#132, AECS Layout, IT Park Road, Kundalahalli, Bangalore 560 037
T: +91 80 28524466/77

CMR
INSTITUTE
OF TECHNOLOGY

DEPARTMENT OF INFORMATION SCIENCE & ENGINEERING

INFORMATION AND NETWORK SECURITY
IAT – 2 SOLUTION

1a) Discuss the "man-in-the-middle" attack. [4]

A **man-in-the-middle attack** (MITM, sometimes called a "bucket brigade attack"[1]) is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

Eg: Suppose Alice wishes to communicate with Bob. Meanwhile, Mallory wishes to intercept the conversation to eavesdrop and optionally to deliver a false message to Bob.

First, Alice asks Bob for his public key. If Bob sends his public key to Alice, but Mallory is able to intercept it, a man-in-the-middle attack can begin. Mallory sends a forged message to Alice that purports to come from Bob, but instead includes Mallory's public key.

Alice, believing this public key to be Bob's, encrypts her message with Mallory's key and sends the enciphered message back to Bob. Mallory again intercepts, deciphers the message using her private key, possibly alters it if she wants, and re-enciphers it using the public key Bob originally sent to Alice. When Bob receives the newly enciphered message, he believes it came from Alice.

1. Alice sends a message to Bob, which is intercepted by Mallory:

   Alice *"Hi Bob, it's Alice. Give me your key."* → Mallory Bob

2. Mallory relays this message to Bob; Bob cannot tell it is not really from Alice:

   Alice Mallory *"Hi Bob, it's Alice. Give me your key."* → Bob

3. Bob responds with his encryption key:

   Alice Mallory ← *[Bob's key]* Bob

4. Mallory replaces Bob's key with her own, and relays this to Alice, claiming that it is Bob's key:

   Alice ← *[Mallory's key]* Mallory Bob

5. Alice encrypts a message with what she believes to be Bob's key, thinking that only Bob can read it:

Alice *"Meet me at the bus stop!" [encrypted with Mallory's key]* → Mallory Bob

6. However, because it was actually encrypted with Mallory's key, Mallory can read it, or, modify it (as desired), re-encrypt with Bob's key, and forward it to Bob:

   Alice Mallory *"Meet me at the van down by the river!" [encrypted with Bob's key]* → Bob

7. Bob thinks that this message is a secure communication from Alice.
8. Bob goes to the van down by the river and gets robbed by Mallory.

1b) Explain different categories of attacks on cryptosystems. [6]

Man in Middle Attack (MIM) − The targets of this attack are mostly public key cryptosystems where key exchange is involved before communication takes place.

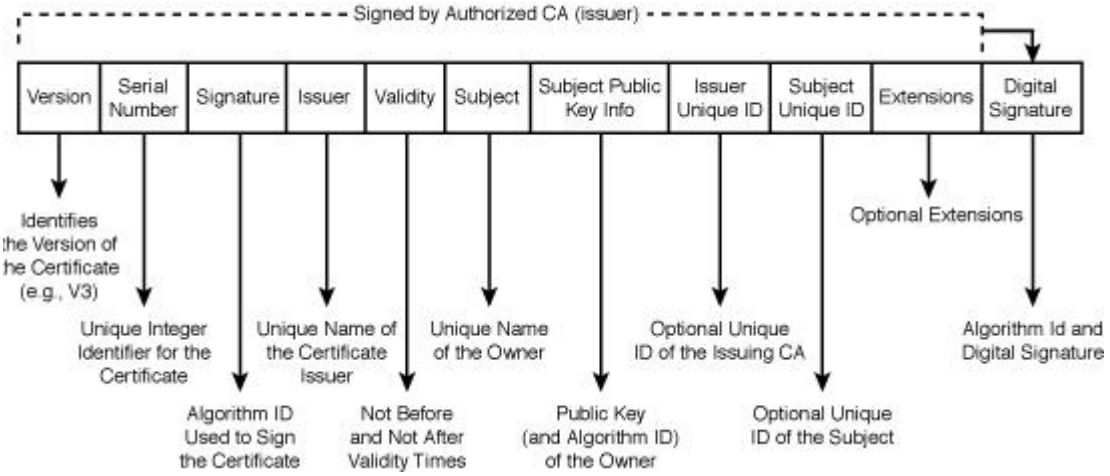
- Host *A* wants to communicate to host *B*, hence requests public key of *B*.
- An attacker intercepts this request and sends his public key instead.
- Thus, whatever host *A* sends to host *B*, the attacker is able to read.
- In order to maintain communication, the attacker re-encrypts the data after reading with his public key and sends to *B*.
- The attacker sends his public key as *A*'s public key so that *B* takes it as if it is taking it from *A*.

Timing Attacks − They exploit the fact that different computations take different times to compute on processor. By measuring such timings, it is be possible to know about a particular computation the processor is carrying out. For example, if the encryption takes a longer time, it indicates that the secret key is long.

Dictionary Attack − This attack has many variants, all of which involve compiling a 'dictionary'. In simplest method of this attack, attacker builds a dictionary of ciphertexts and corresponding plaintexts that he has learnt over a period of time. In future, when an attacker gets the ciphertext, he refers the dictionary to find the corresponding plaintext.

In cryptography, **correlation attacks** are a class of known plaintext attacks for breaking stream ciphers whose keystream is generated by combining the output of several linear feedback shift registers (called LFSRs for the rest of this article) using a Boolean function. Correlation attacks exploit a statistical weakness that arises from a poor choice of the Boolean function – it is possible to select a function which avoids correlation attacks, so this type of cipher is not inherently insecure.

2a) **Explain the general format of a X.509 public key certificate**



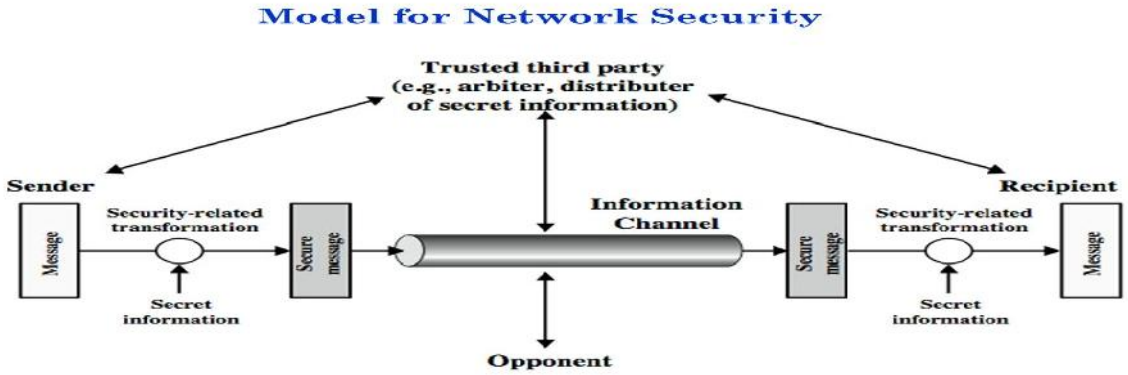
- **Serial Number**: Used to uniquely identify the certificate within a CA's systems. In particular this is used to track revocation information.
- **Subject**: The entity a certificate belongs to: a machine, an individual, or an organization.
- **Issuer**: The entity that verified the information and signed the certificate.
- **Not Before**: The earliest time and date on which the certificate is valid. Usually set to a few hours or days prior to the moment the certificate was issued, to avoid clock skew problems.
- **Not After**: The time and date past which the certificate is no longer valid.
- **Key Usage**: The valid cryptographic uses of the certificate's public key. Common values include digital signature validation, key encipherment, and certificate signing.
- **Extended Key Usage**: The applications in which the certificate may be used. Common values include TLS server authentication, email protection, and code signing.
- **Public Key**: A public key belonging to the certificate subject.
- **Signature Algorithm**: The algorithm used to sign the public key certificate.
- **Signature**: A signature of the certificate body by the issuer's private key.

2b)List difference between Kerberos version 4 and version 5.

Kerberos Version 4	**Kerberos Version 5**	
Chronology	Kerberos v4 was released prior to the version 5 in the late 1980's.	The version 5 was published in 1993, years after the appearance of version 5.
Key salt algorithm	Uses the principal name partially.	Uses the entire principal name.
Encoding	Uses the "receiver-makes-right" encoding system.	Uses the ASN.1 coding system.
Ticket support	Satisfactory	Well extended. Facilitates forwarding, renewing and postdating tickets.

3a) Explain the network security model?

Explanation of the process



A message is to be transferred from one party to another across some sort of int ernet. The two parties, who are theprincipals in this transaction, must cooperate for the exchange to take place. A logical information channel is established by defining a route through the internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals. Security aspects come into play when it is necessary or desirable to p rotect the information transmission from an opponent who may present a threat to confidentiality, authenticity, and so onAll the techniques for providing security have two components: A security-related transformation on the information to be sent. Examples include the encryption of the message, whichscrambles the message so that it is unreadable by the opponent, and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender Some secret information shared by the two principals and, it is hoped, unknown to the opponent. Anexample is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception

.

3b) Explain in detail the types of security attacks? What are the difference between active and passive security attacks?

Active attack-alteration
Passive attack-no alteration

Passive Attacks:

1. Passive attacks are in the nature of eavesdropping on, or monitoring of transmissions.
2. The goal of the opponent is to obtain information that is being transmitted.
3. There are 2 types of passive attacks they are

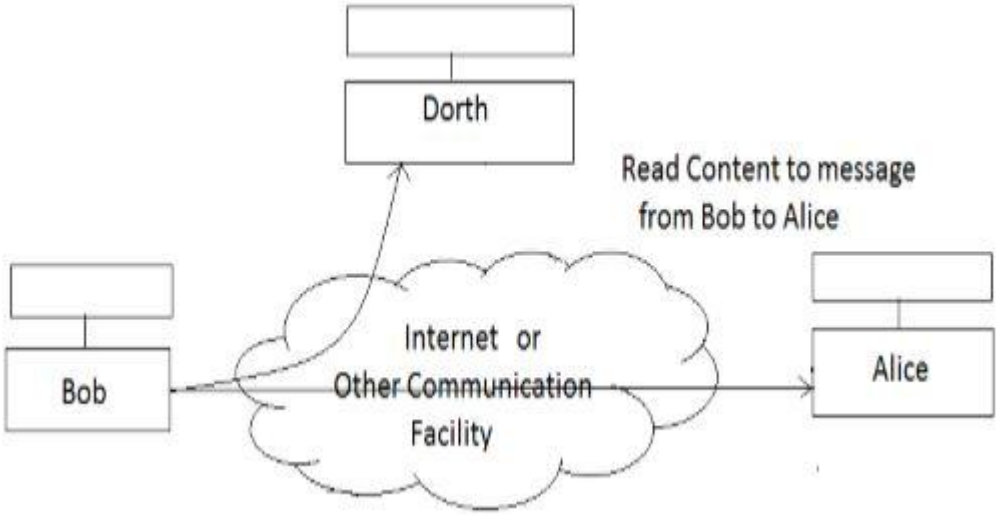


Figure Release of Message Contents

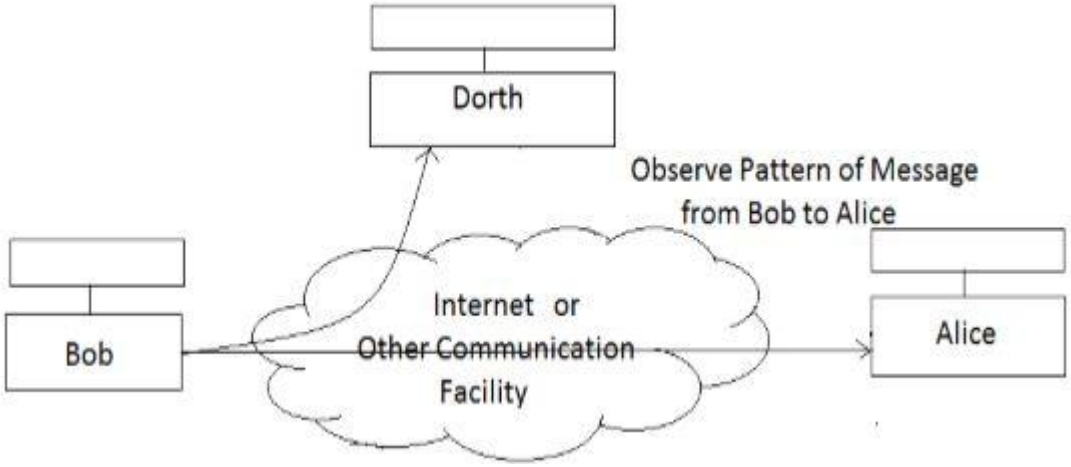


Figure Traffic analysis

- Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message.
- The common technique for masking content is encryption. However if the opponent might still be able to observe the pattern of these messages. The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.

- Passive attacks are very difficult to detect because they do not involve any alteration of the data. Typically, the message traffic is not sent and received in an apparently normal fashion and the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern.
- However, it is feasible to prevent the success of these attacks, usually by means of encryption. Thus the emphasis in dealing with passive attacks is on prevention rather than detection.

Active Attacks:

- Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories:

A. Masquerade: It takes place when one entity pretends to be a different entity.

E.g. Authentication sequences can be captured and replayed after a valid authentication sequences has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by interpersonating an entity that has those privileges.

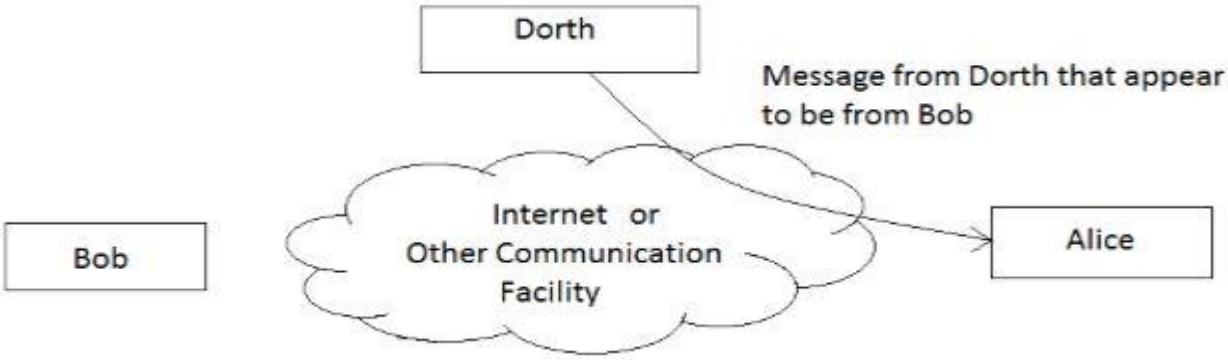


Figure Masquerade

B. Replay: Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

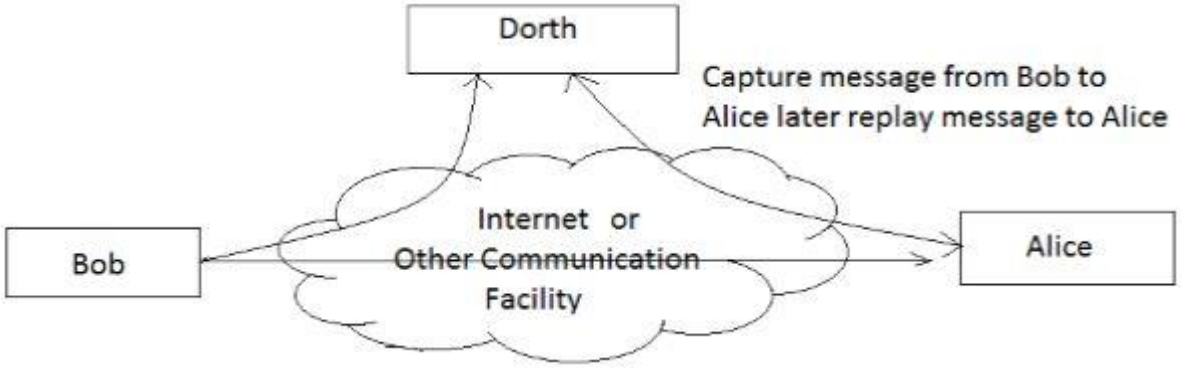


Figure Replay

C. Modification of Messages: The some portion of a legitimate message is altered or that messages are delayed or reordered, to produce an unauthorized effect.

E.g A message meaning "Allow John Smith to read confidential file accounts" is modified to mean "Allow Fred Brown to read the confidential file accounts".

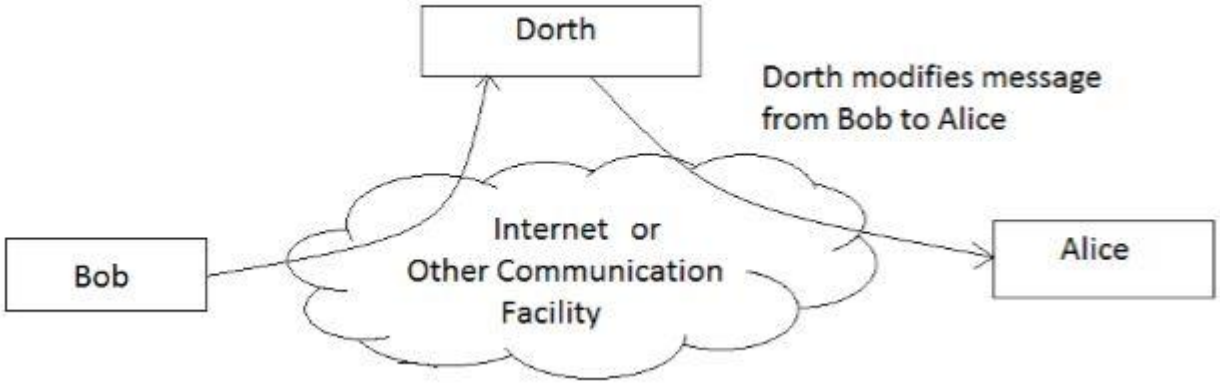


Figure Modification of Messages

D. Denial of Service: It prevents or inhibits the normal use or management of communications facilities. This attack may have a specific target;

Ex. An entity may suppress all messages directed to a particular destination. (e.g The security audit service) Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.

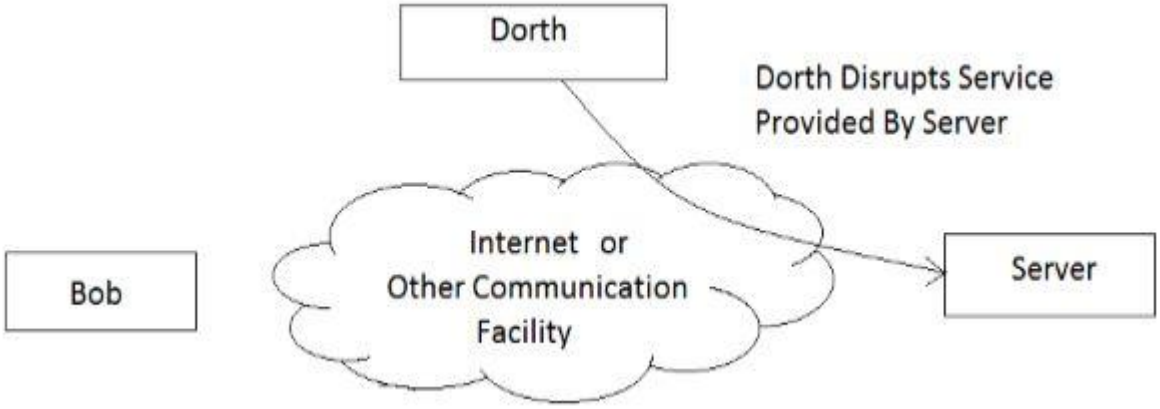


Figure Denial of Service

- Active attacks present the opposite characteristics of passive attacks. Whereas passive attacks are difficult to detect, measures are available to prevent their success.
- On the other hand, it is quite difficult to prevent active attacks absolutely because of the wide variety of potential physical, software and network vulnerabilities.

- Instead, the goal is to detect active attacks and to recover from any disruption or delays caused by them. If the detection has a deterrent effect, it may also contribute to prevention.

4a) Explain Kerberos 4 message exchanges.

(1) C → AS $ID_c \| ID_{tgs} \| TS_1$

(2) AS → C $E(K_c, [K_{c,tgs} \| ID_{tgs} \| TS_2 \| Lifetime_2 \| Ticket_{tgs}])$

$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \| ID_C \| AD_C \| ID_{tgs} \| TS_2 \| Lifetime_2])$

(a) Authentication Service Exchange to obtain ticket-granting ticket

(3) C → TGS $ID_v \| Ticket_{tgs} \| Authenticator_c$

(4) TGS → C $E(K_{c,tgs}, [K_{c,v} \| ID_v \| TS_4 \| Ticket_v])$

$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \| ID_C \| AD_C \| ID_{tgs} \| TS_2 \| Lifetime_2])$

$Ticket_v = E(K_v, [K_{c,v} \| ID_C \| AD_C \| ID_v \| TS_4 \| Lifetime_4])$

$Authenticator_c = E(K_{c,tgs}, [ID_C \| AD_C \| TS_3])$

(b) Ticket-Granting Service Exchange to obtain service-granting ticket

(5) C → V $Ticket_v \| Authenticator_c$

(6) V → C $E(K_{c,v}, [TS_5 + 1])$ (for mutual authentication)

$Ticket_v = E(K_v, [K_{c,v} \| ID_C \| AD_C \| ID_v \| TS_4 \| Lifetime_4])$

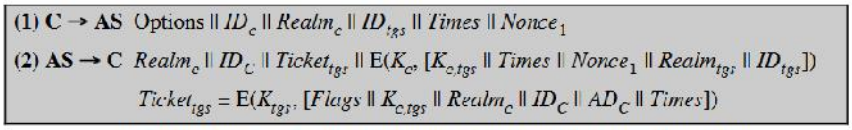
$Authenticator_c = E(K_{c,v}, [ID_C \| AD_C \| TS_5])$

(c) Client/Server Authentication Exchange to obtain service

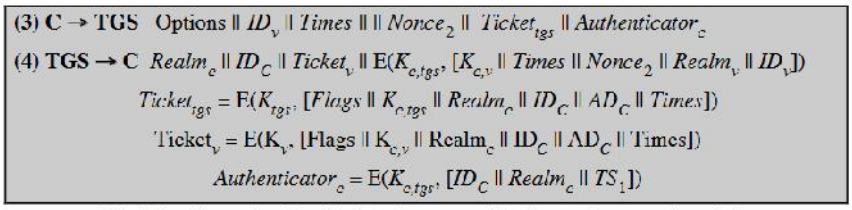
4b) What are the differences between digital signature and digital certificate?

Digital signatures are mainly applied for the verification of authenticity, integrity and non-repudiation. A **digital certificate** is a **certificate** issued by a CA to verify the identity of the **certificate** holder. It actually uses a **digital signature** to attach a public key with a particular individual or an entity.

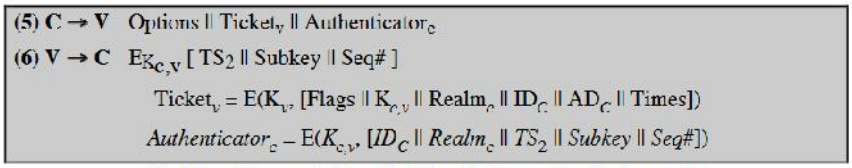
5a) Write the summary of Kerberos version 5 message exchanges?



(a) Authentication Service Exchange to obtain ticket-granting ticket



(b) Ticket-Granting Service Exchange to obtain service-granting ticket



(c) Client/Server Authentication Exchange to obtain service

5b) What is meant by info security? Discuss the 3 aspects of info security.

Def of info security(1)
3 common characteristics of info sec
Availability
Confidentiality
Integrity
Non repudiation
Access control

Information security, sometimes shortened to InfoSec, is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical).

Confidentiality

In information security, confidentiality "is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes" .

Integrity

In information security, data integrity means maintaining and assuring the accuracy and completeness of data over its entire life-cycle.[21] This means that data cannot be modified in an unauthorized or undetected manner. This is not the same thing as referential integrity in databases, although it can be viewed as a special case of consistency as understood in the classic ACID model of transaction processing. Information security systems typically provide message integrity in addition to data confidentiality.

Availability

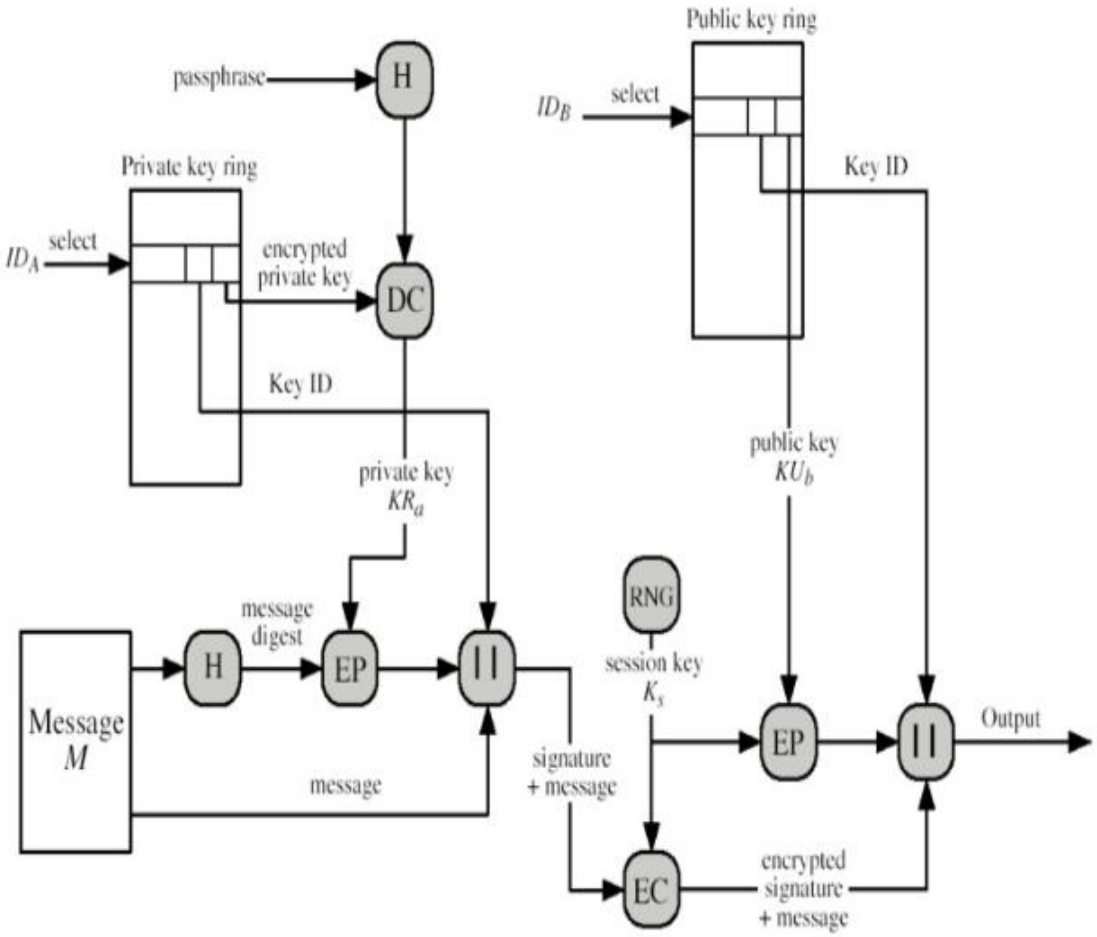
For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the

security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks, such as a flood of incoming messages to the target system essentially forcing it to shut down.[22]

Non-repudiation

In law, non-repudiation implies one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction.

6a)Describe PGP message generation from user A and user B with a block schematic diagram?



With explaination.

6b) What is S/MIME? List its header forms?

S/MIME (**Secure/Multipurpose Internet Mail Extensions**) is a standard for public key encryption and signing of MIME data..

MIME introduces five new headers.

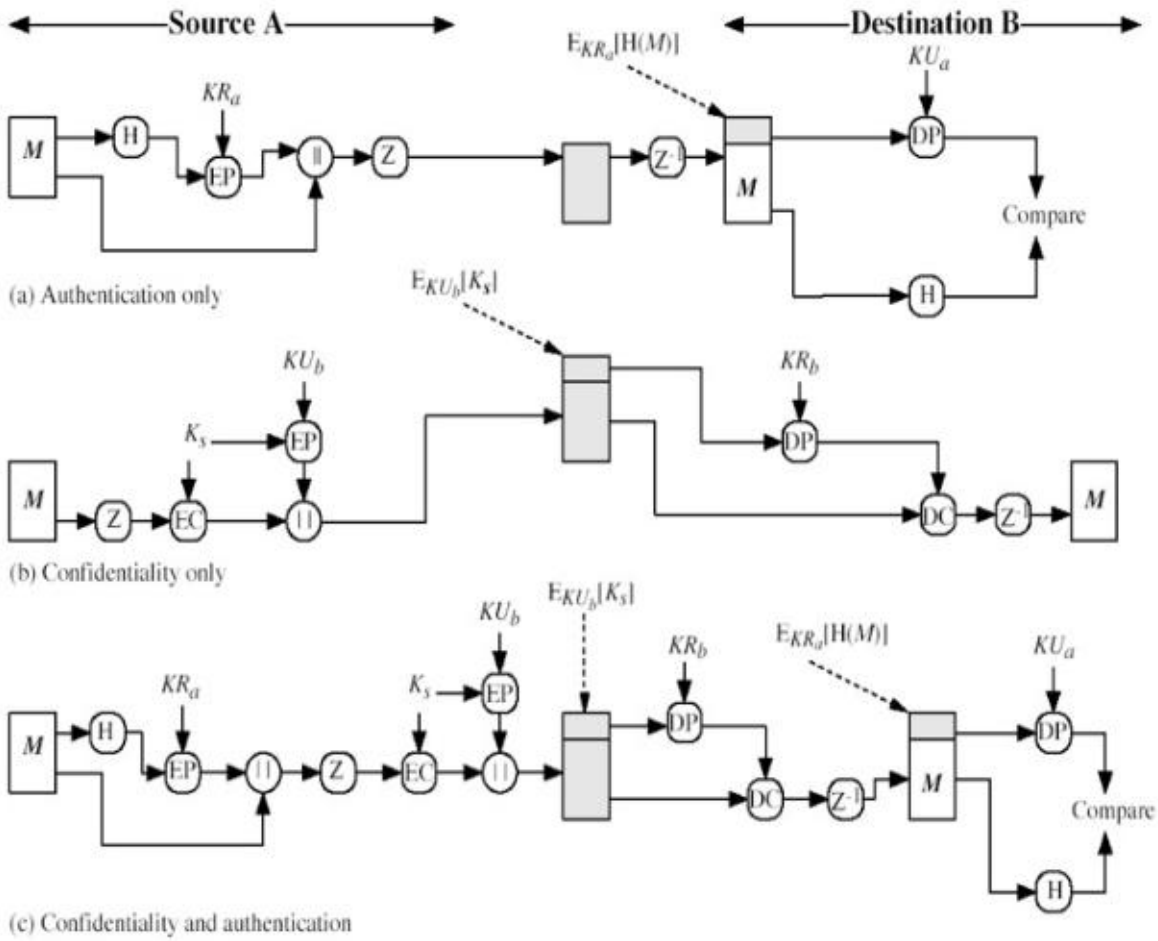
1. MIME-Version: This field must have a parameters value of 1.0 to indicate that the message conforms to RFC 2045 and 2046.
2. Content-Type: Describes the data contained in the body so that the receiver can pick the appropriate application to represent the data to the user.
3. Content-Transfer-Encoding: Indicates the type of transformation that has been used to represent the body of the message in order to render it amenable to the mail tranport.
4. Content-ID: Used to identify MIME entities.
5. Content-Description: A text description of the object within the body, e.g. audio-data.

7 What are the five principal services provided by PGP? Explain the operational description of PGP?

PGP consists of the following five services:

1.Authentication
2.Confidentiality
3.Compression
4.E-mail compatibility
5.Segmentation

Authentication,confidentiality

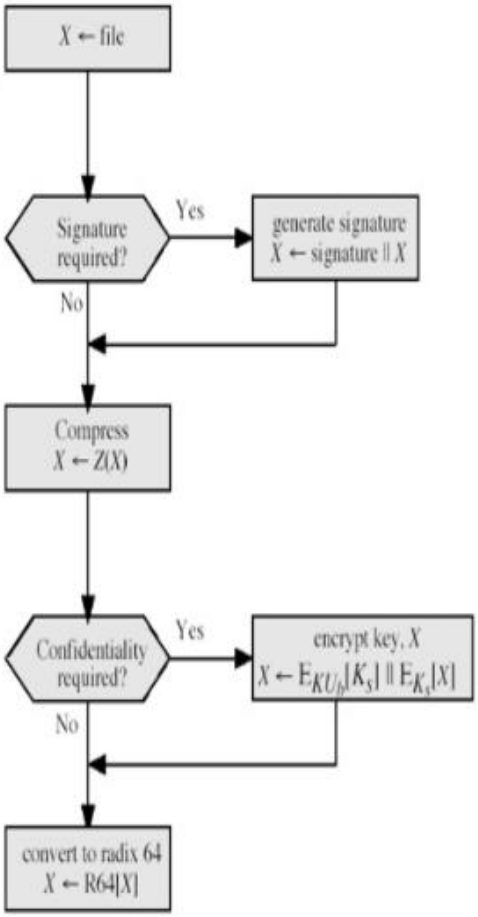


Compression

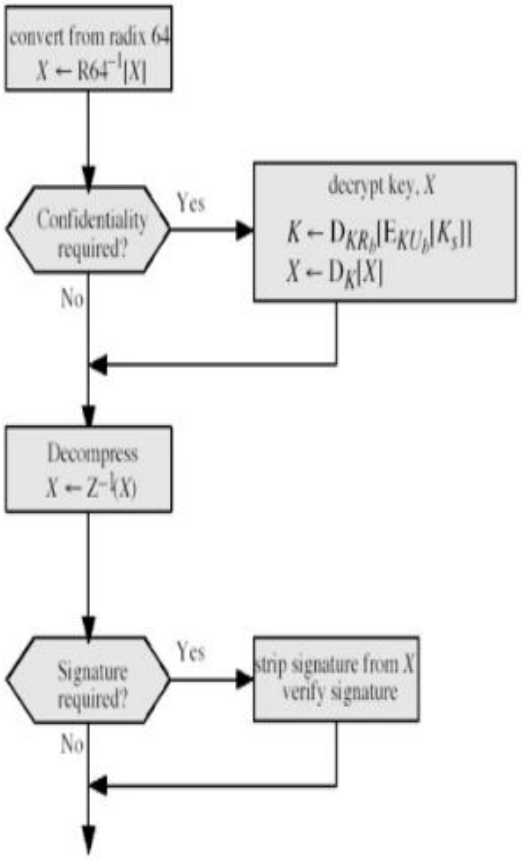
As a default, PGP compresses the message after applying the signature but before encryption. This has the benefit of saving space both for e-mail transmission and for file storage.

E-mail compatibility

Many electronic mail systems only permit the use of blocks consisting of ASCII text.When PGP is used, at least part of the block to be transmitted is encrypted. This ba-sically produces a sequence of arbitrary binary words which some mail systems won’taccept. To accommodate this restriction PGP uses and algorithm known asradix64which maps 6 bits of a binary data into and 8 bit ASCII character.



(a) Generic Transmission Diagram (from A)



(b) Generic Reception Diagram (to B)

Function	Algorithms Used	Description
Digital signature	DSS/SHA or RSA/SHA	A hash code of a message is created using SHA-1. This message digest is encrypted using DSS or RSA with the sender's private key and included with the message.
Message encryption	CAST or IDEA or Three-key Triple DES with Diffie-Hellman or RSA	A message is encrypted using CAST-128 or IDEA or 3DES with a one-time session key generated by the sender. The session key is encrypted using Diffie-Hellman or RSA with the recipient's public key and included with the message.
Compression	ZIP	A message may be compressed, for storage or transmission, using ZIP.
Email compatibility	Radix 64 conversion	To provide transparency for email applications, an encrypted message may be converted to an ASCII string using radix 64 conversion.
Segmentation	—	To accommodate maximum message size limitations, PGP performs segmentation and reassembly.