implemented using a random set of non-repeating characters as the input cipher text. The most significant point here is that once an input cipher text for transposition is used, it is never used again for any other message (hence the name one-time).

The length of the input cipher text is equal to the length of the original plain text. The algorithm used in Vernam Cipher

1. Treat each plain text alphabet as a number in an increasing sequence, i.e. A=0, B=1, ... Z=25.
2. Do the same for each character of the input cipher text.
3. Add each number corresponding to the plain text alphabet to the corresponding input cipher text alphabet number.
4. If the sum thus produced is greater than 26, subtract 26 from it.
5. Translate each number of the sum back to the corresponding alphabet. This gives the output cipher text.

Let us apply the Vernam Cipher algorithm to a plain text message HOW ARE YOU using a one-time pad NCBTZQARX to produce a cipher text message UQXTQUYFR.

It should be clear that since the one-time pad is discarded after a single use, this technique is highly secure and suitable for small plain text message, but is clearly impractical for large messages. The Vernam Cipher was first implemented at AT&T with the help of a device called as Vernam Machine.

Vernam Cipher uses a one-time pad, which is discarded after a single use and therefore, is suitable only for short messages.

2.4 ENCRYPTION & DECRYPTION

Encryption or Encoding or Encode:

- ➢ The process of converting or transforming plain text or original text into cipher text is called as encoding.
- ➢ This new form of the message is totally different from the initial message.
- ➢ It occurs at the sender's side.
- ➢ The sender uses an encryption algorithm and a key to transform the original message into an encrypted message i.e., cipher text.
- ➢ Encryption is also called enciphering .

Decryption or Decoding :

- ➢ The process of converting cipher text into plain text is called as decoding.
- ➢ It occurs at the receiver's end.
- ➢ The receiver uses decryption algorithms and a key to transform the cipher text back to original plaintext message.
- ➢ The decryption is also called deciphering or decipherment.
- ➢ Decryption is the reverse process of encryption.

Questions on Unit-II

1. What is substitution technique? Explain with example.
2. What is transposition technique ? Explain with example.
3. Write down the difference between encryption and decryption.

UNIT-III

SYMMETRIC & ASYMMETRIC KEY ALGORITHMS

ALGORITHM TYPES:

➢ It defines what size of plain text should be encrypted in each step of algorithm.

There are two aspects of algorithms: algorithm types and algorithms modes.

Algorithm Types:- An algorithms type defines what size of plain text should be encrypted in each step of algorithm. Based on this, algorithms are of two types:

Stream Cipher- In stream cipher the plain text is encrypted one byte at a time and the decryption happens one byte at a time.

Block Cipher-In block cipher the plain text is encrypted one block of text at a time and decryption also takes one block at a time.

ALGORITHM MODES:

The algorithm mode define the details of the cryptography algorithm, once the type is decided. An algorithm mode is combination of a series of the basic algorithm steps on the block cipher and some kind of feedback from the previous steps. There are 4 types of algorithm modes.

Electronic Code Book- ECB is the simplest mode of operation; the incoming plain text message is divided into blocks of 64 bits each. Each such block is then encrypted independently of the other blocks. For all blocks in a message, the same key is used for encryption.

Cipher Block Chaining- CBC mode ensures that even if a block of plain text repeats in the input, these two identical plain text yields totally different cipher text blocks in the output. For this a feedback mechanism is used.

Cipher Feedback- CFB mode encrypts data in units that's smaller e.g. they could be of size 8 bits than a defined block size.

Output Feedback- OFB mode is extremely similar to the CFB. The only difference is that is the case of CFB, the cipher text is fed into the next stage of encryption process. But in the case of OFB, the output of the Initial Vector (IV) encryption process is fed into the next stage of encryption process.

The important aspects of Encryption & Decryption process are:

Algorithm:

➢ The technique/ method used to encrypt or decrypt. Algorithm is generally not kept secret.

Key:

➢ A key is a character or a group of characters used to encrypt or decrypt the plain text. A key is generally kept secret.

Depending on what keys are used, there are two types of cryptography mechanisms/ types of cryptography:

Symmetric Key Cryptography:

➢ Symmetric key cryptography uses the same key for encryption and decryption.

Asymmetric Key Cryptography:

➢ Asymmetric key cryptography uses one key for encryption, and another different key for decryption.

3.1 OVERVIEW OF SYMMETRIC KEY CRYPTOGRAPHY

An encryption system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message.

Symmetric-key systems are simpler and faster, but their main drawback is that the two parties must somehow exchange the key in a secure way.

With symmetric encryption, both parties use the same key for encryption and decryption purposes. Each user must possess the same key to send encrypted messages to each other.

The sender uses the key to encrypt their message, and then transmits it to the receiver.

The receiver, who is in procession of the same key, uses it to decrypt the message.

The security of this encryption model relies on the end users to protect the secret key properly. If an unauthorized user were able to intercept the key, they would be able to read any encrypted messages sent by other users.

Conceptually it as similar to physical lock, perhaps a door lock. The same key is used to lock and unlock the door.

Some examples of symmetric-key algorithms include Data Encryption Standard (DES), double DES, triple DES, and Advanced Encryption Standard (AES).

Diffie-Hellman Key Exchange/Agreement Algorithm :

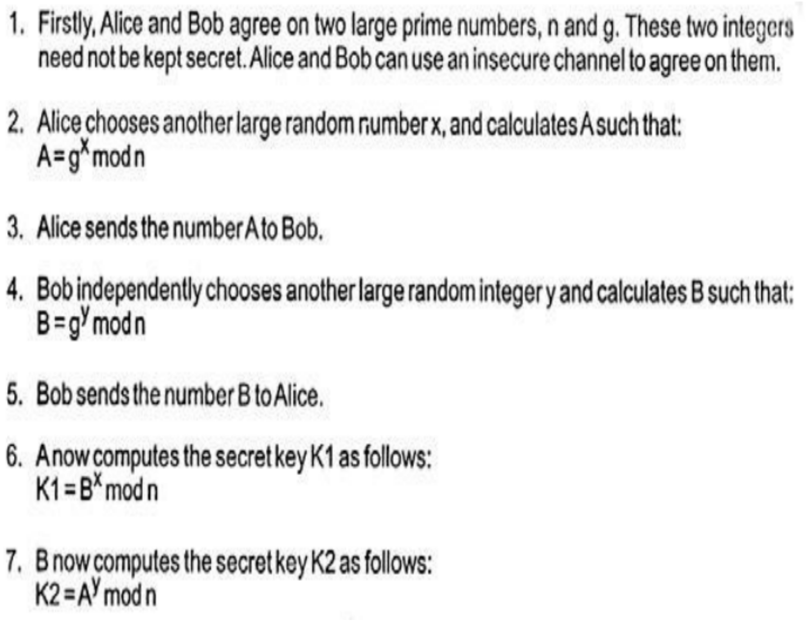
Whitefield Diffie and Martin Hellman devised an amazing solution to the problem of key agreement or key exchange in 1976.

This solution is called as the Diffie-Hellman Key Exchange/Agreement Algorithm.

The two parties, who want to communicate securely, can agree on a symmetric key using this technique.

This key can then be used for encryption / decryption. However, we must note that Diffie – Hellman key exchange algorithm can be used only for key agreement, but not for encryption or decryption of messages.

Description of the Algorithm: Let us assume that Alice and Bob want to agree upon a key to be used for encrypting / decrypting messages that would be exchanged between them. Then, the Diffie-Hellman key exchange algorithm works as follows.



1. Firstly, Alice and Bob agree on two large prime numbers, n and g. These two integers need not be kept secret. Alice and Bob can use an insecure channel to agree on them.

2. Alice chooses another large random number x, and calculates A such that:
   $A = g^x \bmod n$

3. Alice sends the number A to Bob.

4. Bob independently chooses another large random integer y and calculates B such that:
   $B = g^y \bmod n$

5. Bob sends the number B to Alice.

6. A now computes the secret key K1 as follows:
   $K1 = B^x \bmod n$

7. B now computes the secret key K2 as follows:
   $K2 = A^y \bmod n$

- Example of Algorithm

.

1. Firstly, Alice and Bob agree on two large prime numbers, n and g. These two integers need not be kept secret. Alice and Bob can use an insecure channel to agree on them.

   Let n = 11, g=7.

2. Alice chooses another large random number x, and calculates A such that :
   $A = g^x \bmod n$

   Let x=3. Then, wwe have, $A=7^3 \bmod 11 = 343 \bmod 11$

   Let x=3. Then, wwe have, $A=7^3 \bmod 11 = 343 \bmod 11 = 2$

3. Alice sends the number A to Bob.

   Alice sends A=2 to Bob

4. Bob independently chooses another large random integer y and calculates B such that :
   $B = g^y \bmod n$

   Let y=6. Then we have,

   $B = 7^6 \bmod 11 = 117649 \bmod 11 = 4$

5. Bob sends B=4 to Alice

6. A now computes the secret key K1 as follows :
   $K1 = B^x \bmod n$

   We have, $K1 = 4^3 \bmod 11 = 64 \bmod 11 = 9$

7. B now computes the secret key K2 as follows :
   $K2 = A^y \bmod n$.

   We have, $K2 = 2^6 \bmod 11 = 64 \bmod 11 = 9$.

Asymmetric Key Operation:

The asymmetric-key encipherment also called public-key encipherment or public-key cryptography, was introduced by Diffie and Hellman in 1976 to overcome the problem found in symmetric key cryptography.

It uses two different keys for encryption and decryption.

Asymmetric Encryption is a form of Encryption where keys come in pairs. What one key encrypts, only the other can decrypt. In the sense that if key A encrypts a message, and then B can decrypt it, and if key B encrypts a message, then key A can decrypt it.

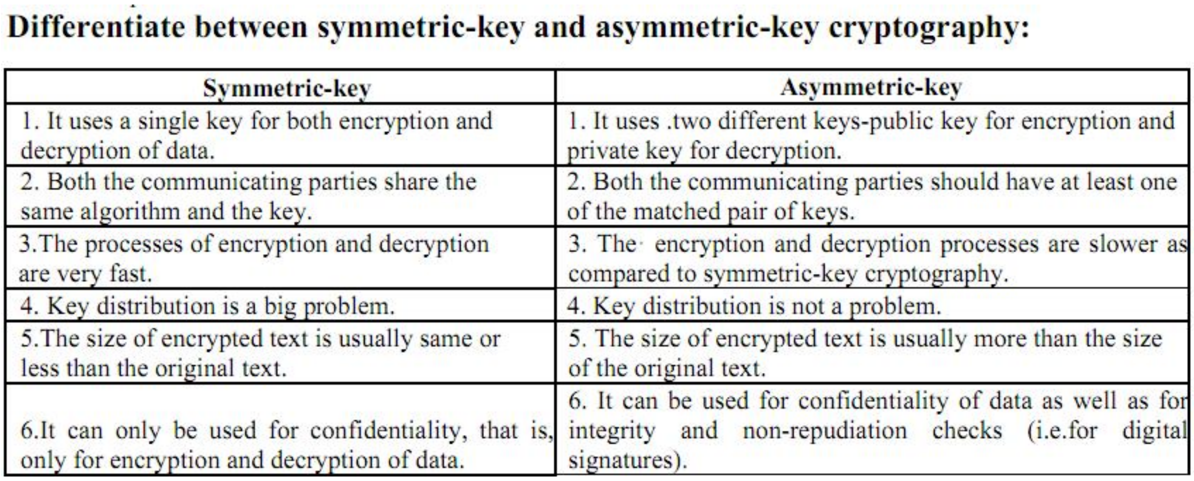
These two keys are referred to as the public key (used for encryption) and the private key (used for decryption).

Each authorized user has a pair of public and private keys. The public key of each user is known to everyone, whereas the private key is known to its owner only.

Asymmetric Encryption is also known as Public Key Cryptography, since users typically create a matching key pair, and make one public while keeping the other secret.

RSA is a well-known example of asymmetric-key algorithm.

The main advantage of public-key cryptography is that the sender and the receiver need not have to share the secret key. All communication involves only public keys.
Thus, the private key is never transmitted or shared. Anyone can send a confidential message using a public key, but the message can only be decrypted with a private key, which is kept by the intended recipient.



Differentiate between symmetric-key and asymmetric-key cryptography:

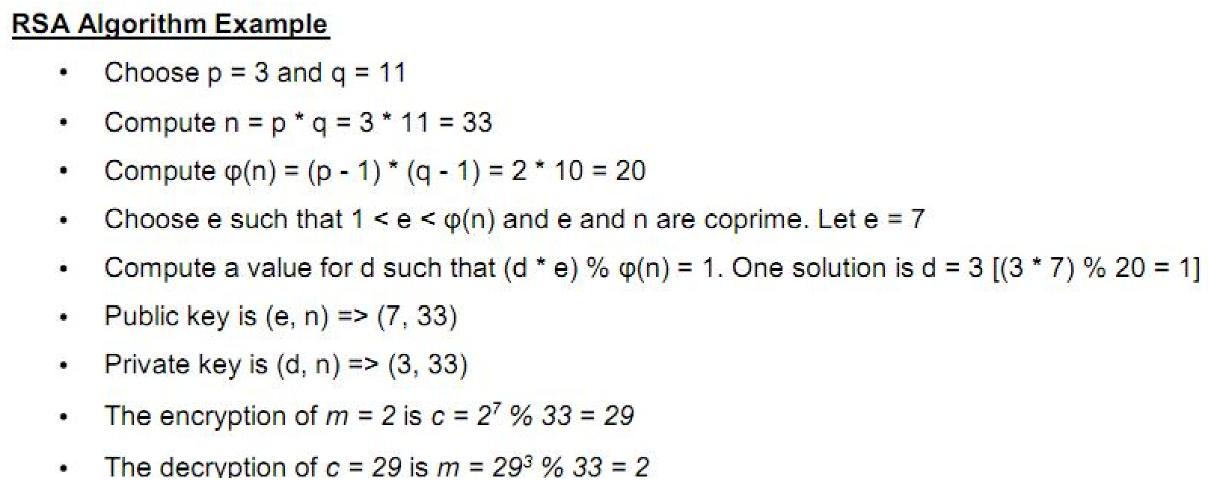
Symmetric-key	Asymmetric-key
1. It uses a single key for both encryption and decryption of data.	1. It uses .two different keys-public key for encryption and private key for decryption.
2. Both the communicating parties share the same algorithm and the key.	2. Both the communicating parties should have at least one of the matched pair of keys.
3.The processes of encryption and decryption are very fast.	3. The encryption and decryption processes are slower as compared to symmetric-key cryptography.
4. Key distribution is a big problem.	4. Key distribution is not a problem.
5.The size of encrypted text is usually same or less than the original text.	5. The size of encrypted text is usually more than the size of the original text.
6.It can only be used for confidentiality, that is, only for encryption and decryption of data.	6. It can be used for confidentiality of data as well as for integrity and non-repudiation checks (i.e.for digital signatures).

3.5 THE RSA ALGORITHM

The RSA algorithm is named after Ron Rivest, Adi Shamir and Len Adleman, who invented it in 1977 [RIVE78].
The RSA cryptosystem is the most widely-used public key cryptography algorithm in the world. It can be used to encrypt a message without the need to exchange a secret key separately.
The RSA algorithm can be used for both public key encryption and digital signatures.
Its security is based on the difficulty of factoring large integers.
Party A can send an encrypted message to party B without any prior exchange of secret keys.
A just uses B's public key to encrypt the message and B decrypts it using the private key, which only he knows. RSA can also be used to sign a message, so A can sign a message using their private key and B can verify it using A's public key

RSA algorithm

1. Choose two large prime number P and Q .
2. Calculate N =P x Q .
3. Select the public key (i.e the encryption key) E such that it is not a factor of (P-1) and (Q-1).
4. Select the private key (i.e the decryption key) D such that the following equation is true:
   (D*E) mod (P-1) *(Q-1) = 1
5. For encryption, calculate the cipher text CT from the plain text PT as follows:
   CT=PTE mod N.
6. Send CT as the cipher text to the receiver.
7. For decryption, calculate the plain text PT from the cipher text CT as follows:
   PT=CTD mod N.



RSA Algorithm Example

- Choose p = 3 and q = 11
- Compute n = p * q = 3 * 11 = 33
- Compute φ(n) = (p - 1) * (q - 1) = 2 * 10 = 20
- Choose e such that 1 < e < φ(n) and e and n are coprime. Let e = 7
- Compute a value for d such that (d * e) % φ(n) = 1. One solution is d = 3 [(3 * 7) % 20 = 1]
- Public key is (e, n) => (7, 33)
- Private key is (d, n) => (3, 33)
- The encryption of $m = 2$ is $c = 2^7 \% 33 = 29$
- The decryption of $c = 29$ is $m = 29^3 \% 33 = 2$

3.3 DATA ENCRYPTION STANDARDS

The data encryption standard (DES) is a common standard for data encryption and a form of secret key cryptography (SKC), which uses only one key for encryption and decryption.

In 1972, the National Bureau of Standards (NBS) approached the Institute for Computer Sciences and Technology (ICST) to devise an encryption algorithm to secure, stored and transmitted data. The algorithm would be publicly available, but its key would be top secret.

The National Security Agency (NSA) assisted with the cryptographic algorithm evaluation processes, and in 1973, submission invitations were posted in the Federal Register.

In 1977, NBS issued the algorithm, i.e., DES.

DES WORKING PRINCIPLE

DES is a block cipher. It encrypts data in block of size 64 bits. That is 64 bits of plain text goes as the input to DES, which produce 64 bits of cipher text. The same algorithm and Key are used for encryption and decryption.

Actually the initial key consists of 64 bits. However before DES process even starts every eight bit of the key is discarded to produce 56 key. The bit position 8,16,24,32,56,64 are discarded.

DES is based on the two fundamental attributes, Substitution (also called as confusion) And transposition (also called as Diffusion).

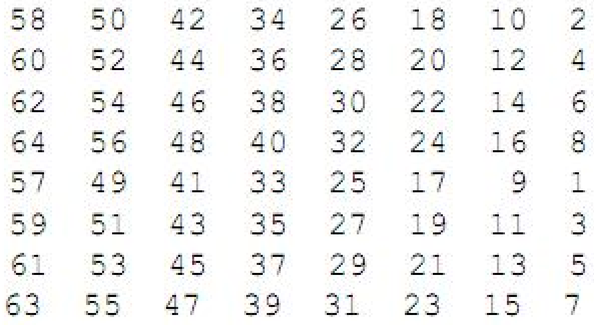
Steps of DES

1. The 64-bit plain text block is handed over to an initial Permutation (IP) function.
2. The Initial Permutation produces 2 halves of permuted block .let Left Plain Text (LPT) and Right Plain Text (RPT).
3. Each LPT and RPT go through 16 rounds of encryption process.
4. In the end LPT and RPT are rejoined and Final Permutation (FP) is performed on the combined block.
5. The result of the process 64 bit cipher text.

Initial Permutation

The 64 bits of the input block to be enciphered are first subjected to the following permutation, called the initial permutation IP:

IP



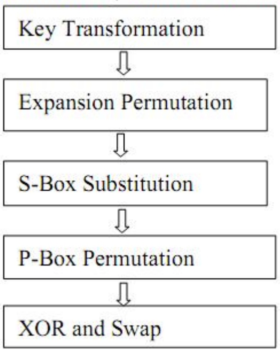
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

That is the permuted input has bit 58 of the input as its first bit, bit 50 as its second bit, and so on with bit 7 as its last bit. The computation which uses the permuted input block as its input to produce the pre-output block consists, but for a final interchange of blocks, of 16 iterations of a calculation that is described below in terms of the cipher function f which operates on two blocks, one of 32 bits and one of 48 bits, and produces a block of 32 bits.

Let the 64 bits of the input block to an iteration consist of a 32 bit block LPT followed by a 32 bit block RPT. Using the notation defined in the introduction, the input block is then LR.

Rounds

Each of the 16 rounds in turn , consists of the following steps



Key Transformation

Let K be a block of 48 bits chosen from the 56-bit key. A different 48 bit sub key is generated during each round using a process called as Key transformation. For this the 56-bit key is divided into 2 halves each of 28 bits. These halves are circularly shifted left by one or two positions, depending on the round. For example, if the round number is 1, 2, 9 or 16, the shift is done by only positions. For other rounds, the circular shift is done by two positions.

Expansion Permutation

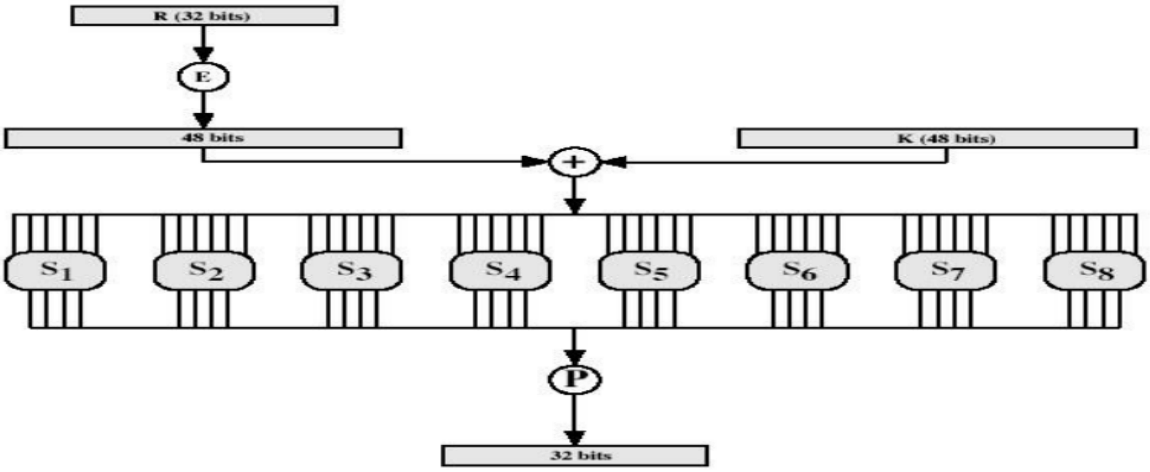
We had two 32 bit plain text called LPT and RPT. During expansion permutation the RPT is expanded from 32 bits to 48 bits. This happens as follows The 32-bit RPT is divided into 8 blocks, having 4 bits in each block.

Each 4 bit blocks of the previous step is then expanded to a corresponding 6 blocks, 2 more bits are added they are actually the repeated first and fourth of the 4 bit block.

The Key transformation processes compress the 56 bit key to 48 bits. Then the Expansion permutation process expands the 32 bit RPT to 48 bit. Now the 48 bit key and 48 bit RPT is XORed and the resulting is given to the S-box Substitution.

S-Box Substitution:

It is the process that accepts 48-bit input from the XOR operations and produces a 32 bit output using substitution technique. The Substitution is performed by 8 substitution boxes called as S-boxes. Each of 8 boxes has a 6 –bit input and 4 bit output.



P-Box Permutation

The out put of S-box consists of 32 bits. these 32 bits are permuted using a P-box.

XOR and Swap

The 32 bit RPT and 32 bit LPT is XORed and swap means the LPT becomes and RPT and vice versa.

Final Permutation

At the end of the 16 rounds the final permutation is performed (only once).

The nature of DES algorithm: of more concern is that cryptanalysis is possible by exploiting the characteristics of DES. The focus is the eight S-boxes used in each iteration.

The design criteria for the complete algorithm has never been published and there has been speculation that the boxes were constructed in such a way that cryptanalysis is possible by an opponent who knows the weakness in the S-boxes. Although this has not been established, the US governments' "clipper project" raises many questions. These are the main reasons DES is now being replaced by the AES standard.

Using a brute-force attack by simply searching for a key is possible. However, for 56-bit key, there are 256 possible key combinations, if we could search one key in 1 µs, then we need 2283 years to try all keys. (Distributed.net broke a DES-56 within 22 hours and 15 minutes, by using 100,000 PCs).

DES decryption

The decryption process with DES is essentially the same as the encryption process and is as follows:

Use the cipher text as the input to the DES algorithm but use the keys K in reverse order.

That is, use K16 on the first iteration, K15 on the second until K1Which is used on the 16th and last iteration .

Variation of DES:

In spite of its strength it is felt that with the tremendous advance in computer hard ware, DES is susceptible to possible attack. However because DES is already proven to be a very competent algorithm, it would be nice to reuse DES by making it stronger by some means, rather than writing a new cryptography algorithm. Two main variation of DES are Double DES and Triple DES.

Double DES

Double DES is quite simple ,it does twice what DES normally does only once. Double DES uses two keys K1 and K2. The final output is encryption of encrypted text.

Triple DES

Triple DES means DES three times. It comes in 2 flavour : one that uses 3 keys and second that uses 2 keys.

Triple DES with 3 keys – the plain text encrypted with K1 , then encrypted with K2,and finally with K3.where K1 ,K2, K3 are all different from each other.

Triple DES with 2 keys – the plain text encrypted with K1 , then encrypted with K2,and finally with K1.where K1 ,K2, are used.

3.7 DIGITAL SIGNATURE

Digital signature:

➢ It is an authentication mechanism that allows the sender to attach an electronic code with the message. This electronic code acts as the signature of the sender and hence, is named digital signature.

➢ It is done to ensure its authenticity and integrity.

➢ Digital signature uses the public-key cryptography technique. The sender uses his or her private key and a signing algorithm to create a digital signature and the signed document can be made public.

The receiver, uses the public key of the sender and a verifying algorithm to verify the digital signature.

➢ A normal message authentication scheme protects the two communicating parties against attacks from a third party (intruder). However, a secure digital signature scheme protects the two parties against each other also.

➢ Suppose A wants to send a signed message (message with A's digital signature) to B through a network. For this, A encrypts the message using his or her private key, which results in a signed message. The signed message is then sent through the network to B.

➢ Now, B attempts to decrypt the received message using A's public key in order to verify that the received message has really come from A.

➢ If the message gets decrypted, B can believe that the message is from A. However, if the message or the digital signature has been modified during transmission, it cannot be decrypted using A's public key. From this, B can conclude that either the message transmission has tampered with, or that the message has not been generated by A.

Message integrity:

➢ Digital signatures also provide message integrity.

➢ If a message has a digital signature, then any change in the message after the signature is attached will invalidate the signature.

➢ That is, it is not possible to get the same signature if the message is changed. Moreover, there is no efficient way to modify a message and its signature such that a new message with a valid signature is produced.

Non-repudiation:

➢ Digital signatures also ensure non-repudiation.

➢ For example, if A has sent a signed message to B, then in future A cannot deny about the sending of the message. B can keep a copy of the message along with A's signature.

➢ In case A denies, B can use A’s public key to generate the original message. If the newly created message is the same as that initially sent by A, it is proved that the message has been sent by A only.

➢ In the same way, B can never create a forged message bearing A's digital signature, because only A can create his or her digital signatures with the help of that private key.

Message confidentiality:

➢ Digital signatures do not provide message confidentiality, because anyone knowing the sender's public key can decrypt the message.

Digital signature process:

The digital signature process is shown in Figure. Suppose user A wants to send a signed message to B through a network. To achieve this communication, these steps are followed:

➢ A uses his private key (EA), applied to a signing algorithm, to sign the message (M).

➢ The message (M) along with A's digital signature (S) is sent to B.

➢ On receiving the message (M) and the signature (S), B uses A's public key (DA), applied to the verifying algorithm, to verify the authenticity of the message. If the message is authentic, B accepts the message, otherwise it is rejected.

Questions on Unit- III

1. What are the algorithm modes?
2. Explain Diffie-Hellman algorithm with example.
3. Explain RSA algorithm with example.
4. What is the difference between symmetric key cryptography and asymmetric key cryptography?
5. Write a short note on digital signature.

UNIT - IV

DIGITAL CERTIFICATE & PUBLIC KEY INFRASTRUCTURE

Digital Certificate

- To solve the man-in-the-middle attack, Digital Certificates were introduced.
- A digital certificate is simply a small computer file. For example, my digital certificate would actually be a computer file with a file name such as name .cer.
- The digital certificate is actually quite similar to a passport. As we know every passport has a unique passport number, similarly every digital certificate has a unique serial number. Also gives information of the issuer's name, serial number, public key, validity period, etc.
- Digital Certificate is issued by a trusted agency called as CA (Certification Authority).
- Another third party called as RA (Registration Authority) acts as a intermediate entity between CA and end user.
- Satisfies the principle of Authentication, non-repudiation.

Who can be a CA?

- CA has to be someone, who everybody trusts. Consequently, the governments in various countries decide who can and who cannot be a CA.
- Usually, a CA is a reputed organization, such as a post office, financial institution, software company, etc. Two of the world's most famous CAs are VeriSign and Entrust.
- Safes crypt Limited is the first Indian CA.
- Thus, a CA has the authority to issue digital certificates to individuals and organizations, who want to use those certificates in asymmetric-key cryptographic applications.

Technical Details of a Digital Certificate

A standard called X.509 defines the structure of a digital certificate. The International Telecommunication Union (ITU) designs this standard. At that time, it was a part of another standard called X.500. The current version of the standard is Version 3, called X.509V3.

Contents of Digital Certificate:

Version: Version of X.509 protocol. Version can be 1,2 or 3

Certificate Serial No.: Contains unique integer which is generated by CA

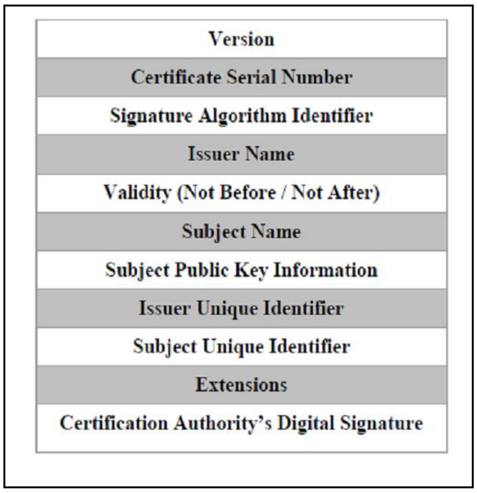
Signature Algorithm Identifier: Identifies the algorithm used by CA to sign the certificate.

Issuer Name: Identifies the Distinguished Name that created & signed the certificate

Validity: (not before/not after) Contains two date-time values. This value generally specifies the date & time up to seconds or milliseconds.

Subject name: Distinguished Name of the end user (user or organization)

Subject Public key info.: This field can never be blank. Contains public key & algorithm related.



Version
Certificate Serial Number
Signature Algorithm Identifier
Issuer Name
Validity (Not Before / Not After)
Subject Name
Subject Public Key Information
Issuer Unique Identifier
Subject Unique Identifier
Extensions
Certification Authority's Digital Signature

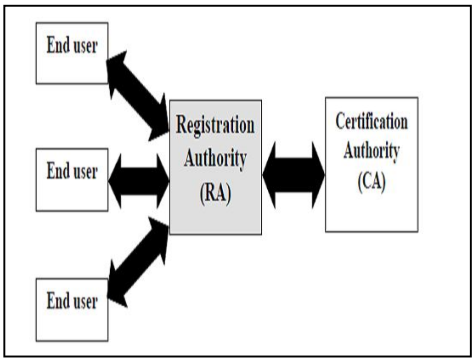
Issuer Unique Identifier: Helps identify a CA uniquely if two or more CAs have used the same Issuer Name over time.
Subject Unique Identifier: Helps identify a subject uniquely if two or more subjects have used the same Subject Name over time.

Digital-Certificate Creation:

1. Parties Involved

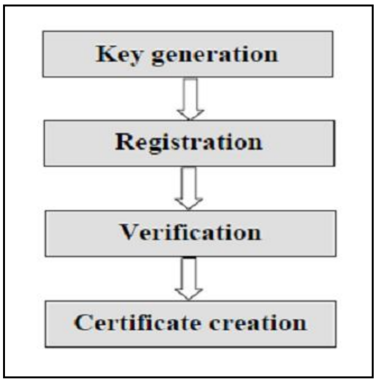
- end user (may be a single user or organization),
- issuer (CA),
- third party is also (optionally) called a Registration Authority (RA), involved in the ertificate creation and management.

The RA commonly provides the following services
Accepting and verifying registration information about new users.
Generating keys on behalf of the end users.
Accepting and authorizing requests for key backups and recovery.
Accepting and authorizing the requests for certificate revocation.
RA is mainly set up for facilitating the interaction between the end users and the CA.
The RA cannot issue digital certificates.
The CA must handle this. Additionally, after a certificate is issued, the CA is responsible for all the certificate management aspects, such as tracking its status, issuing revocation notices if the certificate needs to be invalidated for some reason, etc.



2. Certificate Creation Steps

Step 1: Key Generation:
The action begins with the subject (i.e. the user/organization) who wants to obtain a certificate.
There are two different approaches for this purpose:
Firstly, the subject can create a private key and public key pair using some software.
The subject must keep the private key which is generated, keep it secret. The subject then sends the public key along with other information to the RA.
Secondly, the RA can generate a key pair on-behalf the subject.
This can happen in cases where either the user is not aware of the technicalities involved in the generation of a key pair.
The RA sends the private key which is generated, to the subject. The RA keeps the public key.



Step 2: Registration:
This step is required only if the user generates the key pair in the first step. If the RA generates the key pair on the user's behalf, this step will also be a part of the first step itself.
Assuming that the user has generated the key pair, the user now sends the public key and the associated registration information (e.g. subject name, as it is desired to appear in the digital certificate) and all the required evidence about himself/herself to the RA.

For this, the software provides a wizard in which the user enters all the data then submits it. This data then travels over the network/Internet to the RA. This format for the certificate requests has been is called Certificate Signing Request (CSR). This is one of the Public Key Cryptography Standards (PKCS).

Note that the user must not send the private key to the RA—the user must keep it securely.

Step 3: Verification:

After the registration process is complete, the RA has to verify the user's credentials.

This verification is in two respects, as follows.

1. Firstly, the RA needs to verify the user's credentials which are provided by the user.
    - If the user were actually an organization then the RA would perhaps like to check the business records, historical documents and credibility proofs.
    - If it is an individual user then simpler checks are in call, such as verifying the postal address, email id, phone number, passport or driving-license details can be sufficient.
2. Secondly, check is to ensure that the user who is requesting for the certificate, whether he/she possesses the private key or not corresponding to the public key that is sent to the RA.

This is very important, because there must be a record that the user possesses the private key corresponding to the given public key. Otherwise, this can create legal problems. This check is called the Proof Of Possession (POP) of the private key.

How can the RA perform this check? There are many approaches to this, the chief ones being as follows.

- The RA can demand that the user must digitally sign his/her Certificate Signing Request (CSR) using his/her private key. If the RA can verify the signature (i.e. de-sign the CSR) correctly using the public key of the user, the RA can believe that the user indeed possesses the private key.
- Alternatively, the RA can create a random number challenge; encrypt it with the user's public key and send the encrypted challenge to the user. If the user can successfully decrypt the challenge using his/her private key, the RA can assume that the user possesses the right private key.
- Thirdly, the RA can actually generate a dummy certificate for the user, encrypt it using the user's public key and send it to the user. The user can decrypt it only if he/she can decrypt the encrypted certificate, and obtain the plain-text certificate.

Step 4: Certificate Creation:

Assuming that all the steps so far have been successfully done, and then RA passes on all the details of the user to the CA.

The CA does its own verification (if required) and creates a digital certificate for the user.

The creation of certificate as per the X.509 standard.

The CA sends the certificate to the user, and also retains a copy of the certificate for its own record.

The CA's copy of the certificate is maintained in a certificate directory. This is a central storage location maintained by the CA.

4.2 Private key management

Protecting private key

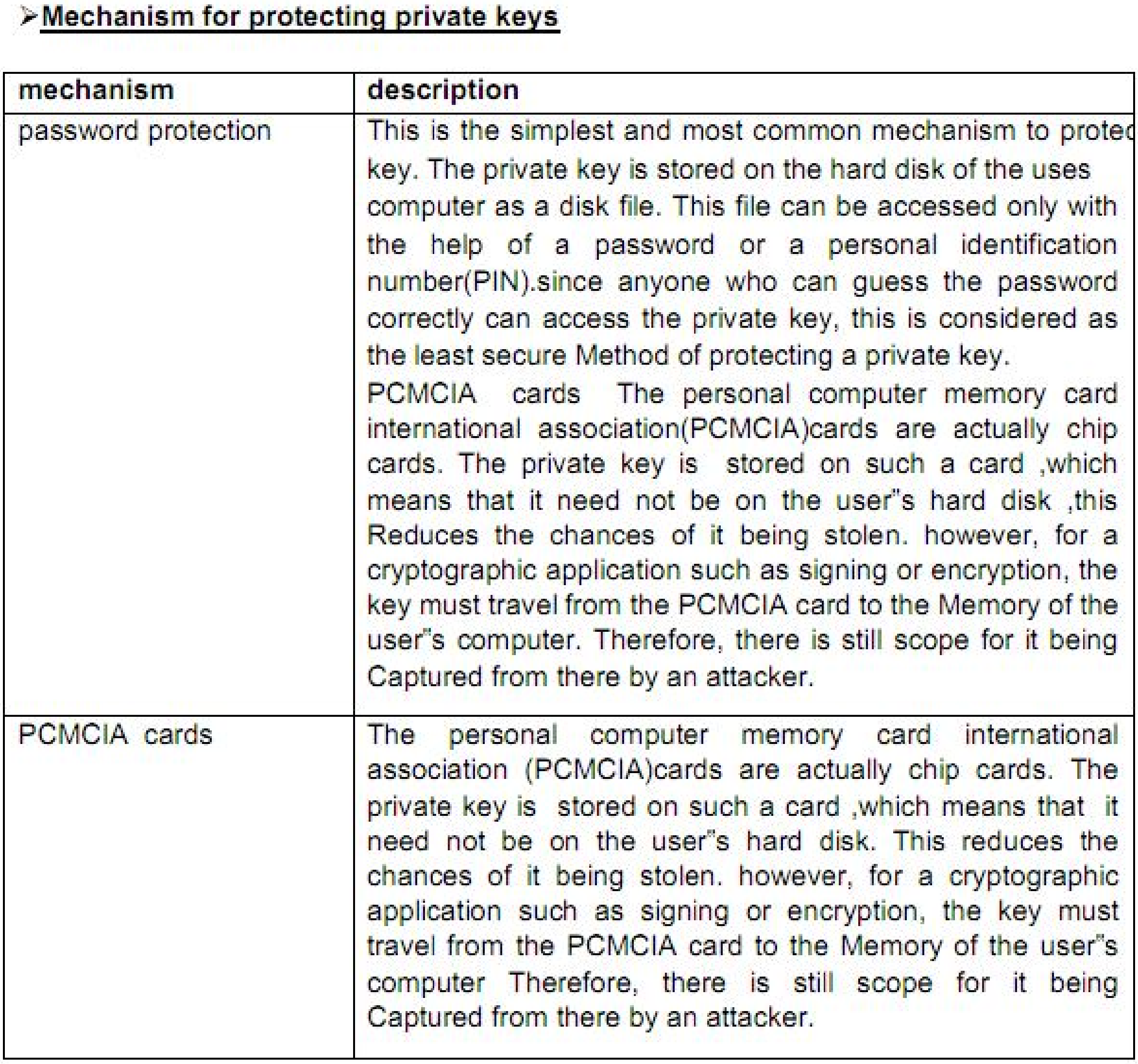
In many situations, the private key of the user might be required to be transported from one location to another. For instance, suppose that the user wants to change her PC. To handle these situations, there is a cryptography standard by the name PKCS#12.This allows a user to export her digital certificate and private key in the form of a computer file.

Obviously, the certificate and the private key must be protected as they are moved to another location. for this ,the PKCS#12 standard ensures that they are encrypted using a symmetric key which is derived from the user's private key protection password.

Multiple key pairs

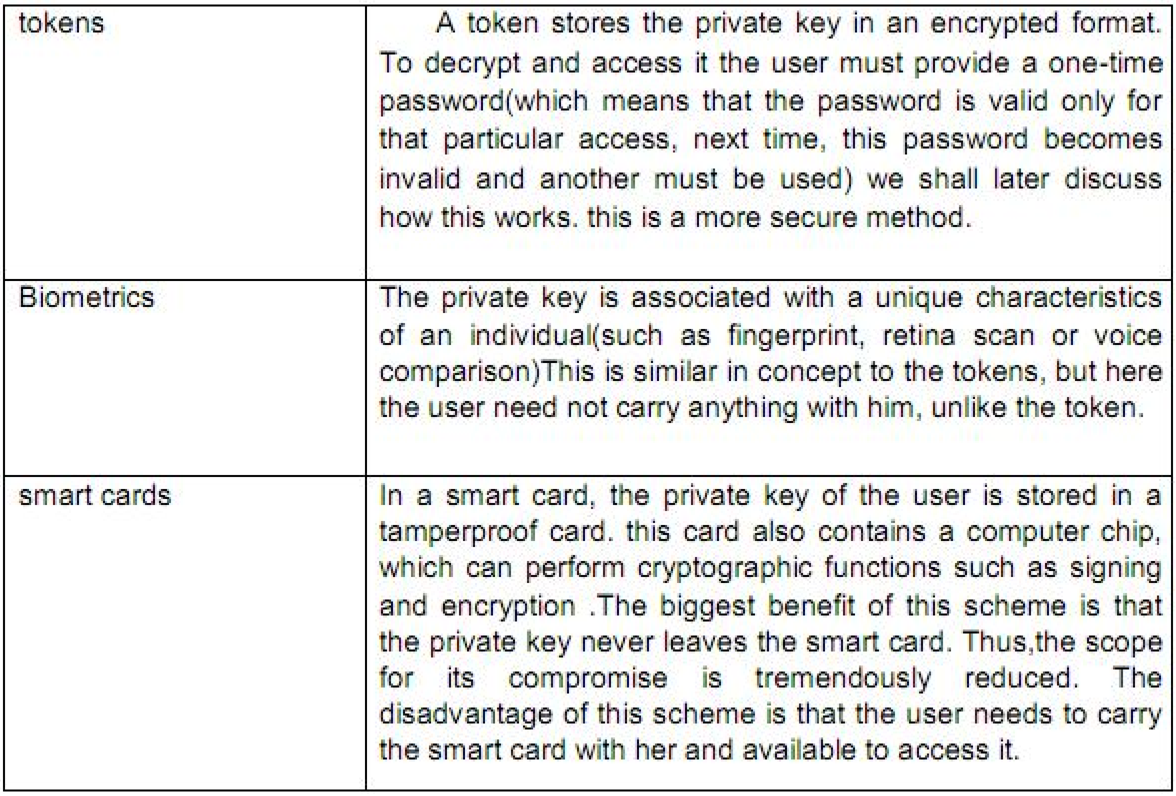
The PKI approach also recommends that in serious business applications, user should posses multiple digital certificates, which also means multiple key pairs. The need for this is that one certificate could be strictly used for signing anther for encryption. This ensures that the loss of one of the private keys does not affect the complete operations of the user. The following guidelines are generally helpful:

The private key that is used for digital signing(non-repudiation)must be backed up or archived after it expires. it must be destroyed. This ensures that it is not used by someone else for signing on behalf of the person at a future date(although chances are that this will be detected by CRL/OCSP checks or certificate expiry date checks, you cannot say this with a 100% guarantee).



➢**Mechanism for protecting private keys**

mechanism	**description**
password protection	This is the simplest and most common mechanism to protec key. The private key is stored on the hard disk of the uses computer as a disk file. This file can be accessed only with the help of a password or a personal identification number(PIN).since anyone who can guess the password correctly can access the private key, this is considered as the least secure Method of protecting a private key. PCMCIA cards The personal computer memory card international association(PCMCIA)cards are actually chip cards. The private key is stored on such a card ,which means that it need not be on the user"s hard disk ,this Reduces the chances of it being stolen. however, for a cryptographic application such as signing or encryption, the key must travel from the PCMCIA card to the Memory of the user"s computer. Therefore, there is still scope for it being Captured from there by an attacker.
PCMCIA cards	The personal computer memory card international association (PCMCIA)cards are actually chip cards. The private key is stored on such a card ,which means that it need not be on the user"s hard disk. This reduces the chances of it being stolen. however, for a cryptographic application such as signing or encryption, the key must travel from the PCMCIA card to the Memory of the user"s computer Therefore, there is still scope for it being Captured from there by an attacker.



tokens	A token stores the private key in an encrypted format. To decrypt and access it the user must provide a one-time password(which means that the password is valid only for that particular access, next time, this password becomes invalid and another must be used) we shall later discuss how this works. this is a more secure method.
Biometrics	The private key is associated with a unique characteristics of an individual(such as fingerprint, retina scan or voice comparison)This is similar in concept to the tokens, but here the user need not carry anything with him, unlike the token.
smart cards	In a smart card, the private key of the user is stored in a tamperproof card. this card also contains a computer chip, which can perform cryptographic functions such as signing and encryption .The biggest benefit of this scheme is that the private key never leaves the smart card. Thus,the scope for its compromise is tremendously reduced. The disadvantage of this scheme is that the user needs to carry the smart card with her and available to access it.

KEY UPDATE

Good security practices demand that the key pairs should be updated periodically. This is because over time, keys become susceptible to analysis attacks. Causing a digital certificate to expire after a certain date ensures this. This requires an update to the key pair. The expiry of a certificate can be dealt with in one of the two following ways:

- The CA reissues a new certificate based on the original key pair (of course, this is not recommended unless there is an all-around confidence in the strength of the original key pair).
- A fresh key pair is generated and the CA issues a new certificate based on that the new pair. The key update process itself can be handled in two ways, as follows:
- In the first approach, the end user has to detect that certificate is about to expire and request the CA to issue a new one.
- In the other approach, the expiry date of the certificate is automatically checked every time it is used and as soon as it is about to expire, its renewal request is sent to the CA. For his, special systems need to be in place.

KEY ARCHIVAL

The CA must plan for and maintain the history of the certificate and the keys of its users. For instance, suppose that someone approaches the CA of Alice, requesting the CA to make Alice's digital certificate available, as was used three years back to sign a legal document for verification purposes. If the CA has not archived the certificates, how can the CA provide this information? This can cause serious legal problems. Therefore, key archival is a very significant aspect of any PKI solution.

4.3 PKIX Model :

Management protocols are the protocols that are required to support on–line interactions between PKI user and management entities. The possible set of functions that can be supported by management protocols is registration of entity, that takes place prior to issuing the certificate . initialisation, for example generation of key–pair.

- certification, the issuance of the certificate .
- key–pair recovery, the ability to recover lost keys .
- key–pair update, when the certificate expires and a new key–pair and certificate have to be generated.
- revocation request, when an authorised person advices the CA to include a specific certificate into the revocation list cross-certification, when two CAs exchange information in order to generate a cross– certificate .

The Certificate Policies and the Certificate Practice Statements are recommendations of documents that will describe the obligations and other rules with regard the usage of the Certificate.

PKIX Architectural Model:

PKIX is working on the following five areas.

Profiles of X.509 v3 Certificate & v2 Certificate Revocation List profiles:

Lists the use of various options while describing extensions of a digital certificate.

Operational Protocol:

Defines the underlying protocols that provide the transport mechanism.

Management Protocol:

Enables exchange of information between the various PKI entities and specifies the structure & details of PKI messages.

Policy outlines:

Defines policies for the creation of Certificate Policies & Certificate Practice Statements.

Timestamp & Data Certification Services:

Both are the trusted third parties that provide services to guarantee the existence of certificate & DCS verifies the correctness of data that it receives.

4.4 Public key cryptography standards

In cryptography, PKCS is a group of public-key cryptography standards devised and published by RSA Security Inc, starting in the early 1990s. The company published the standards to promote the use of the cryptography techniques to which they had patents, such as the RSA algorithm, the Schnorr signature algorithm and several others. Though not industry standards(because the company retained control over them), some of the standards in recent years[when?] have begun to move into the "standards-track" processes of relevant standards organizations such as the IETF and the PKIX working-group.