Types of Attacks

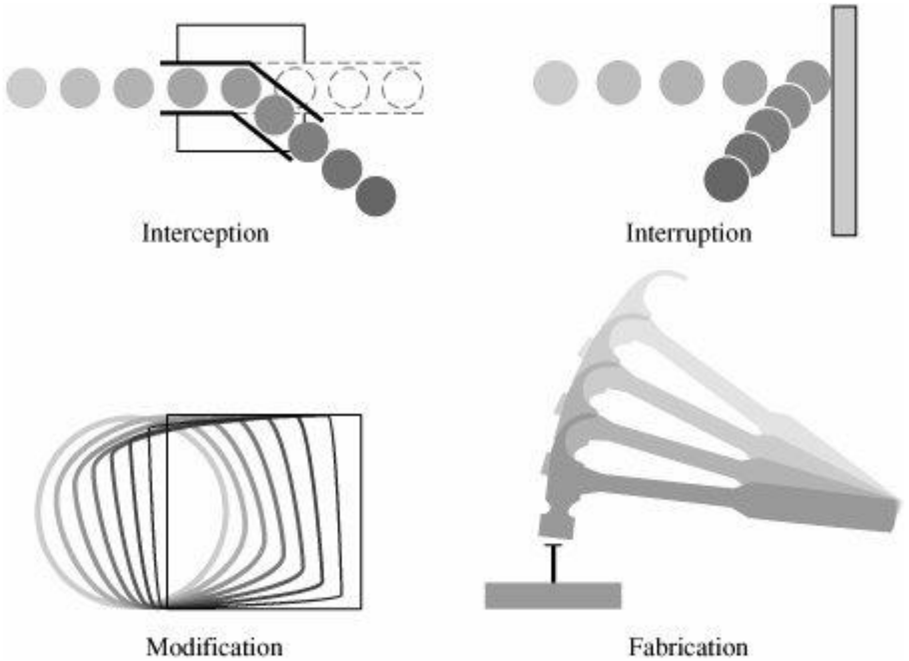
Weaknesses or Vulnerabilities: is a weakness in the security system, for example, in procedures, design, or implementation, that might be exploited to cause loss or harm.

A **threat** to a computing system is a set of circumstances that has the potential to cause loss or harm.

Attacks:

Consider the steps involved in sending messages from a **sender**, S, to a **recipient**, R. If S entrusts the message to T, who then delivers it to R, T then becomes the **transmission medium**. If an outsider, O, wants to access the message (to read, change, or even destroy it), we call O an **interceptor** or **intruder**. Any time after S transmits it via T, the message is vulnerable to exploitation, and O might try to access the message in any of the following ways:

1. Block it, by preventing its reaching R, thereby affecting the availability of the message.
2. Intercept it, by reading or listening to the message, thereby affecting the confidentiality of the message.
3. Modify it, by seizing the message and changing it in some way, affecting the message's integrity.
4. Fabricate an authentic-looking message, arranging for it to be delivered as if it came from S, thereby also affecting the integrity of



Interception

Interruption

Modification

Fabrication

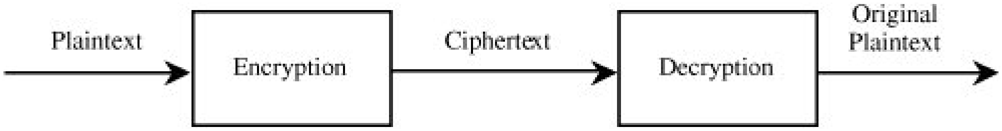
We use a **control** as a protective measure. That is, a control is an action, device, procedure, or technique that removes or reduces a vulnerability

The original form of a message is known as **plaintext**, and the encrypted form is called **ciphertext**

The word c***ryptography*** means hidden writing, and it refers to the practice of using ***encryption*** to conceal text.

A **cryptanalyst** studies encryption and encrypted messages, hoping to find the hidden meanings.

Cryptology: Is the research into and study of encryption and decryption; it includes both cryptography and cryptanalysis.



We use this formal notation to describe the transformations between plaintext and ciphertext. For example, we write C = E(P) and P = D
(C), where C represents the ciphertext, E is the encryption rule, P is the plaintext, and D is the decryption rule. What we seek is a cryptosystem for which
P = D(E(P)).

In other words, we want to be able to convert the message to protect it from an intruder, but we also want to be able to get the original message back so that the receiver can read it properly.

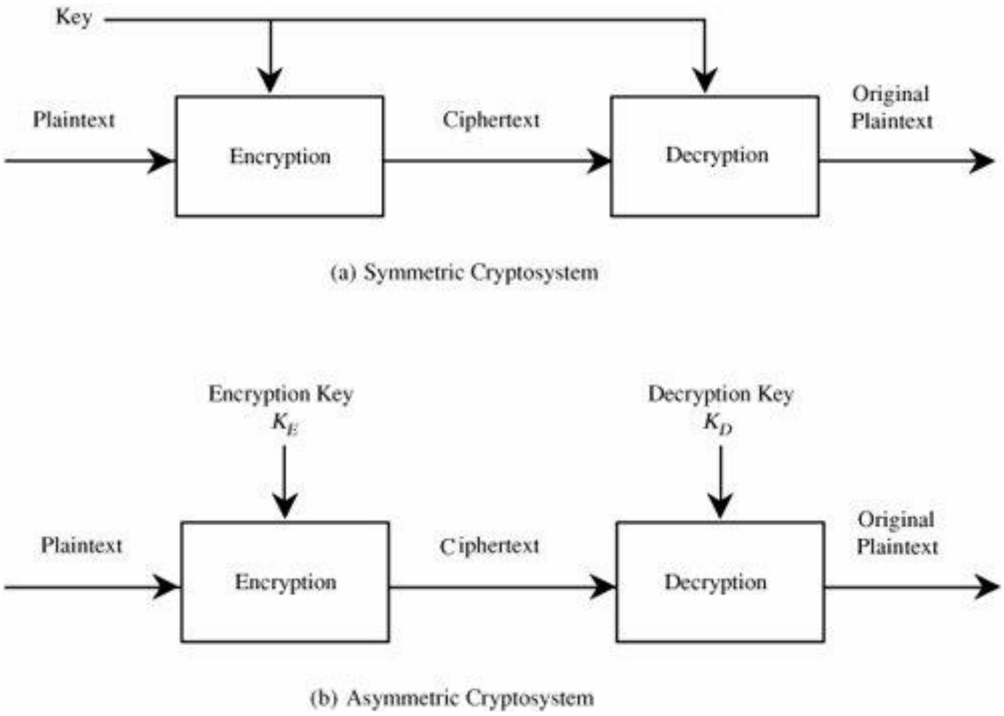
Encryption Algorithms

The cryptosystem involves a set of rules for how to encrypt the plaintext and how to decrypt the ciphertext.

The cryptosystem involves a set of rules for how to encrypt the plaintext and how to decrypt the ciphertext.

The encryption and decryption rules, called **algorithms**, often use a device called a **key**, denoted by K, so that the resulting ciphertext depends on the original plaintext message, the algorithm, and the key value.

We write this dependence as C = E(K, P). Essentially, E is a set of encryption algorithms, and the key K selects one specific algorithm from the set. We see later in this chapter that a cryptosystem, such as the Caesar cipher, is keyless
but that keyed encryptions are more difficult to break.



(a) Symmetric Cryptosystem

(b) Asymmetric Cryptosystem

Cryptanalysis

A cryptanalyst's is trying to break an encryption

Breakable Encryption

An encryption algorithm is called breakable when, given enough time and data, an analyst can determine the algorithm.

The Caesar Cipher

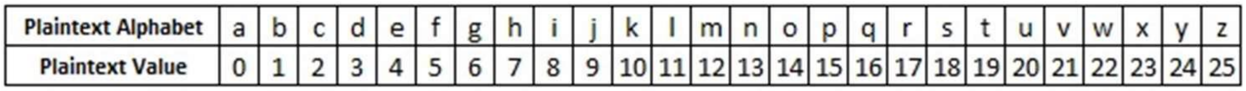
The **Caesar cipher** has an important place in history. Julius Caesar is said to have been the first to use this scheme, in which each letter is translated to the letter a fixed number of places after it in the alphabet. Caesar used a shift of 3, so plaintext letter pi was enciphered as cipher text letter ci by the rule

ci = E(pi) = pi + 4

suppose that the key e is chosen to be the permutation which maps each letter to the one which is three

positions to its right, as shown below

e =



Plaintext Alphabet	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
Plaintext Value	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

P: 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

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

Encryption

4

Enter the message: HELLOWORLD

Encrypted message: LIPPSASVPH

Decryption

4

Message to decrypt: LIPPSASVPH

Decrypted message: HELLOWORLD

EX1

K: LOVE

P: Al MUSTAQBAL

P: 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

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

P: ALMUSTAQBAL → E: LIJTRSLPOLI