Unit 1: Introduction and Classical Ciphers

Security:

Security, in information technology (IT), is the defense of digital information and IT assets against internal and external, malicious and accidental threats. This defense includes detection, prevention and response to threats through the use of security policies, software tools and IT services.

Computer Security: It is a process and the collection of measures and controls that ensures the Confidentiality, Integrity and Availability (CIA) of the assets in computer systems. Computer Security protects you from both software and hardware part of a computer systems from getting compromised and be exploited.

Information Security: Information security is primarily concerned with making sure that data in any form is kept secure in terms of preserving its confidentiality, integrity and availability.

Information is a significant asset that can be stored in different ways such as digitally stored, printed, written on papers or in human memory. It can be communicated through different channels such as spoken languages, gestures or using digital channel such as email, SMS, social media, video, audio etc.

Information security differs from cybersecurity such that information security aims to keep data in any form secure, whereas cybersecurity protects only digital data. Cybersecurity is the subset of information security.

Network Security: It is any activity designed to protect the usability and integrity of your network and data. It includes both hardware and software technologies.

An effective network security manages access to the network. It targets a variety of threats and stop them from entering or spreading on your network.

Network security, a subset of cybersecurity, aims to protect any data that is being sent through devices in your network to ensure that the information is not changed or intercepted.

CIA Triad:

Confidentiality, integrity and availability, also known as the CIA triad, is a model designed to guide policies for information security within an organization.

Confidentiality: Preserving authorized restrictions on information access and disclosure. 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: Guarding against improper information modification or destruction. This term covers two related concepts:

Data integrity: Assures that information (both stored and in transmitted packets) 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.

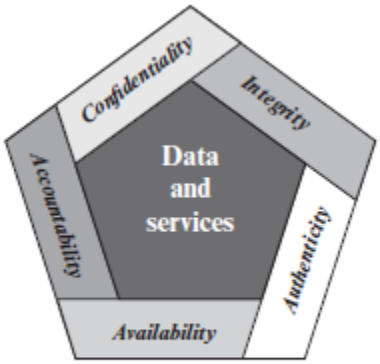


Figure 1.1 Essential Network and Computer Security Requirements

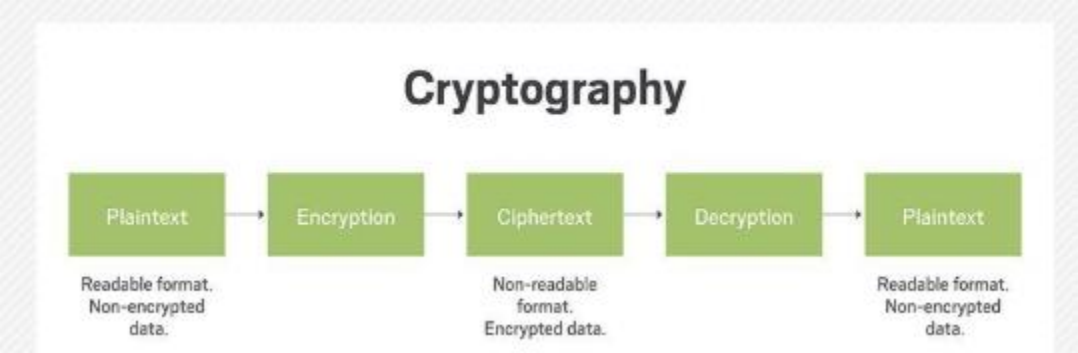
Authenticity: The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.

Accountability: It means that every individual who works with an information system should have specific responsibilities for information assurance.

Access Control: The prevention of unauthorized use of a resource.

Nonrepudiation: Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

Cryptography: Cryptography is a method of protecting information and communications through the use of codes so that only those for whom the information is intended can read and process it.



Cryptosystem:

In cryptography, a cryptosystem is a structure or scheme consisting of a set of algorithms needed to implement a particular security service, most commonly for achieving confidentiality. Typically, a cryptosystem consists of three algorithms: one for key generation, one for encryption, and one for decryption. The term cipher is often used to refer to a pair of algorithms, one for encryption and one for decryption.

Cryptanalysis:

Cryptanalysis is the study of ciphertext, ciphers and cryptosystems with the aim of understanding how they work and finding techniques for defeating or weakening them. Cryptanalysis is used to breach cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key is unknown.

Security Threats and Attacks:

Threat:

Threat can be anything that can take advantage of a vulnerability to breach security and negatively alter, erase, harm object or objects of interest. In simple words, a threat is a potential violation of security which might or might not occur.

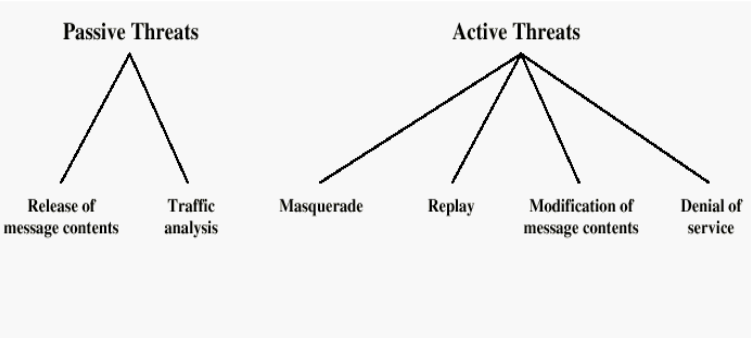


Figure 1.2 Active and Passive Security Threats

Security Attack: Any action that compromises the security of information.

Passive attack: unauthorized reading of a message or a file.

Active attack: modification of messages or files, and denial of service.

Interruption: This is an attack on availability

Interception: This is an attack on confidentiality

Modification: This is an attack on integrity

Fabrication: This is an attack on authenticity

Snooping:

It is the unauthorized interception of information and disclosure. Passively listening (or reading) to communications or browsing through files or system information.

Modification or Alteration:

Unauthorized change of information. If modified data controls the operation of the system, threats of failure may arise.

Masquerading or Spoofing:

One entity pretends to be a different entity.

Repudiation of origin:

A false denial that an entity sent or created something.

Denial of receipt:

A false denial that an entity received some information or message.

Delay:

Usually delivery of a message or service requires some time t. If an attacker can force the delivery to take more than time t, the attacker has successfully delayed delivery.

Replay:

A replay attack is a category of network attack in which an attacker detects a data transmission and fraudulently has it delayed or repeated.

Denial of service:

The attacker prevents a server from providing a service. The denial may occur at the source (by preventing the server from obtaining the resources), at the destination (by blocking the communications from the server) or along the intermediate path (by discarding messages from either the client or the server, or both).

Security Service:

A service that enhances the security of data processing systems and information transfers. A security service makes use of one or more security mechanisms.

- Confidentiality (privacy)
- Authentication (who created or sent the data)
- Integrity (has not been altered)
- Non-repudiation (the order is final)
- Access control (prevent misuse of resources)
- Availability (permanence, non-erasure)
  - Denial of Service Attacks
  - Virus that deletes files

Security Mechanism:

A mechanism that is designed to detect, prevent, or recover from a security attack.

- Encipherment
- Digital Signature
- Access Control
- Data Integrity
- Authentication exchange
- Traffic padding
- Notarization

Classical Cryptosystems:

Classical cryptosystems (also called single-key or symmetric cryptosystems) are cryptosystems that use the same key for encipherment and decipherment.

Substitution Techniques:

A substitution cipher changes characters in the plaintext to produce the ciphertext.

Caesar cipher (Shift Cipher):

The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet.

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

For example,

plain: meet me after the toga party

cipher: PHHW PH DIWHU WKH WRJD SDUWB

Algorithm:

For each plain text letter p, substitute the ciphertext letter C.

C = E (3, p) = (p + 3) mod 26

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

C = E (k, p) = (p + k) mod 26

where k takes on a value in the range 1 to 25.

The decryption algorithm is simply p = D (k, C) = (C - k) mod 26

Monoalphabetic Ciphers:

Monoalphabetic cipher is a substitution cipher in which for a given key, the cipher alphabet for each plain alphabet is fixed throughout the encryption process. For example, if 'A' is encrypted as 'D', for any number of occurrences in that plaintext, 'A' will always get encrypted to 'D'.

With only 25 possible keys, the Caesar cipher is far from secure. An increase in the key space can be achieved by allowing an arbitrary substitution, which can improve the security.

In Caesar cipher,

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

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.

Let $p=C=Z_{26}$ and K consists of all possible permutations of the 26 alphabets.

For each permutation $\pi \varepsilon K$, define:

$e_\pi (x)= \pi (x)$

$d_\pi (y)= \pi^{-1}(y)$

where π^{-1} is the inverse permutation. (possible keys= 26!)

For example,

Let π be:

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

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

Plain Text: hello

Cipher text: PGDDL

Plain text: meet me after the toga party

Cipher text: UGGV UG RSVGY VPG VLKR NRYVI

Polyalphabetic cipher:

A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets.

Playfair Cipher:

In Playfair cipher, unlike traditional cipher we encrypt a pair of alphabets(digraphs) instead of a single alphabet. The Playfair algorithm is based on the use of a 5 * 5 matrix of letters constructed using a keyword.

Algorithm:

1. Generate the key square.

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 key square is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table (as the table can hold only 25 alphabets). If the plaintext contains J, then it replaces I.

   In the above example, the key is "monarchy". Thus, the initial entries are ‘m', 'o', 'n', 'a', 'r', 'c', 'h', 'y' followed by remaining characters of a-z (except 'j') in that order.

2. Algorithm to encrypt the plain text: The plaintext is split into pairs of two letters (digraphs). If there is an odd number of letters, a Z is added to the last letter.

   For example:

   PlainText: "instruments"

   After Split: 'in' 'st' 'ru' 'me' 'nt' 'sz'

   <u>Rules for Encryption:</u>

   - If both the letters are in the same column: Take the letter below each one (going back to the top if at the bottom).

For example:

Diagraph: "me"

Encrypted Text: CL

Encryption:

m -> C

e -> L

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

- If both the letters are in the same row: Take the letter to the right of each one (going back to the leftmost if at the rightmost position).

  For example:

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

  Diagraph: "st"

  Encrypted Text: TL

  Encryption:

  s -> T

  t -> L

- If neither of the above rules is true: Form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.

  For example:

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

Diagraph: "nt"

Encrypted Text: RQ

Encryption:

n -> R

t -> Q

For example:

Plain Text: "instrumentsz"

Encrypted Text: GATLMZCLRQTX

Encryption:

i -> g

n -> a

s -> t

t -> l

r -> m

u -> z

m -> c

e -> l

n -> r

t -> q

s -> t

z -> x

Hill Cipher:

Hill cipher is a multilettered substitution cipher based on linear algebra. Each letter is represented by a number modulo 26. Often the simple scheme A = 0, B = 1, …, Z = 25 is used, but this is not an essential feature of the cipher. To encrypt a message, each block of n letters (considered as an n-component vector) is multiplied by an invertible n × n matrix, against modulus 26. To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.

The matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible n × n matrices (modulo 26).

Algorithm:

Let m=3 and plaintext x= (x1, x2, x3), then ciphertext y= (y1, y2, y3) can be calculated as:

(y1, y2, y3) = (x1, x2, x3) (k11 k12 k13)

(k21 k22 k23)

(k31 k32 k33)

For example:

Let k= $\begin{vmatrix} 11 & 8 \\ 3 & 7 \end{vmatrix}$

Plaintext: july

ju= (9 20) & ly= (11 24)

So, (9 20) $\begin{vmatrix} 11 & 8 \\ 3 & 7 \end{vmatrix}$

gives (3 4) i.e DE

(11 24) $\begin{vmatrix} 11 & 8 \\ 3 & 7 \end{vmatrix}$

gives (11 22) i.e. LW

Hence, the ciphertext is DELW.

For decryption, find k^{-1} and multiply with the ciphertext in the form of matrix.

To find the inverse of a 2x2 matrix: swap the positions of a and d, put negatives in front of b and c, and divide everything by the determinant (ad-bc).

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

determinant

Example 2:

Plaintext: act

Key: GYBNQKURP

Ciphertext: POH

Encryption: We have to encrypt the message 'ACT' (n=3). The key is 'GYBNQKURP' which can be written as the nxn matrix:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

The message 'ACT' is written as vector:

$$\begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$$

The enciphered vector corresponds to ciphertext of 'QRT'.

Decryption: To decrypt the message, we turn the ciphertext back into a vector, then simply multiply by the inverse matrix of the key matrix (IFKVIVVMI in letters). The inverse of the matrix used in the previous example is:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}^{-1} \equiv \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \pmod{26}$$

For the previous Ciphertext 'QRT', we obtain act after decryption.

One Time Pad:

In cryptography, a one-time pad is a system in which a private key generated randomly is used only once to encrypt a message. Messages encrypted with keys based on randomness have the advantage that there is theoretically no way to "break the code" by analyzing the messages. Each encryption is unique and bears no relation to the next encryption, so patterns between the messages cannot be detected. When a message is to be sent, the sender uses the secret key to encrypt each character, one at a time. With a one-time pad, however, the decrypting party must have access to the same key used to encrypt the message and this raises the problem of how to get the key to the decrypting party safely. The key used in a one-time pad is called a secret key because if it is revealed, the messages encrypted with it can easily be deciphered.

Typically, a one-time pad is created by generating a string of characters or numbers that will be at least as long as the longest message that may be sent. This string of values is generated in some random fashion. If the key is (1) truly random, (2) at least as long as the plaintext, (3) never reused in whole or in part, and (4) kept completely secret, then the resulting ciphertext will be impossible to decrypt or break.

Vigenere Cipher:

This scheme of cipher uses a text string (say, a word) as a key, which is then used for doing a number of shifts on the plaintext.

For example, let's assume the key is 'point'. Each alphabet of the key is converted to its respective numeric value: In this case,

p → 16, o → 15, i → 9, n → 14, and t → 20.

Thus, the key is: 16 15 9 14 20.

Process of Vigenere Cipher

The sender and the receiver decide on a key. Say 'point' is the key. Numeric representation of this key is '16 15 9 14 20'.

The sender wants to encrypt the message, say 'attack from south east'. He will arrange plaintext and numeric key as follows:

a	t	t	a	c	k	f	r	o	m	s	o	u	t	h	e	a	s	t
16	15	9	14	20	16	15	9	14	20	16	15	9	14	20	16	15	9	14

The sender now shifts each plaintext alphabet by the number written below it to create ciphertext as shown below:

a	t	t	a	c	k	f	r	o	m	s	o	u	t	h	e	a	s	t
16	15	9	14	20	16	15	9	14	20	16	15	9	14	20	16	15	9	14
Q	I	C	O	W	A	U	A	C	G	I	D	D	H	B	U	P	B	H

Here, each plaintext character has been shifted by a different amount and that amount is determined by the key. The key must be less than or equal to the size of the message.

For decryption, the receiver uses the same key and shifts received ciphertext in reverse order to obtain the plaintext.

Q	I	C	O	W	A	U	A	C	G	I	D	D	H	B	U	P	B	H
16	15	9	14	20	16	15	9	14	20	16	15	9	14	20	16	15	9	14
a	t	t	a	c	k	f	r	o	m	s	o	u	t	h	e	a	s	t

Variants of Vigenere Cipher

There are two special cases of Vigenere cipher:

- The keyword length is same as plaintext message. This case is called Vernam Cipher. It is more secure than typical Vigenere cipher.
- Vigenere cipher becomes a cryptosystem with perfect secrecy, which is called One-time pad.

Perfect secrecy is the concept that given a ciphertext from a perfectly secure encryption system, absolutely nothing will be revealed about the plaintext by the ciphertext.

Transposition Techniques:

In transposition technique, the identity of the characters remains unchanged, but their positions are changed to create the ciphertext. Transposition Techniques are based on the permutation of the plain-text instead of substitution.

Rail Fence Cipher:

Rail fence is the simplest transposition cipher technique in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows. i.e. first, we write the message in a zigzag manner then read it out direct row-wise to change it to cipher-text.

For example,

Plaintext: meet me after the toga party

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

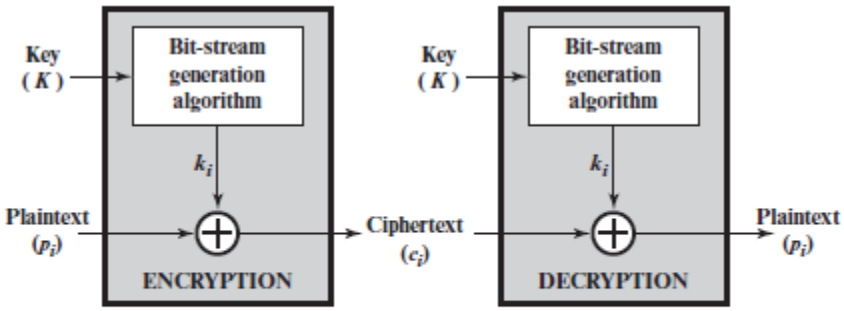
Ciphertext: MEMATRHTGPRYETEFETEOAAT

Modern Ciphers:

In Modern ciphers, digital data is represented in strings of binary digits (bits) unlike alphabets. Modern cryptosystems need to process these binary strings to convert into another binary string. Based on how these binary strings are processed, a symmetric encryption scheme can be classified into stream cipher and block cipher.

Stream cipher:

A stream cipher is the mechanism that encrypts a digital data stream one bit or one byte at a time. In this scheme, the plaintext is processed one bit at a time i.e. one bit of plaintext is taken, and a series of operations are performed on it to generate one bit of ciphertext.

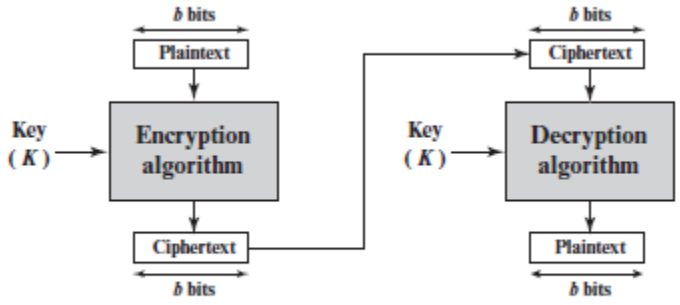


(a) Stream cipher using algorithmic bit-stream generator

For practical reasons, the bit-stream generator must be implemented as an algorithmic procedure, so that the cryptographic bit stream can be produced by both users. In this approach, the bit-stream generator is a key-controlled algorithm and must produce a bit stream that is cryptographically strong. That is, it must be computationally impractical to predict future portions of the bit stream based on previous portions of the bit stream. The two users need only share the generating key, and each can produce the keystream.

Block Cipher:

A block cipher is the mechanism in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length. The number of bits in a block is fixed. Typically, a block size of 64 or 128 bits is used. As with a stream cipher, the two users share a symmetric encryption key.



(b) Block cipher

Comparison between Block Cipher and Stream Cipher:

S.N.	BLOCK CIPHER	STREAM CIPHER
1	Block Cipher Converts the plain text into cipher text by taking plain text's block at a time.	Stream Cipher Converts the plaint text into cipher text by taking 1 byte of plain text at a time.
2	Block cipher uses either 64 bits or more than 64 bits.	Stream cipher uses 8 bits.
3	Simple design	Complex comparatively
4	Reversing encrypted text is hard.	Reversing encrypted text is comparatively easy.
5	Suitable for transmission of bulk data.	Suitable for audio and video streaming.

Comparison between Symmetric cipher and Asymmetric cipher:

Basis for Comparison	**Symmetric cipher**	**Asymmetric cipher**
Basic	Symmetric cipher uses a single key for both encryption and decryption, called as secret key.	Asymmetric cipher uses a different key for encryption and decryption, namely public key and private key respectively.
Performance	Symmetric encryption is fast in execution.	Asymmetric Encryption is slow in execution due to the high computational burden.
History	Old technique	Relatively new.
Security	Less Secure	More Secure
Cipher Key	Secret key should be delivered to the receiver.	Key delivery is not required.