USN | | | | | | | | | | |

Internal Assesment Test II –April. 2018(Scheme and Solution)

Sub:	INFORMATION AND NETWORK SECURITY			Sub Code:	10CS835	Branch :	CSE	
Date:	17 / 04 / 2018	Duration :	90 mins	Max Marks:	50	Sem / Sec:	8 (A,B,C)	OBE

Answer Any FIVE FULL Questions

		MARKS	CO	RBT
1 (a)	What are the five principal services provided by PGP? Explain the operational description of PGP?	[10]	CO5,6	L1.L3

Operational Description

The actual operation of PGP, as opposed to the management of keys, consists of four services: **authentication, confidentiality, compression, and e-mail compatibility**

.

AUTHENTICATION

Figure 7.1a illustrates the digital signature service provided by PGP

1. The sender creates a message.
2. SHA-1 is used to generate a 160-bit hash code of the message.
3. The hash code is encrypted with RSA using the sender's private key, and the result is prepended to the message.
4. The receiver uses RSA with the sender's public key to decrypt and recover the hash code.
5. The receiver generates a new hash code for the message and compares it with the decrypted hash code. If the two match, the message is accepted as authentic.

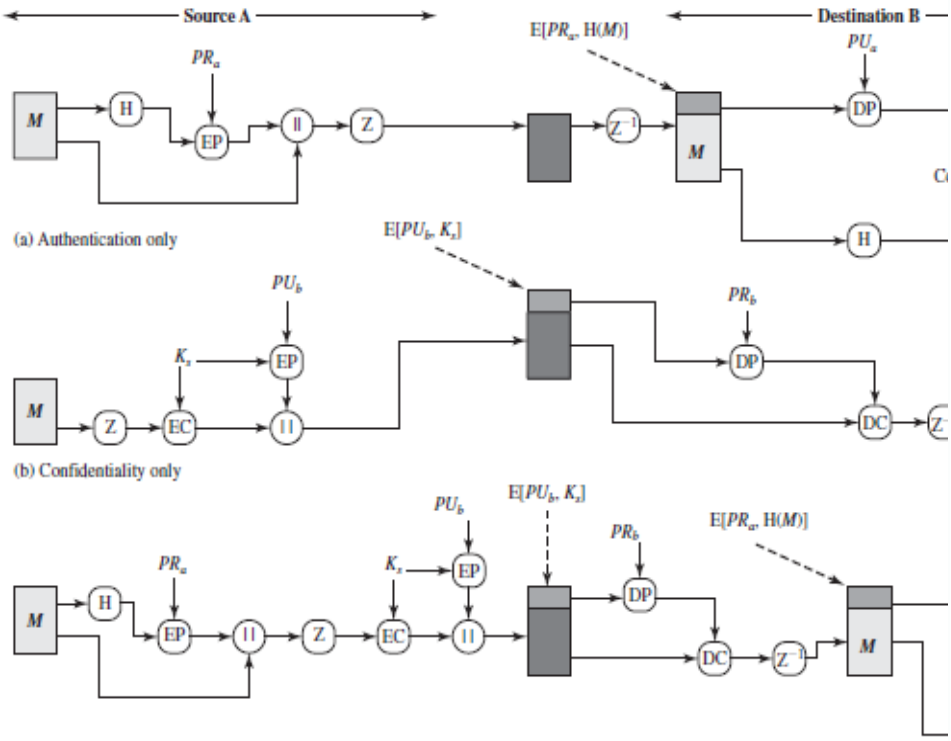


Figure 7.1 PGP Cryptographic Functions

CONFIDENTIALITY

Another basic service provided by PGP is confidentiality, which is provided by encrypting messages to be transmitted or to be stored locally as files. In both cases, the symmetric encryption algorithm CAST-128 may be used. Alternatively, IDEA or 3DES may be used.fig(7.1 b)

1. The sender generates a message and a random 128-bit number to be used as a session key for this message only.
2. The message is encrypted using CAST-128 (or IDEA or 3DES) with the session key.
3. The session key is encrypted with RSA using the recipient's public key and is prepended to the message.
4. The receiver uses RSA with its private key to decrypt and recover the session key.
5. The session key is used to decrypt the message.

CONFIDENTIALITY AND AUTHENTICATION

As Figure 7.1c illustrates, both services may be used for the same message. First, a signature is generated for the plaintext message and prepended to the message.Then the plaintext message plus signature is encrypted using CAST-128 (or IDEA or 3DES), and the session key is encrypted using RSA (or ElGamal). This sequence is preferable to the opposite: encrypting the message and then generating a signature for the encrypted message. It is generally more convenient to store a signature with a plaintext version of a message. Furthermore, for purposes of third-party verification, if the signature is performed first, a third party need not be concerned with the symmetric key when verifying the signature.

In summary, when both services are used, the sender first signs the message with its own private key, then encrypts the message with a session key, and finally encrypts the session key with the recipient's public key.

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. The placement of the compression algorithm, indicated by Z for compression and Z^{-1} for decompression in Figure 7.1, is critical.

1. The signature is generated before compression for two reasons:

a. It is preferable to sign an uncompressed message so that one can store only the uncompressed message together with the signature for future verification. mIf one signed a compressed document, then it would be necessary either to store a compressed version of the message for later verification or to recompress the message when verification is required.

b. Even if one were willing to generate dynamically a recompressed message for verification, PGP's compression algorithm presents a difficulty.The algorithm is not deterministic; various implementations of the algorithm achieve different tradeoffs in running speed versus compression ratio and, as a result, produce different compressed forms. However, these different compression algorithms are interoperable because any version of the algorithm can correctly decompress the output of any other version.

2. Message encryption is applied after compression to strengthen cryptographic security. Because the compressed message has less redundancy than the original plaintext, cryptanalysis is more difficult.

E-MAIL COMPATIBILITY

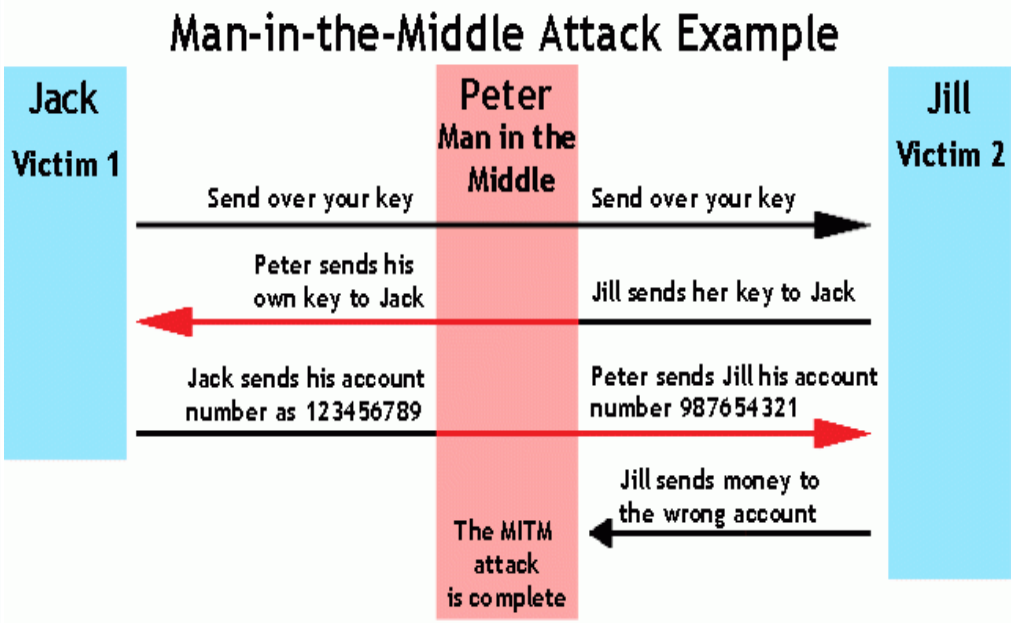
When PGP is used, at least part of the block to be transmitted is encrypted. If only the signature service is used, then the message digest is encrypted (with the sender's private key). If the confidentiality service is used, the message plus signature (if present) are encrypted (with a one-time symmetric key).
Thus, part or all of the resulting block consists of a stream of arbitrary 8-bit octets. However, many electronic mail systems only permit the use of blocks consisting of ASCII text.To accommodate this restriction, PGP provides the service of converting the raw 8-bit binary stream to a stream of printable ASCII characters. The scheme used for this purpose is radix-64 conversion. Each group of three octets of binary data is mapped into four ASCII characters. This format also appends a CRC to detect

transmission errors.

2 (a) Explain Man In the Middle Attack? [4] CO5 L3

MAN-IN-THE-MIDDLE ATTACK

A **man-in-the-middle attack**, attempts to intercept a public key or even to insert a known key structure in place of the requested public key. Thus, attackers attempt to place themselves between the sender and receiver, and once they've intercepted the request for key exchanges, they send each participant a valid public key, which is known
only to them. To the victims of such attacks, encrypted communication appears to be occurring normally, but in fact the attacker is receiving each encrypted message and decoding it (with the key given to the sending party), and then encrypting and sending it to the intended recipient. Establishing public keys with digital signatures can prevent the traditional manin- the-middle attack, as the attacker cannot duplicate the signatures.



(b) Explain different cryptography tools? [6] CO5 L3

Public-key Infrastructure

Public-key Infrastructure (PKI) is an integrated system of software, encryption methodologies, protocols, legal agreements, and third-party services that enables users to communicate securely. PKI systems are based on public-key cryptosystems and include digital certificates and certificate authorities (CAs).
A **certificate authority (CA)**, which issues, manages, authenticates, signs, and revokes users' digital certificates, which typically contain the user name, public key, and other identifying information.

A **registration authority (RA)**, which operates under the trusted collaboration of the certificate authority and can handle day-to-day certification functions, such as verifying registration information, generating end-user keys, revoking certificates, and validating user certificates.
Certificate directories, which are central locations for certificate storage that provide a single access point for administration and distribution. Management protocols, which organize and manage the communications among CAs, RAs, and end users. This includes the functions and procedures for setting up new users, issuing keys, recovering keys, updating keys, revoking keys, and

enabling the transfer of certificates and status information among the parties involved in the PKI's area of authority. Policies and procedures, which assist an organization in the application and management of certificates, in the formalization of legal liabilities and limitations, and in actual business use.

DIGITAL SIGNATURE

Digital signatures were created in response to the rising need to verify information transferred via electronic systems. Asymmetric encryption processes are used to create digital signatures. When an asymmetric cryptographic process uses the sender's private key to encrypt a message, the sender's public key must be used to decrypt the message. When the decryption is successful, the process verifies that the message was sent by the sender and thus cannot be refuted. This process is known as **nonrepudiation** and is the principle of cryptography that underpins the authentication mechanism collectively known as a digital signature. **Digital signatures** are, therefore, encrypted messages that can be mathematically proven authentic.

DIGITAL CERTIFICATE

A digital certificate is an electronic document or container file that contains a key value and identifying information about the entity that controls the key. The certificate is often issued and certified by a third party, usually a certificate authority. A digital signature attached to the certificate's container file certifies the file's origin and integrity. This verification process often occurs when you download or update software via the Internet

STEGANOGRAPHY

The word **steganography**—the art of secret writing—is derived from the Greek words *steganos*, meaning "covered" and *graphein*, meaning "to write." While steganography is technically not a form of cryptography, it is another way of protecting the confidentiality of information in transit. The most popular modern version of steganography involves hiding information within files that contain digital pictures or other images

3 (a) Define the term 'Attack'. What are the different types of attacks? Explain in brief. [8] CO5 L1,L2

SECURITY ATTACKS

Classified as -

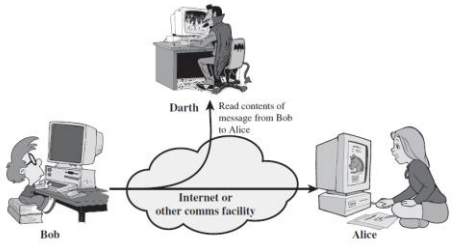
- A passive attack attempts to learn or make use of information from the system but does not affect system resources.
- An active attack attempts to alter system resources or affect their operation.

Passive Attacks

- Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions.
- The goal of the opponent is to obtain information that is being transmitted.
- Two types of passive attacks are the release of message contents and

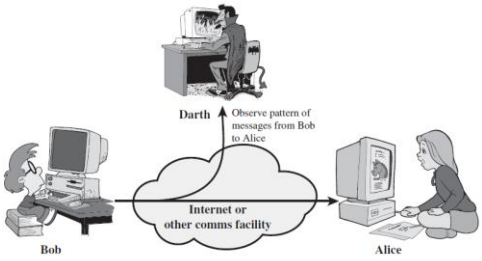
traffic analysis.

- **Release of message contents →** A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.



(a) Release of message contents

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 contents is encryption. If we had encryption protection in place, an opponent still might 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.

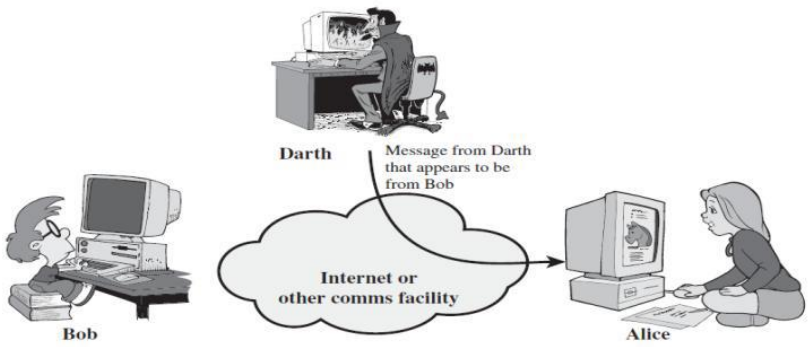


(b) Traffic analysis

Active Attacks

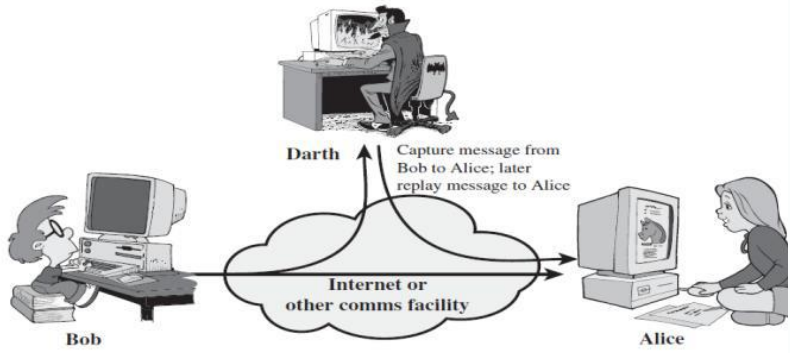
- Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service.
- A **masquerade** takes place when one entity pretends to be a different entity (Figure 1.3a). A masquerade attack usually includes one of the other forms of active attack.

- 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.
  -



(a) Masquerade

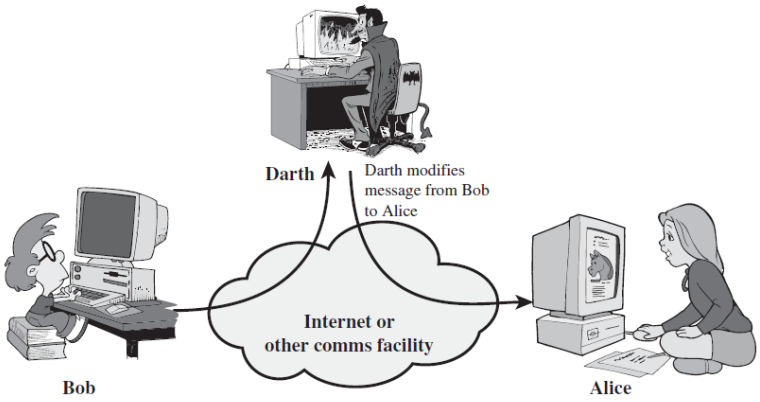
- **Replay** involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect (Figure 1.3b).



(b) Replay

- **Modification of messages** simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect (Figure 1.3c).

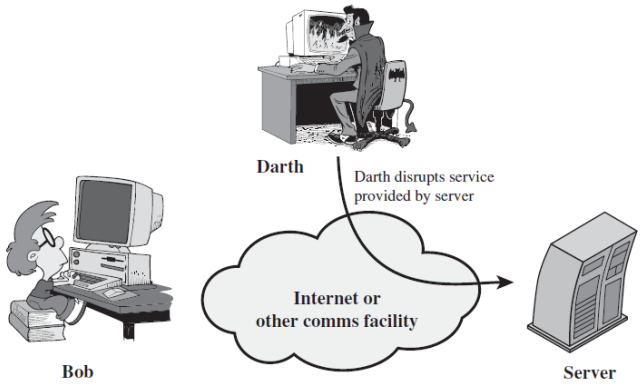
- E.g A message meaning "Allow John Smith to read confidential file accounts" is modified to mean "Allow Fred Brown to read the confidential file accounts".



(c) Modification of messages

- The **denial of service** prevents or inhibits the normal use or management of communications facilities (Figure 1.3d). This attack may have a specific target. 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.
- 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



(d) Denial of service

(b) What is S/MIME? List its header forms? [2] CO6 L1

Secure/Multipurpose Internet Mail Extension (S/MIME) is a security enhancement to the MIME Internet
e-mail format standard based on technology from RSA Data Security. Although both PGP and S/MIME are on an IETF standards track, it appears likely that S/MIME will emerge as the industry standard for commercial and organizational use, while PGP will remain the choice for personal e-mail security for
many users. S/MIME is defined in a number of documents—most importantly RFCs 3370, 3850, 3851, and 3852.

MIME-Version: Must have the parameter value 1.0. This field indicates that the message conforms to RFCs 2045 and 2046.

- **Content-Type:** Describes the data contained in the body with sufficient detail that the receiving user agent can pick an appropriate agent or mechanism to represent the data to the user or otherwise deal with the data in an appropriate manner.
- **Content-Transfer-Encoding:** Indicates the type of transformation that has been used to represent the body of the message in a way that is acceptable for mail transport.
- **Content-ID:** Used to identify MIME entities uniquely in multiple contexts.
- **Content-Description:** A text description of the object with the body; this is useful when the object is not readable (e.g., audio data). Any or all of these fields may appear in a normal RFC 5322 header

4 (a) Describe PGP message generation from user A and user B with a block schematic diagram? [10] CO6 L2

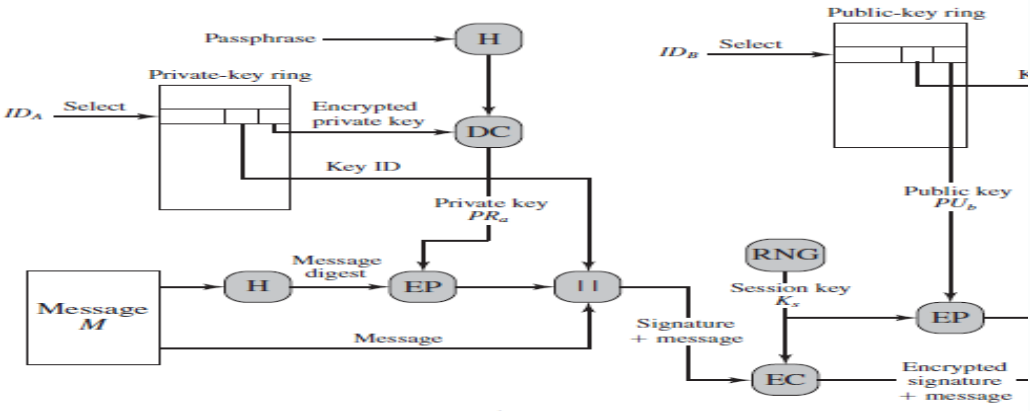


Figure 7.5 PGP Message Generation (from User A to User B: no compression or conversion)

1. Signing the message:

a. PGP retrieves the sender's private key from the private-key ring using

`your_userid` as an index. If `your_userid` was not provided in the command, the first private key on the ring is retrieved.
b. PGP prompts the user for the passphrase to recover the unencrypted private key.
c. The signature component of the message is constructed.

2.Encrypting the message:

a. PGP generates a session key and encrypts the message.
b. PGP retrieves the recipient's public key from the public-key ring using `her_userid` as an index.
c. The session key component of the message is constructed.

The receiving PGP entity performs the following steps (Figure 7.6)
.
1. Decrypting the message:
a. PGP retrieves the receiver's private key from the private-key ring using the Key ID field in the session key component of the message as an index.
b. PGP prompts the user for the passphrase to recover the unencrypted private key.
c. PGP then recovers the session key and decrypts the message.
2. Authenticating the message:

a. PGP retrieves the sender's public key from the public-key ring using the Key ID field in the signature key component of the message as an index.
b. PGP recovers the transmitted message digest.
c. PGP computes the message digest for the received message and compares it to the transmitted message digest to authenticate.

5 (a) Explain KERBEROS V4 dialogue. Differentiate between KERBEROS V4 and V5 authentication dialogues? [10] CO4 L2.L3

1. The client requests a ticket-granting ticket on behalf of the user by sending its user's ID to the AS, together with the TGS ID, indicating a request to use the TGS service.
2. The AS responds with a ticket that is encrypted with a key that is derived from the user's password (K_C). If the correct password is supplied, the ticket is successfully recovered.
3. The client requests a service-granting ticket on behalf of the user
. **4.** The TGS decrypts the incoming ticket using a key shared only by the AS and the TGS (K_{tgs}) and verifies the success of the decryption by the presence of its ID.

1. The client requests access to a service on behalf of the user.

First, we would like to minimize the number of times that a user has to enter a password.

✓ The second problem is that the earlier scenario involved a plaintext transmission of the password. An eavesdropper could capture the password and use any service accessible to the victim.
✓ To solve these additional problems, we introduce a scheme for avoiding plaintext passwords and a new server, known as the **ticket-granting server (TGS)**.
✓ The new (but still hypothetical) scenario is shown above table
✓ Figure 4.1 gives just an overview of kerbero

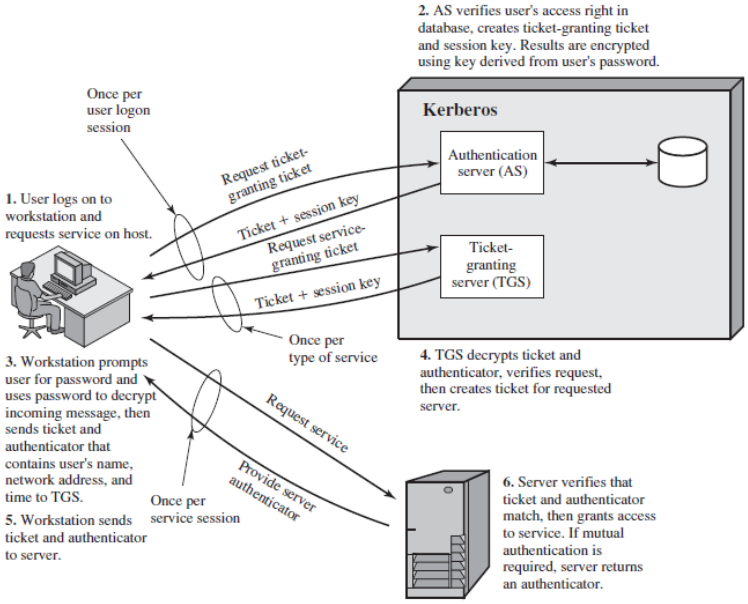


Figure 4.1 Overview of Kerberos

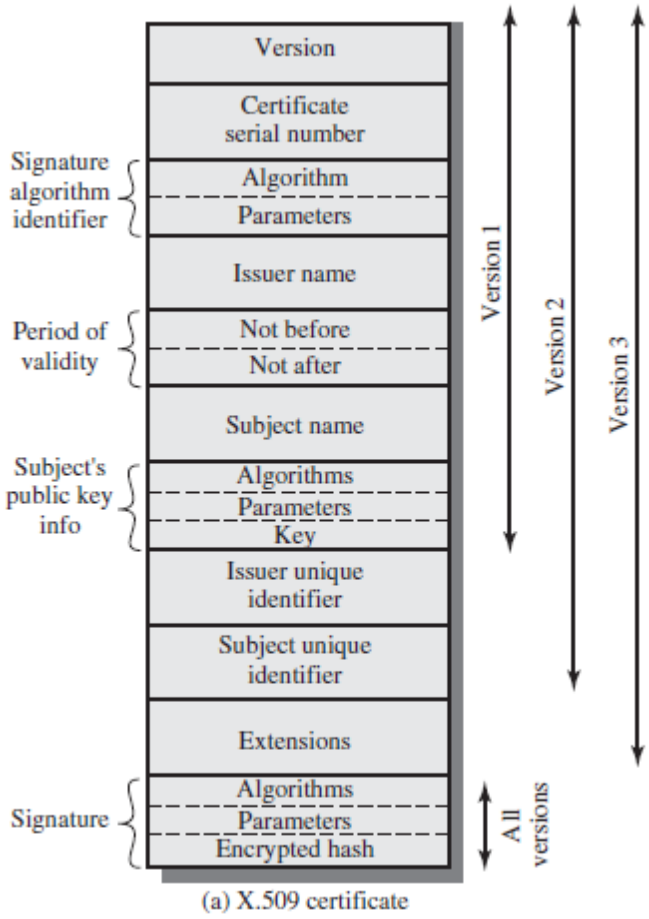
1. Encryption system dependence: Version 4 requires the use of DES. In version 5, cipher text is tagged with an encryption-type identifier so that any encryption technique may be used.
2. Internet protocol dependence: Version 4 requires the use of Internet Protocol (IP) addresses. Other address types, such as the ISO network address, are not accommodated. Version 5 network addresses are tagged with type and length, allowing any network addresses type to be used.
3. Message byte ordering: In version 4, the sender of a message employs a byte ordering of its own choosing and tags the message to indicate least significant byte in lowest address or most significant

byte in lowest address. In version 5, all message structures are defined using Abstract Syntax Notation One (ASN.1) and Basic Encoding Rules (BER), which provide an unambiguous byte ordering.
4. Ticket lifetime: Lifetime values in version 4 are encoded in an 8-bit quantity in units of five minutes. In version 5, tickets include an explicit start time and end time, allowing tickets with arbitrary lifetimes.
5. Authentication forwarding: Version 4 does not allow credentials issued to one client to be forwarded to some other host and used by some other client. Version 5 provides this capability.
6. Inter-realm authentication: In version 4, interoperability among *N* realms requires on the order of *N*2 Kerberos-to-Kerberos relationships. Version 5 supports a method that requires fewer relationships.
Deficiencies of version 4
1. ***Double encryption*** → that tickets provided to clients are encrypted twice—once with the secret key of the target server and then again with a secret key known to the client. The second encryption is not necessary and is computationally wasteful.
2. ***PCBC encryption*** → Encryption in version 4 makes use of a nonstandard mode of DES known as propagating cipher block chaining (PCBC). It has been demonstrated that this mode is vulnerable to an attack involving the interchange of ciphertext blocks
. 3. ***Session keys*** → Each ticket includes a session key that is used by the client to encrypt the authenticator sent to the service associated with that ticket. However, because the same ticket may be used repeatedly to gain

service from a particular server, there is the risk that an opponent will replay messages from an old session to the client or the server.

4. ***Password attacks*** → Both versions are vulnerable to a password attack. The message from the AS to the client includes material encrypted with a key based on the client's password. An opponent can capture this message and attempt to decrypt it by trying various passwords.

6 (a) With a neat diagram, explain X.509 digital certificate format. What are the authentication procedures used in X.509? [7] CO4 L1,L3



(a) X.509 certificate

Figure 4.4 X.509 Formats

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.

(b) What are the differences between active and passive security attacks? [3] CO5 L2

	Passive Attacks	Active attacks
	It is indirect attack	It is direct attack
	Very difficult to detect because they do not involve any alteration of data	Comparatively not very difficult to detect
	Measures are available to prevent their success, usually by means of encryption	Quite difficult to prevent absolutely because it requires physical protection of all communication facilities and paths at all times
	Involves eavesdropping on, or monitoring of, transmissions	Involve some modification of the data stream or the creation of a false stream
	Two types → release of message contents and traffic analysis	Four categories → masquerade, replay, modification of messages and denial of service
	Goal → prevention rather than detection	Goal → detect and recover from any disruption or delays caused by them

7 (a) Explain the network security model. List and Explain the X.800 standard Security Mechanisms? [5+5] CO5 L1,L2

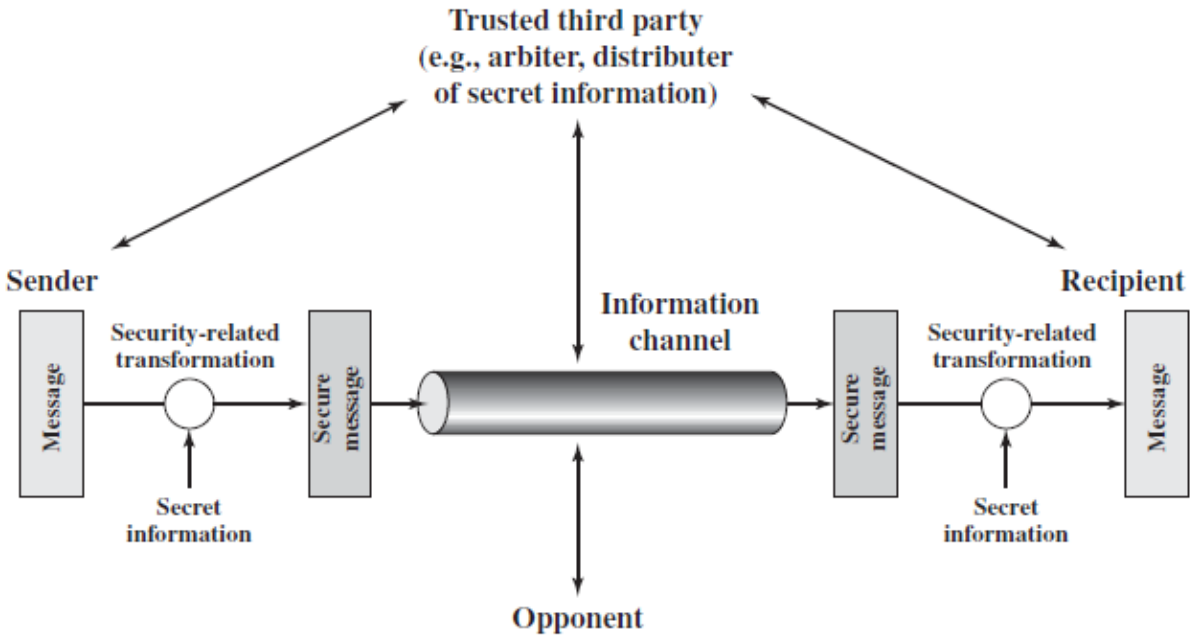


Figure 1.4 Model for Network Security

A MODEL FOR NETWORK SECURITY

- A message is to be transferred from one party to another across some sort of Internet service.
- The two parties, who are the *principals* 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.
- All of the techniques for providing security have two components:

- A security-related transformation on the information to be sent. Some secret information shared by the two principals and, it is hoped, unknown to the opponent.
- A trusted third party may be needed to achieve secure transmission.
- This general model shows that there are four basic tasks in designing a particular security service:
- Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.
- Generate the secret information to be used with the algorithm.
- Develop methods for the distribution and sharing of the secret information.
- Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.
- A general model of these other situations is illustrated by Figure 1.5, which reflects a concern for protecting an information system from unwanted access.
- The hacker can be someone who, with no malign intent, simply gets satisfaction from breaking and entering a computer system.
- The intruder can be a disgruntled employee who wishes to do damage or a criminal who seeks to exploit computer assets for financial gain (e.g., obtaining credit card numbers or performing illegal money transfers).

Programs can present two kinds of threats:

1. **Information access threats:** Intercept or modify data on behalf of users who should not have access to that data
2. . **Service threats:** Exploit service flaws in computers to inhibit use by legitimate users.

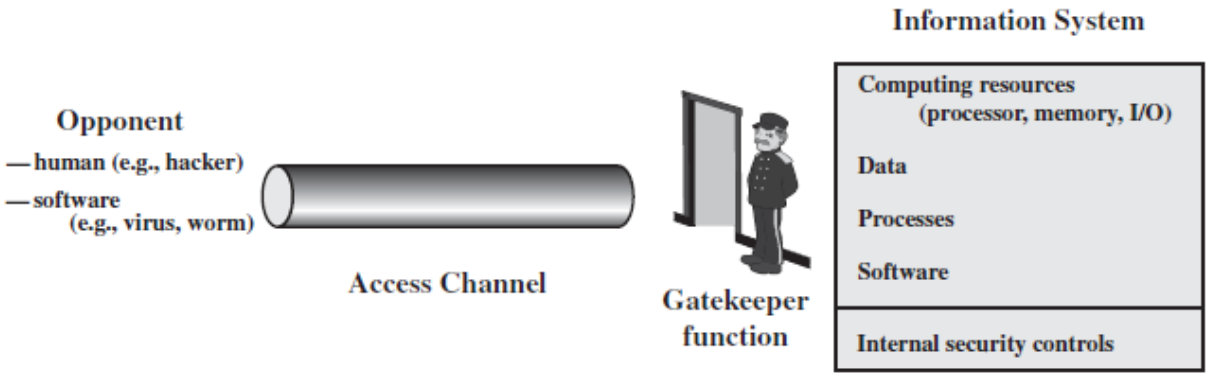


Figure 1.5 Network Access Security Model

Table 1.3 Security Mechanisms (X.800)

SPECIFIC SECURITY MECHANISMS	PERVASIVE SECURITY MECHANISMS
May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.	Mechanisms that are not specific to any particular OSI security service or protocol layer.
Encipherment The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.	**Trusted Functionality** That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).
Digital Signature Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).	**Security Label** The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.
Access Control A variety of mechanisms that enforce access rights to resources.	**Event Detection** Detection of security-relevant events.
Data Integrity A variety of mechanisms used to assure the integrity of a data unit or stream of data units.	**Security Audit Trail** Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.
Authentication Exchange A mechanism intended to ensure the identity of an entity by means of information exchange.	**Security Recovery** Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.
Traffic Padding The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.	
Routing Control Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.	
Notarization The use of a trusted third party to assure certain properties of a data exchange.	