CRYPTOGRAPHY AND NETWORK SECURITY

LECTURE NOTES
UNIT 1

UNIT I INTRODUCTION

COMPUTER SECURITY CONCEPTS

The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/ data, and telecommunications)

This definition introduces three key objectives that are at the heart of computer security:

- **Confidentiality:** This term covers two related concepts:
- **Data confidentiality:** Assures that private or confidential information is not made available or disclosed to unauthorized individuals.
- **Privacy:** Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.
- **Integrity:** This term covers two related concepts:
- **Data integrity:** Assures that information and programs are changed only in a specified and authorized manner.
- **System integrity:** Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.
- **Availability:** Assures that systems work promptly and service is not denied to authorized users

These three concepts form what is often referred to as the **CIA triad** (Figure 1.1). The three concepts embody the fundamental security objectives for both data and for information and computing services

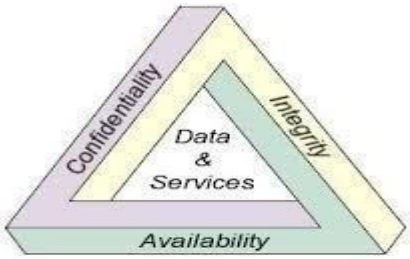

Figure 1.1 CIA triad

Although the use of the CIA triad to define security objectives is well established, some in the security field feel that additional concepts are needed to present a complete picture. Two of the most commonly mentioned are as follows:

- **Authenticity:** The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.
- **Accountability:** The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.
- **Computer Security** - Generic name for the collection of tools designed to protect data and to thwart 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 Our Focus is on Internet Security which consists of measures to deter, prevent, detect and correct security violations that involve the transmission and storage of information

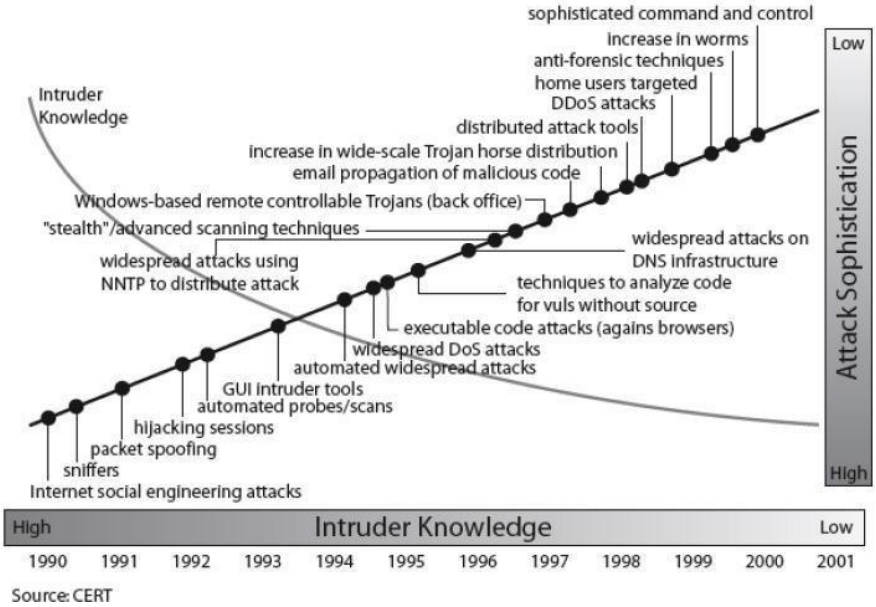

Figure 1.2 Security Trends

1.1.1 THE CHALLENGES OF COMPUTER SECURITY

Computer and network security is both fascinating and complex. Some of the reasons follow:

1. Security is not as simple as it might first appear to the novice. The requirements seem to be straightforward; indeed, most of the major requirements for security services can be given self- explanatory, one-word labels: confidentiality, authentication, non repudiation, or integrity

2. In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features.

3. Typically, a security mechanism is complex, and it is not obvious from the statement of a particular requirement that such elaborate measures are needed.

4. Having designed various security mechanisms, it is necessary to decide where to use them. This is true both in terms of physical placement and in a logical sense

.

5. Security mechanisms typically involve more than a particular algorithm or protocol

6. Computer and network security is essentially a battle of wits between a perpetrator who tries to find holes and the designer or administrator who tries to close them. The great advantage that the attacker has is that he or she need only find a single weakness, while the designer must find and eliminate all weaknesses to achieve perfect security.

7. There is a natural tendency on the part of users and system managers to perceive little benefit from security investment until a security failure occurs.

8. Security requires regular, even constant, monitoring, and this is difficult in today‟s short-term, overloaded environment.

9. Security is still too often an afterthought to be incorporated into a system after the design is complete rather than being an integral part of the design process.

10. Many users and even security administrators view strong security as an impediment to efficient and user-friendly operation of an information system or use of information.

A MODEL FOR NETWORK SECURITY

A model for much of what we will be discussing is captured, in very general terms, in Figure 1.3. A message is to be transferred from one party to another across some sort of Internet service.

A security-related transformation on the information to be sent, Examples include the encryption of the message, which scrambles 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. An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.

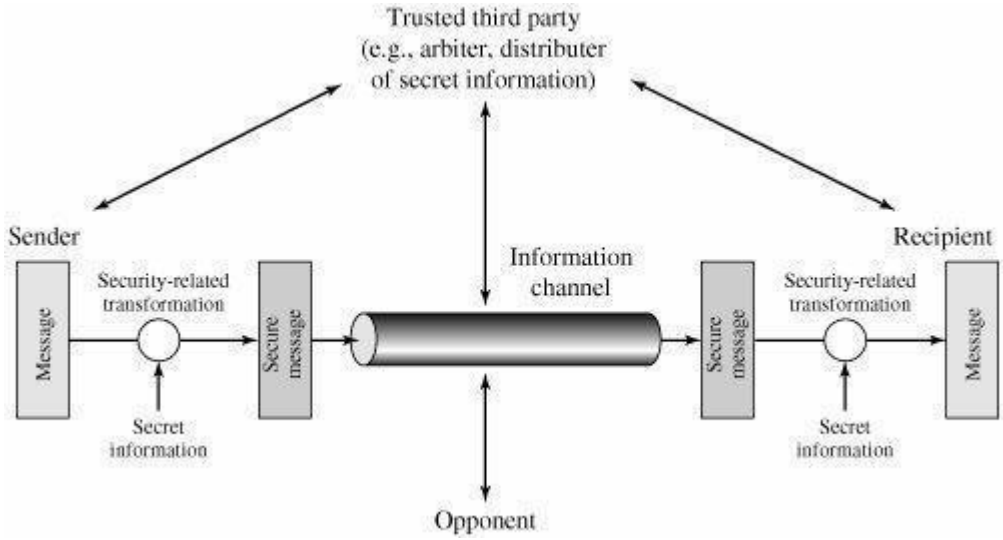

Figure 1.3 Model for Network Security

All the techniques for providing security have two components:

This general model shows that there are four basic tasks in designing a particular security service:

1. Design an algorithm for performing the security-related transformation.

The algorithm should be such that an opponent cannot defeat its purpose.

2. Generate the secret information to be used with the algorithm.

3. Develop methods for the distribution and sharing of the secret information.

4. 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 1.4, which reflects a concern for protecting an information system from unwanted access. Most readers are familiar with the concerns caused by the existence of hackers, who attempt to penetrate systems that can be accessed over a network. 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).

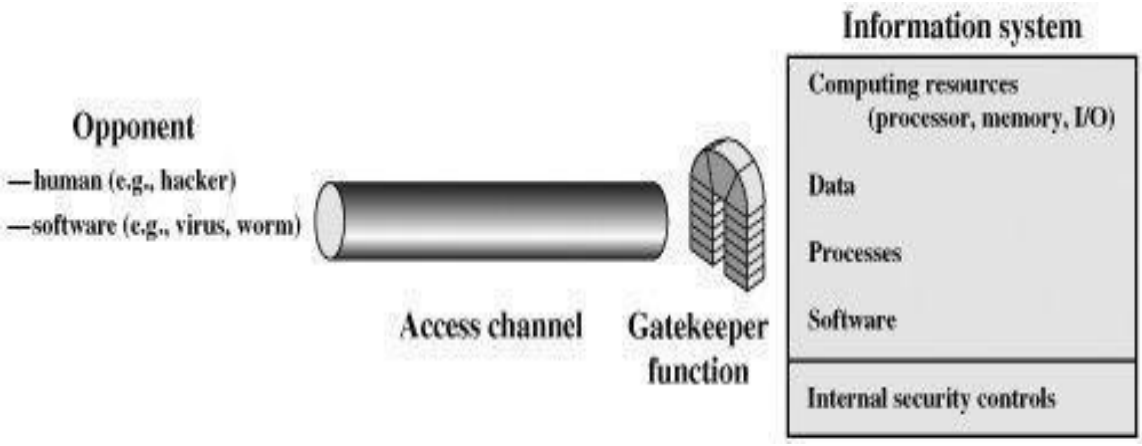

Figure 1.4 Network Access Security Model

Another type of unwanted access is the placement in a computer system of logic that exploits vulnerabilities in the system and that can affect application programs as well as utility programs, such as editors and compilers. Programs can present two kinds of threats:

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

Viruses and worms are two examples of software attacks. Such attacks can be introduced into a system by means of a disk that contains the unwanted logic concealed in otherwise useful software.

The security mechanisms needed to cope with unwanted access fall into two broad categories (see Figure 1.4).The first category might be termed a gatekeeper function. It includes password-based login procedures that are designed to deny access to all but authorized users and screening logic that is designed to detect and reject worms, viruses, and other similar attacks. Once either an unwanted user or unwanted software gains access,

The second line of defense consists of a variety of internal controls that monitor activity and analyze stored information in an attempt to detect the presence of unwanted intruders.

THE OSI SECURITY ARCHITECTURE

ITU-T Recommendation X.800, *Security Architecture for OSI*, defines such a systematic approach. The OSI security architecture is useful to managers as a way of organizing the task of providing security. This architecture was developed as an international standard, computer and communications vendors have developed security features for their products and services that relate to this structured definition of services and mechanisms.

The OSI security architecture focuses on security attacks, mechanisms, and services.

These can be defined briefly as

- **Security attack:** Any action that compromises the security of information owned by an organization.

- **Security mechanism:** A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

- **Security service:** A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service. In the literature, the terms *threat* and *attack* are commonly used to mean more or less the same thing.
-

Table 1.1 provides definitions taken from RFC 2828, *InternetSecurity Glossary.*

Threat
A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.
Attack
An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

ATTACKS

The security attacks can be classified into two types' *passive attacks* and *active attacks.* 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

Two types of passive attacks are the release of message contents and traffic analysis.

The **release of message contents** is easily understood (Figure 1.5a).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 second type of passive attack, **traffic analysis**, is subtler (Figure 1.5b). 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 might still be able to observe the pattern of these messages.

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.

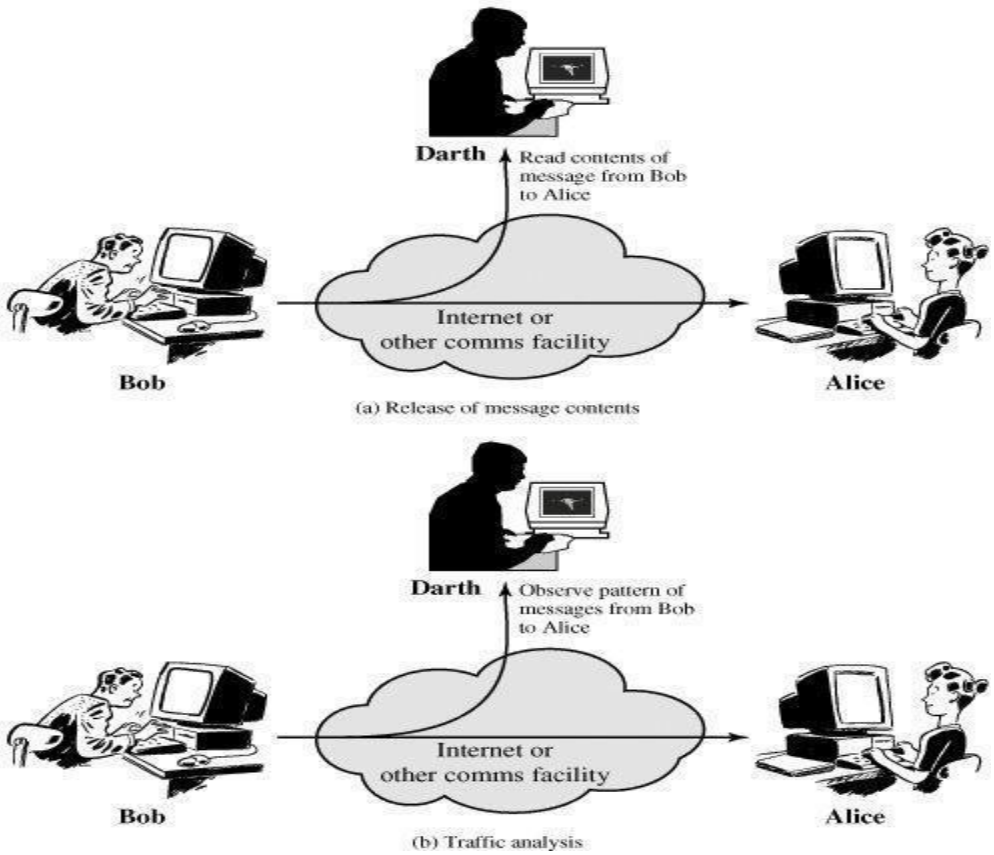

Figure 1.5 Passive Attacks

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 1.6a). A masquerade attack usually includes one of the other forms of active attack. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.

Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect (Figure 1.6b).

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 1.6c). For example, a message meaning "Allow John Smith to read confidential file *accounts*" is modified to mean "Allow Fred Brown to read confidential file *account.*

The **denial of service** prevents or inhibits the normal use or management of communications facilities (Figure 1.6d). This attack may have a specific target.

Active attacks present the opposite characteristics of passive attacks. Whereas passive attacks are difficult to detect, measures are available to prevent their success.

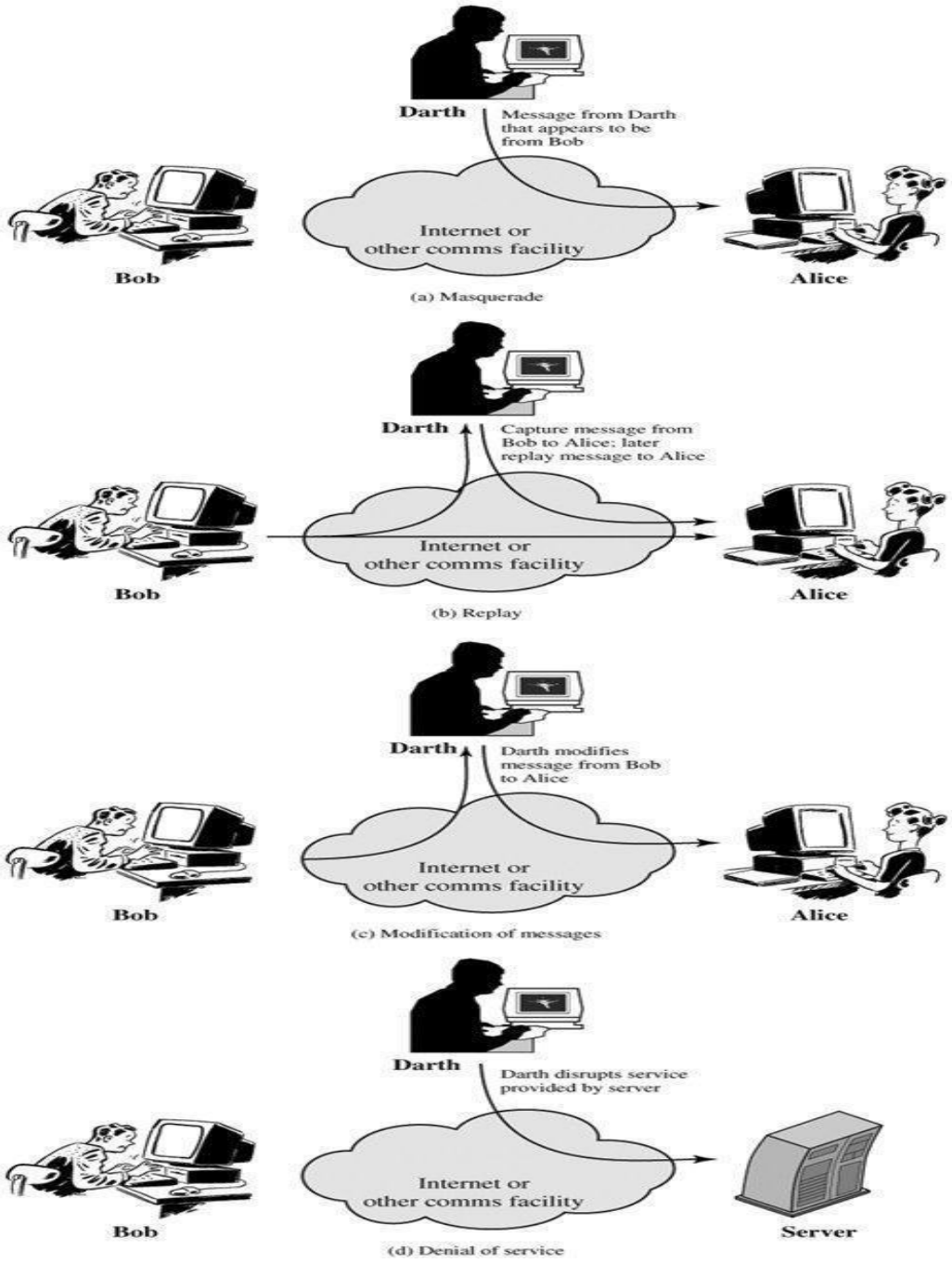

Figure 1.6 Active Attacks

SERVICES

X.800 defines a security service as a service that is provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers. Perhaps a clearer definition is found in RFC 2828, which provides the following definition: a processing or communication service that is provided by a system to give a specific kind of protection to system resources; security services implement security policies and are implemented by security mechanisms.

X.800 divides these services into five categories and fourteen specific services (Table 1.2)

Table 1.2 Security Services (X.800)

AUTHENTICATION	DATA INTEGRITY
The assurance that the communicating entity is the one that it claims to be.	The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).
Peer Entity Authentication Used in association with a logical connection to provide confidence in the identity of the entities connected.	**Connection Integrity with Recovery** Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.
Data-Origin Authentication In a connectionless transfer, provides assurance that the source of received data is as claimed.	**Connection Integrity without Recovery** As above, but provides only detection without recovery.
ACCESS CONTROL The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).	**Selective-Field Connection Integrity** Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.
DATA CONFIDENTIALITY The protection of data from unauthorized disclosure.	**Connectionless Integrity** Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.
Connection Confidentiality The protection of all user data on a connection.	**Selective-Field Connectionless Integrity** Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.
Connectionless Confidentiality The protection of all user data in a single data block	**NONREPUDIATION** Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.
Selective-Field Confidentiality The confidentiality of selected fields within the user data on a connection or in a single data block.	**Nonrepudiation, Origin** Proof that the message was sent by the specified party.
Traffic-Flow Confidentiality The protection of the information that might be derived from observation of traffic flows.	**Nonrepudiation, Destination** Proof that the message was received by the specified party.

MECHANISMS

Table 1.3 lists the security mechanisms defined in X.800. The mechanisms are divided into those that are implemented in a specific protocol layer, such as TCP or an application-layer protocol, and those that are not specific to any particular protocol layer or security service

. 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.	

CLASSICAL ENCRYPTION TECHNIQUES

Symmetric encryption is a form of cryptosystem in which encryption and decryption are performed using the same key. It is also known as conventional encryption.

- Symmetric encryption transforms plaintext into ciphertext using a secret key and an encryption algorithm. Using the same key and a decryption algorithm, the plaintext is recovered from the ciphertext.
- The two types of attack on an encryption algorithm are cryptanalysis, based on properties of the encryption algorithm, and brute-force, which involves trying all possible keys.
- Traditional (precomputer) symmetric ciphers use substitution and/or transposition techniques. Substitution techniques map plaintext elements (characters, bits) into ciphertext elements. Transposition techniques systematically transpose the positions of plaintext elements.
- Rotor machines are sophisticated precomputer hardware devices that use substitution techniques.
- Steganography is a technique for hiding a secret message within a larger one in such a way that others cannot discern the presence or contents of the hidden message.

An original message is known as the **plaintext**, while the coded message is called the **ciphertext**. The process of converting from plaintext to ciphertext is known as **enciphering** or **encryption**; restoring the plaintext from the ciphertext is **deciphering** or **decryption**. The many schemes used for encryption constitute the area of study known as **cryptography**.

Such a scheme is known as a **cryptographic system** or a **cipher**. Techniques used for deciphering a message without any knowledge of the enciphering details fall into the area of **cryptanalysis**. Cryptanalysis is

what the layperson calls “breaking the code” The areas of cryptography and cryptanalysis together are called **cryptology**.

SYMMETRIC CIPHER MODEL

A symmetric encryption scheme has five ingredients (Figure 1.7):

- **Plaintext:** This is the original intelligible message or data that is fed into the algorithm as input.
- **Encryption algorithm:** The encryption algorithm performs various substitutions and transformations on the plaintext.
- **Secret key:** The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key
- **Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts. The ciphertext is an apparently random stream of data and, as it stands, is unintelligible.
- **Decryption algorithm:** This is essentially the encryption algorithm run in reverse. It takes the cipher text and the secret key and produces the original plaintext.

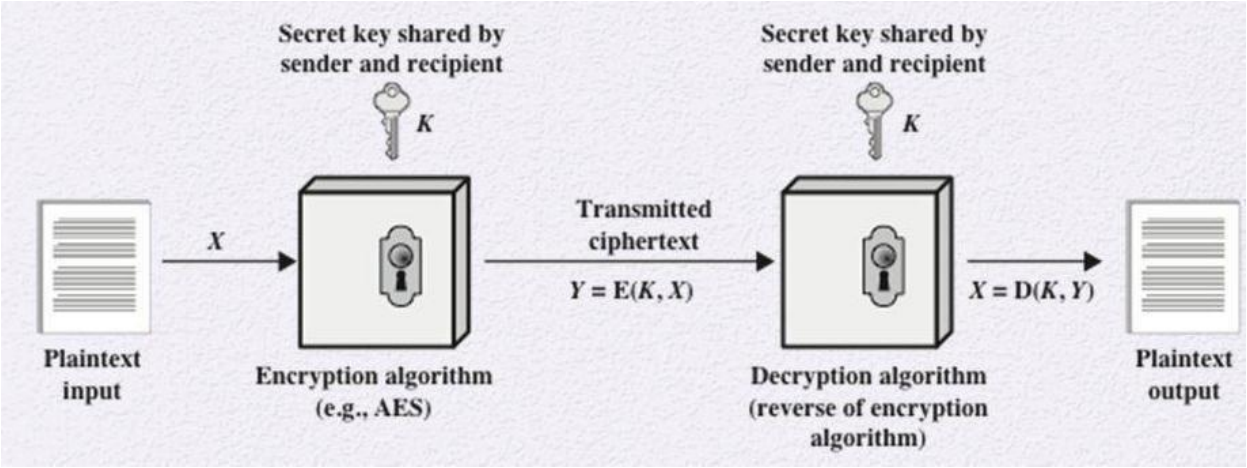

Figure 1.7 Simplified Model of Symmetric Encryption

There are two requirements for secure use of conventional encryption:

1. We need a strong encryption algorithm. At a minimum, we would like the algorithm to be such that an opponent who knows the algorithm and has access to one or more ciphertexts would be unable to decipher the ciphertext or figure out the key. This requirement is usually stated in a stronger form: The opponent should be unable to decrypt ciphertext or discover the key even if he or she is in possession of a number of ciphertexts together with the plaintext that produced each ciphertext.

2. Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure. If someone can discover the key and knows the algorithm, all communication using this key is readable.

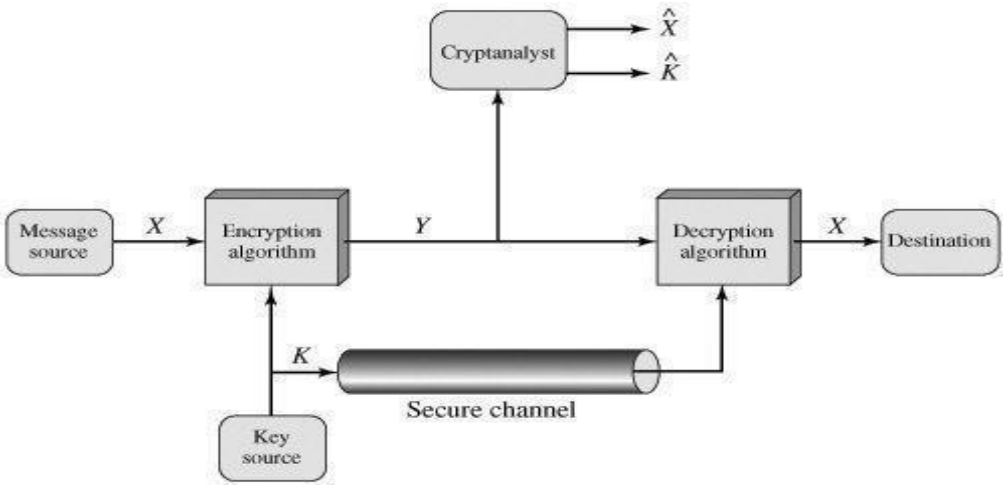

Figure 1.8 Model of Symmetric Cryptosystem

With the message X and the encryption key K as input, the encryption algorithm forms the ciphertext Y=[Y1,Y2,.....Y_N] .We can write this as Y=E(K,X)This notation indicates that is produced by using encryption algorithm E as a function of the plaintext X , with the specific function determined by the value of the key K .
The intended receiver, in possession of the key, is able to invert the transformation:

X=D(K,Y)

An opponent, observing Y but not having access K to X or, may attempt to recover X or K or both X and K. It is assumed that the opponent knows the encryption (E) and decryption (D) algorithms. If the opponent is interested in only this particular message, then the focus of the effort is to recover X by generating a plaintext estimate X. Often, however, the opponent is interested in being able to read future messages as well, in which case an attempt is made to recover K by generating an estimate K.

Cryptography

Cryptographic systems are characterized along three independent dimensions:

The type of operations used for transforming plaintext to ciphertext:

All encryption algorithms are based on two general principles: substitution, in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element, and transposition, in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost (that is, that all operations are reversible). Most systems, referred to as *product systems*, involve multiple stages of substitutions and transpositions.

1. **The number of keys used.** If both sender and receiver use the same key, the system is referred to as symmetric, single-key, secret-key, or conventional encryption. If the sender and receiver use different keys, the system is referred to as asymmetric, two-key, or public-key encryption.
2. **The way in which the plaintext is processed.** A *block cipher* processes the input one block of elements at a time, producing an output block for each input block. A *stream cipher* processes the input elements continuously, producing output one element at a time, as it goes along.
3. **Cryptanalysis and Brute-Force Attack**

Typically, the objective of attacking an encryption system is to recover the key in use rather than simply to recover the plaintexts of a single ciphertext. There are two general approaches to attacking a conventional encryption scheme:

- **Cryptanalysis:** Cryptanalytic attacks rely on the nature of the algorithm plusperhaps some knowledge of the general characteristics of the plaintext oreven some sample plaintext- ciphertext pairs. This type of attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.

- **Brute-force attack**: The attacker tries every possible key on a piece of cipher text until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

Table 1.4 summarizes the various types of cryptanalytic attacks based on the amount of information known to the cryptanalyst. The most difficult problem is presented when all that is available is the ciphertext only.

Table 1.4 Types of Attacks on Encrypted Messages

Type of Attack	Known to Cryptanalyst
Ciphertext Only	• Encryption algorithm • Ciphertext
Known Plaintext	• Encryption algorithm • Ciphertext • One or more plaintext–ciphertext pairs formed with the secret key
Chosen Plaintext	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen Ciphertext	• Encryption algorithm • Ciphertext • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen Text	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

A **brute-force attack** involves trying every possible key until an intelligible translation of the ciphertext into plaintext is obtained.

SUBSTITUTION TECHNIQUES

The two basic building blocks of all encryption techniques are substitution and transposition. A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols.1 If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns.

1. Caesar Cipher

The earliest known, and the simplest, use of a substitution cipher was by Julius Caesar. The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet. For example,

plain: meet me after the toga party cipher: PHHW PH DIWHU WKH WRJD SDUWB

Note that the alphabet is wrapped around, so that the letter following Z is A. We can define the transformation by listing all possibilities, as follows: plain: 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
cipher: 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

Let us assign a numerical equivalent to each letter:
When letters are involved, the following conventions are used in this book. Plaintext is always in lowercase; ciphertext is in uppercase; key values are in italicized lowercase.

Let us assign a numerical equivalent to each letter:

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Then the algorithm can be expressed as follows. For each plaintext letter, substitute the cipher text letter:

$C = E(3, p) = (p + 3) \bmod 26$

A shift may be of any amount, so that the general Caesar algorithm is

$C = E(k, p) = (p + k) \bmod 26$

where takes on a value in the range 1 to 25.The decryption algorithm is simply $p = D(k, C) =$

$(C - k) \bmod 26$

If it is known that a given ciphertext is a Caesar cipher, then a brute-force cryptanalysis is easily performed: simply try all the 25 possible keys. Three important characteristics of this problem enabled us to use a bruteforce cryptanalysis:

1. The encryption and decryption algorithms are known.

2. There are only 25 keys to try.

3. The language of the plaintext is known and easily recognizable.

KEY	PHHW PH DIWHU WKH WRJD SDUWB
1	oggv og chvgt vjg vqic rctva
2	nffu nf bgufs uif uphb qbsuz
3	meet me after the toga party
4	ldds ld zesdq sgd snfz ozqsx
5	kccr kc ydrcp rfc rmey nyprw
6	jbbq jb xcqbo qeb qldx mxoqv
7	iaap ia wbpan pda pkcw lwnpu
8	hzzo hz vaozm ocz ojbv kvmot
9	gyyn gy uznyl nby niau julns
10	fxxm fx tymxk max mhzt itkmr
11	eww1 ew sxlwj lzw lgys hsjlq
12	dvvk dv rwkvi kyv kfxr grikp
13	cuuj cu qvjuh jxu jewq fqhjo
14	btti bt puitg iwt idvp epgin
15	assh as othsf hvs hcuo dofhm
16	zrrg zr nsgre gur gbtn cnegl
17	yqqf yq mrfqd ftq fasm bmdfk
18	xppe xp lqepc esp ezrl alcej
19	wood wo kpdob dro dyqk zkbdi
20	vnnc vn jocna cqn cxpj yjach
21	ummb um inbmz bpm bwoi xizbg
22	tlla tl hmaly aol avnh whyaf
23	skkz sk glzkx znk zumg vgxze
24	rjjy rj fkyjw ymj ytlf ufwyd
25	qiix qi ejxiv xli xske tevxc

Figure 1.9 Brute-Force Cryptanalysis of Caesar Cipher

2. Monoalphabetic Ciphers

With only 25 possible keys, the Caesar cipher is far from secure.A dramatic increasein the key space can be achieved by allowing an arbitrary substitution. A **permutation** of a finite set of elements is an ordered sequence of all the elements of, with each element appearing exactlyonce. For example, if S ={a,b,c} , there are six permutations of : abc, acb, bac, bca, cab, cba

In general, there are n! permutations of a set of elements, because the first element can be chosen in one of *n* ways, the second in n-1 ways, the third in n-2 ways, and so on.

Recall the assignment for the Caesar cipher:

plain: a b c d e f g h I j kl m n o p q r s t u v w x y z

cipher: 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

If, instead, the “cipher” line can be any permutation of the 26 alphabetic characters, then there are 26! or greater than $4*10^{26}$ possible keys. This is 10 orders of magnitude greater than the key space for DES and would seem to eliminate brute-force techniques for cryptanalysis. Such an approach is referred to as a **monoalphabetic substitution cipher**, because a single cipher alphabet (mapping from plain alphabetto cipher alphabet) is used per message.

The ciphertext to be solved is

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

As a first step, the relative frequency of the letters can be determined and compared to a standard frequency distribution for English, such as is shown in Figure 1.9. If the message were long enough, this technique alone might be sufficient, but because this is a relatively short message, we cannot expect an exact match. In any case, the relative frequencies of the letters in the ciphertext (in percentages) are as follows:

P 13.33	H 5.83	F 3.33	B 1.67	C 0.00
Z 11.67	D 5.00	W 3.33	G 1.67	K 0.00
S 8.33	E 5.00	Q 2.50	Y 1.67	L 0.00
U 8.33	V 4.17	T 2.50	I 0.83	N 0.00
O 7.50	X 4.17	A 1.67	J 0.83	R 0.00
M 6.67				

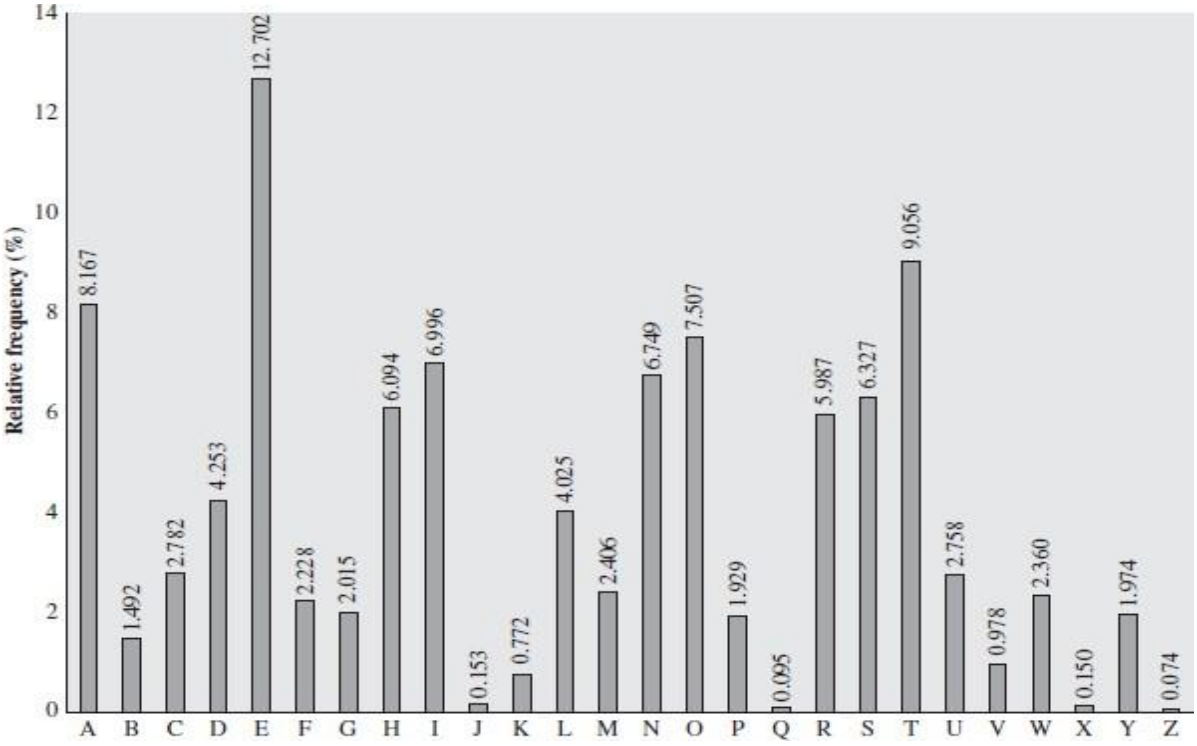

Figure 1.10 Relative Frequencies of Letters in English Text

That cipher letters P and Z are the equivalents of plain letters e and t, but it is not certain which is which. The letters S, U, O, M, and H are all of relatively high frequency and probably correspond to plain letters from the set {a, h, i, n, o, r, s}. The letters with the lowest frequencies (namely A, B, G, Y, I, J) are likely included in the set {b, j, k, q, v, x, z}.

A powerful tool is to look at the frequency of two-letter combinations, known as **digrams.** The most common such digram is th. In our ciphertext, the most common digram is ZW, which appears three times. So we make the correspondence of Z with t and W with h. Then, by our earlier hypothesis, we can equate P with e. Now notice that the sequence ZWP appears in the ciphertext, and we can translate that sequence as “the.” This is the most frequent trigram (three- letter combination). Next, notice the sequence ZWSZ in the first line. We do not know that these four letters form a complete word, but if they do, it is of the form th_t. If so, Sequates with a.

So far, then, we have

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
 t a        e  e te  a that e e a       a
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
   e t   ta t ha e ee  a e  th    t  a
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
 e  e e tat  e   the   t
```

Only four letters have been identified, but already we have quite a bit of the message. Continued analysis of frequencies plus trial and error should easily yield a solution from this point. The complete plaintext, with spaces added between words, follows:

it was disclosed yesterday that several informal but direct contacts have been made with political representatives of the viet cong in moscow

Monoalphabetic ciphers are easy to break because they reflect the frequency data of the original alphabet. A countermeasure is to provide multiple substitutes, known as homophones, for a single letter.

3. Playfair Cipher

The best-known multiple-letter encryption cipher is the Playfair, which treats digrams in the plaintext as single units and translates these units into ciphertext digrams. The Playfair algorithm is based on the use of a 5 × 5 matrix of letters constructed using a keyword. Here is an example, solved by Lord Peter Wimsey inDorothy Sayers"s *Have His Carcase*

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

In this case, the keyword is *monarchy*. The matrix is constructed by filling in the letters of the keyword (minus duplicates) from left to right and from top to bottom, and then filling in the remainder of the matrix with the remaining letters in alphabetic order. The letters I and J count as one letter. Plaintext is encrypted two letters at a time, according to the following rules:

1. Repeating plaintext letters that are in the same pair are separated with a filler letter, such as x, so that balloon would be treated as ba lx lo on.

2. Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last. For example, ar is encrypted as RM.

3. Two plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last. For example, mu is encrypted as CM.

4. Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter. Thus, hs becomes BP and ea becomes IM (or JM, as the encipherer wishes).

The Playfair cipher is a great advance over simple monoalphabetic ciphers. For one thing, whereas there are only 26 letters, there are 26 × 26 = 676 digrams, so that identification of individual digrams is more difficult. Furthermore, the relative frequencies of individual letters exhibit a much greater range than that of digrams, making frequency analysis much more difficult. For these reasons, the Playfair cipher was for a long time considered unbreakable. It was used as the standard field system by the British Army in World War I and still enjoyed considerable use by the U.S. Army and other Allied forces during World War II.

TRANSPOSITION TECHNIQUES

All the techniques examined so far involve the substitution of a ciphertext symbol for a plaintext symbol. A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is referred to as a transposition cipher. The simplest such cipher is the **rail fence** technique, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows. For example, to encipher the message “meet me after the toga party” with a rail fence of depth 2, we write the following:

```
m e m a t r h t g p r y
 e t e f e t e o a a t
```

The encrypted message is

MEMATRHTGPRYETEFETEOAAT

This sort of thing would be trivial to cryptanalyze. A more complex scheme is to write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns. The order of the columns then becomes the key to the algorithm. For example,

```
Key:          4 3 1 2 5 6 7
Plaintext:    a t t a c k p
              o s t p o n e
              d u n t i l t
              w o a m x y z
Ciphertext:   TTNAAPTMTSUOAODWCOIXKNLYPETZ
```

Thus, in this example, the key is 4312567.To encrypt, start with the column that is labeled 1, in this case column 3.Write down all the letters in that column. Proceed to column 4, which is labeled 2, then column 2, then column 1, then columns 5, 6, and 7.A pure transposition cipher is easily recognized because it has the same letter frequencies as the original plaintext. For the type of columnar transposition just shown, cryptanalysis is fairly straightforward and involves laying out the ciphertext in a matrix and playing around with column positions. Digram and trigram frequency tables can be useful.

The transposition cipher can be made significantly more secure by performing more than one stage of transposition. The result is a more complex permutation that is not easily reconstructed. Thus, if the foregoing message is reencrypted using the same algorithm,

```
Key:        4 3 1 2 5 6 7
Input:      t t n a a p t
            m t s u o a o
            d w c o i x k
            n l y p e t z
Output:     NSCYAUOPTTWLTMDNAOIEPAXTTOKZ
```

To visualize the result of this double transposition, designate the letters in the original plaintext message by the numbers designating their position. Thus, with 28 letters in the message, the original sequence of letters is

01 02 03 04 05 06 07 08 09 10 11 12 13 14

15 16 17 18 19 20 21 22 23 24 25 26 27 28 After the first transposition, we have

03 10 17 24 04 11 18 25 02 09 16 23 01 08

15 22 05 12 19 26 06 13 20 27 07 14 21 28

MEMATRHTGPRYETEFETEOAAT

STEGANOGRAPHY

A plaintext message may be hidden in one of two ways. The methods of **steganography** conceal the existence of the message, whereas the methods of cryptography render the message unintelligible to outsiders by various transformations of the text.

A simple form of steganography, but one that is time-consuming to construct, is one in which an arrangement of words or letters within an apparently innocuous text spells out the real message. For example, the sequence of first letters of each word of the overall message spells out the hidden message. Figure shows an example in which a subset of the words of the overall message is used to convey the hidden message.

3rd March

Dear George,

Greetings to all at Oxford. Many thanks for your letter and for the Summer examination package. All Entry Forms and Fees Forms should be ready for final despatch to the Syndicate by Friday 20th or at the very latest, I'm told. by the 21st. Admin has improved here, though there's room for improvement still; just give us all two or three more years and we'll really show you! Please don't let these wretched 16+ proposals destroy your basic O and A pattern. Certainly this sort of change, if implemented immediately, would bring chaos.

Sincerely yours.

Various other techniques have been used historically; some examples are the following: **Character marking:** Selected letters of printed or typewritten text are overwritten in pencil. The marks are ordinarily not visible unless the paper is held at an angle to bright light.

Invisible ink: A number of substances can be used for writing but leave no visible trace until heat or some chemical is applied to the paper.

Pin punctures: Small pin punctures on selected letters are ordinarily not visible unless the paper is held up in front of a light.

Typewriter correction ribbon: Used between lines typed with a black ribbon, the results of typing with the correction tape are visible only under a strong light

Steganography has a number of drawbacks when compared to encryption. It requires a lot of overhead to hide a relatively few bits of information, although using a scheme like that proposed in the preceding paragraph may make it more effective. Also, once the system is discovered, it becomes virtually worthless. This problem, too, can be overcome if the insertion method depends on some sort of key.

The advantage of steganography is that it can be employed by parties who have something to lose should the fact of their secret communication (not necessarily the content) be discovered. Encryption flags traffic as important or secret or may identify the sender or receiver as someone with something to hide.

Foundations of modern cryptography

Modern encryption is the key to advanced computer and communication security. This stream of cryptography is completely based on the ideas of mathematics such as number theory and computational complexity theory as well as concepts of probability.

Characteristics of Modern Cryptography

There are four major characteristics that separate modern cryptography from the classical approach.

Table 1.5 Differences between Traditional Encryption and Modern Encryption

Traditional Encryption	Modern Encryption
For making ciphertext, manipulation is done in the characters of the plaintext	For making ciphertext, operations are performed on binary bit sequence
The whole of the ecosystem is required to communicate confidentiality	Here, only the parties who want to execute secure communication possess the secret key
These are weaker as compared to modern encryption	The encryption algorithm formed by this encryption technique is stronger as compared to traditional encryption algorithms
It believes in the concept of security through obscurity	Its security depends on the publicly known mathematical algorithm

Context of Cryptography

Cryptology, the study of cryptosystems, can be subdivided into two branches −

- Cryptography
- Cryptanalysis **Cryptography**

Cryptography is the art and science of making a cryptosystem that is capable of providing information security. Cryptography deals with the actual securing of digital data. It refers to the design of mechanisms based on mathematical algorithms that provide fundamental information security services.

Cryptanalysis

The art and science of breaking the cipher text is known as cryptanalysis. Cryptanalysis is the sister branch of cryptography and they both co-exist. The cryptographic process results in the cipher text for transmission or storage. It involves the study of cryptographic mechanism with the intention to break them. Cryptanalysis is also used during the design of the new cryptographic techniques to test their security strengths.

Note − Cryptography concerns with the design of cryptosystems, while cryptanalysis studies the breaking of cryptosystems.

REALTIME SECURITY ATTACKS

1.DDoS attacks:

DDoS attacks, or Distributed Denial-of-Service attacks, are a type of cyberattack that aims to disrupt online services by overwhelming the target's servers with a flood of traffic. This excessive traffic can render the service unavailable to legitimate users, causing significant disruption and potential financial loss.

How DDoS Attacks Work

In a DDoS attack, the attacker utilizes a network of compromised devices, known as a botnet, to launch the attack. These devices, often infected with malware, are controlled remotely by the attacker. The attacker sends commands to the botnet, instructing each device to send a large volume of traffic to the target server simultaneously.

Types of DDoS Attacks

There are several types of DDoS attacks, each targeting different vulnerabilities:

- Volume-based attacks: These attacks aim to overwhelm the target's network bandwidth by flooding it with a massive amount of traffic. Common types include UDP floods, ICMP floods, and HTTP floods.
- Protocol attacks: These attacks target specific network protocols, such as TCP or SYN, by sending malformed or incomplete packets to disrupt the communication process.
- Application layer attacks: These attacks target specific applications or services running on the target server, such as web servers or databases. They exploit vulnerabilities in the application's code or configuration to disrupt its functionality.

Mitigating DDoS Attacks

Mitigating DDoS attacks requires a multi-layered approach, including:

- Network-level mitigation: This involves implementing techniques like rate limiting, blackholing, and traffic scrubbing to filter out malicious traffic.
- Application-level mitigation: This involves using techniques like web application firewalls (WAFs) and bot management solutions to identify and block malicious traffic at the application layer.
- Cloud-based DDoS protection: This involves leveraging cloud-based security solutions that can provide advanced protection against DDoS attacks, including large-scale mitigation capabilities and AI-powered threat detection.

Additional Considerations

- DDoS protection services: Many service providers offer DDoS protection services that can help organizations mitigate these attacks effectively.
- Regular security audits: Conducting regular security audits can help identify and address vulnerabilities that could be exploited in a DDoS attack.
- Employee training: Educating employees about the risks of DDoS attacks and best practices for cybersecurity can help prevent accidental attacks.

By understanding the mechanics of DDoS attacks and implementing appropriate mitigation strategies, organizations can significantly reduce their risk of falling victim to these disruptive cyberattacks.

2. Session hijacking attack:

Session hijacking is a type of cyberattack where an attacker steals a valid user session to gain unauthorized access to a system or network. Think of it as someone stealing your online identity and using it to access your accounts without your knowledge.

How Does It Work?

1. Session Establishment: When you log into a website, the server creates a unique session ID to identify your connection. This ID is often stored in a cookie on your browser.
2. Session Hijacking: An attacker can intercept this session ID through various methods:
    - Packet Sniffing: Monitoring network traffic to capture the session ID as it's transmitted.
    - Cross-Site Scripting (XSS): Exploiting vulnerabilities in websites to inject malicious code that steals the session ID.
    - Man-in-the-Middle (MitM) Attacks: Intercepting communication between the user and the server to capture the session ID.
3. Unauthorized Access: Once the attacker has the session ID, they can impersonate the legitimate user and access their accounts, data, or sensitive information.

Preventing Session Hijacking

To protect yourself from session hijacking, follow these best practices:

1. Strong, Unique Passwords: Use strong, unique passwords for all your online accounts.
2. Enable Two-Factor Authentication (2FA): 2FA adds an extra layer of security by requiring a second form of verification, such[1] as a code sent to your phone.
3. Use HTTPS: Ensure that you're using HTTPS, which encrypts communication between your browser and the website.
4. Be Cautious of Public Wi-Fi: Avoid accessing sensitive information on public Wi-Fi networks, as they're more vulnerable to attacks.
5. Keep Software Updated: Regularly update your operating system and web browser to patch security vulnerabilities.
6. Use Security Software: Install and use reputable antivirus and anti-malware software.
7. Be Wary of Phishing Attacks: Be cautious of suspicious emails and links that may lead to malicious websites.

By following these guidelines, you can significantly reduce your risk of falling victim to session hijacking and other cyber threats.

3.Spoofing attack

Spoofing is a type of cyberattack where an attacker disguises their identity as a trusted entity to gain unauthorized access or deceive victims. It's like a digital version of trickery, where the attacker pretends to be someone or something they're not.

Types of Spoofing:

There are several common types of spoofing attacks:

1. Email Spoofing:
    - Attackers send emails that appear to be from legitimate sources (like banks, online retailers, or government agencies) to trick recipients into revealing personal information or clicking on malicious links.
    - They achieve this by forging the sender's email address, making it look like the email is from a trusted source.
2. Caller ID Spoofing:
    - Attackers manipulate the caller ID display on a phone to make it appear as if a call is coming from a different number, often a legitimate business or government agency.
    - This technique is often used in phishing scams or to harass individuals.
3. IP Address Spoofing:
    - Attackers forge the source IP address of a network packet to disguise their true origin.
    - This allows them to bypass security measures and launch attacks, such as DDoS attacks or unauthorized access to networks.
4. Website Spoofing:
    - Attackers create fake websites that mimic legitimate ones, often with similar domain names or URLs.
    - They trick users into entering sensitive information, such as login credentials or credit card details, on these fraudulent sites.
5. GPS Spoofing:
    - Attackers interfere with GPS signals to mislead devices about their location.
    - This can be used to disrupt transportation systems, military operations, or other GPS-reliant services.

How to Protect Yourself:

Here are some tips to protect yourself from spoofing attacks:

- Be cautious of unsolicited emails and phone calls: Verify the sender's identity before responding or clicking on links.
- Look for suspicious signs: Check the sender's email address, the URL of the website, and the caller ID carefully.
- Use strong, unique passwords: Avoid using the same password for multiple accounts.
- Enable two-factor authentication: This adds an extra layer of security[1] to your accounts.
- Keep your software up-to-date: Regularly update your operating system and security software.
- Be aware of phishing attacks: Educate yourself about common phishing tactics and how to identify them.
- Use reputable security solutions: Install antivirus and anti-malware software to protect your devices.

By staying vigilant and following these tips, you can significantly reduce your risk of falling victim to spoofing attacks.

4.Phishing attack:

A Persistent Threat in Network Security Phishing is a type of cyberattack where malicious actors disguise themselves as trustworthy entities to deceive individuals into revealing sensitive information. This technique often involves sending fraudulent emails, text messages, or creating fake websites to trick users into clicking malicious links or downloading harmful attachments.

How Phishing Attacks Work

1. Crafting the Lure: Attackers carefully craft messages that appear to come from legitimate sources like banks, social media platforms, or online retailers. These messages often create a sense of urgency or fear, urging the recipient to take immediate action.

2. The Bait: The message may contain a malicious link or attachment that, when clicked, downloads malware onto the victim's device. Alternatively, it may direct the victim to a fake website designed to steal personal information.
3. The Hook: Once the victim falls for the trick, they may unwittingly provide their sensitive information, such as login credentials, credit card numbers, or social security numbers.

Types of Phishing Attacks

- Email Phishing: The most common type, involves sending fraudulent emails that mimic legitimate messages.
- Smishing: Phishing attacks carried out through text messages (SMS).
- Vishing: Phishing attacks conducted over the phone.
- Spear Phishing: Targeted phishing attacks aimed at specific individuals or organizations.

Protecting Yourself from Phishing Attacks

- Be Skeptical: Always be cautious of unsolicited emails, text messages, or phone calls.
- Verify the Sender: Check the sender's email address and look for any spelling or grammatical errors.
- Avoid Clicking on Suspicious Links: Hover over links to see the actual URL before clicking.
- Use Strong, Unique Passwords: Create strong, unique passwords for each of your online accounts.
- Enable Two-Factor Authentication: Add an extra layer of security to your accounts.
- Keep Your Software Updated: Regularly update your operating system and software to patch security vulnerabilities.
- Use a Reputable Antivirus Program: Protect your device from malware.
- Be Aware of Social Engineering Tactics: Phishers often use social engineering techniques to manipulate people into revealing sensitive information.

Mitigating Phishing Attacks in Network Security

Organizations can implement the following measures to protect their networks:

- Employee Training: Educate employees about phishing tactics and how to identify suspicious emails.
- Email Filtering: Use email filters to block suspicious emails and spam.
- Web Filtering: Block access to malicious websites.
- Intrusion Detection Systems (IDS): Monitor network traffic for signs of malicious activity.
- Security Awareness Training: Conduct regular training sessions to keep employees informed about the latest threats.
- Incident Response Plan: Have a plan in place to respond to phishing attacks and other security incidents.

By staying informed and taking proactive steps, individuals and organizations can significantly reduce their risk of falling victim to phishing attacks.

Would you like to know more about specific phishing techniques or how to create a strong security awareness program?