Types of Attacks

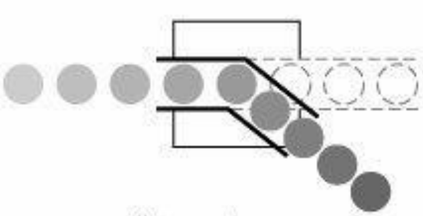
Weaknesses or Vulnerabilities: is a weakness in the security system, for example, in procedures, design, or implementation, that might be exploited to cause loss or harm.

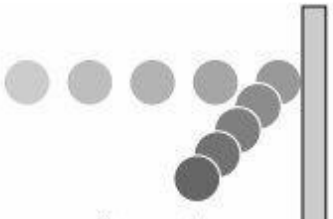
A **threat** to a computing system is a set of circumstances that has the potential to cause loss or harm.

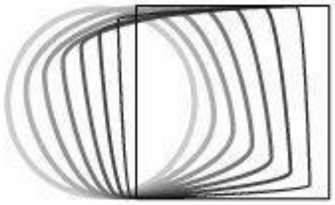
Attacks:

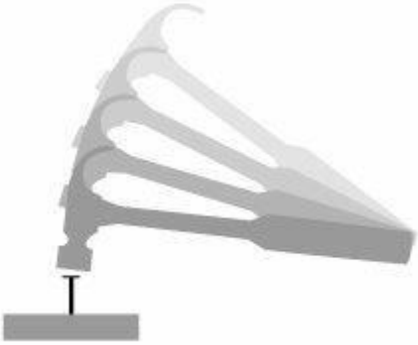
Consider the steps involved in sending messages from a **sender**, S, to a **recipient**, R. If S entrusts the message to T, who then delivers it to R, T then becomes the **transmission medium**. If an outsider, O, wants to access the message (to read, change, or even destroy it), we call O an **interceptor** 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

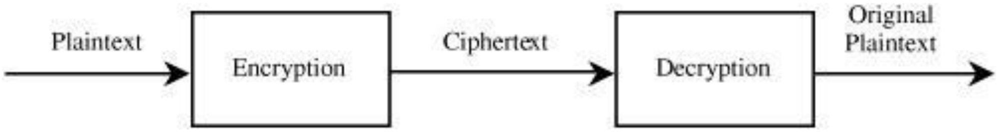
We use a **control** as a protective measure. That is, a control is an action, device, procedure, or technique that removes or reduces a vulnerability

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

The word ***cryptography*** 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.

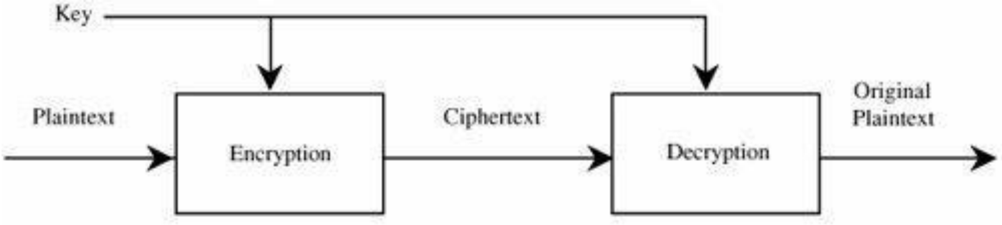
Encryption Algorithms

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

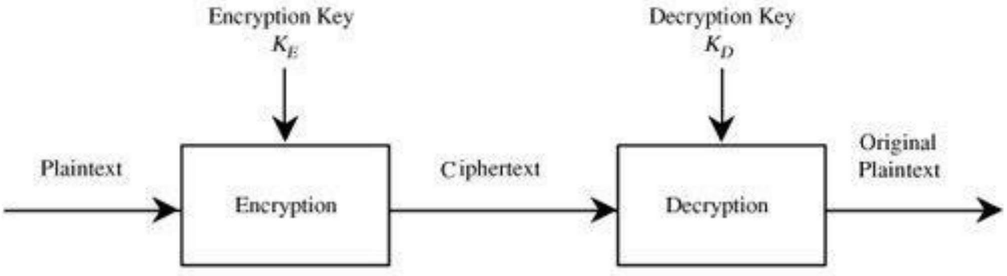
The cryptosystem involves a set of rules for how to encrypt the plaintext and how to decrypt the ciphertext.

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

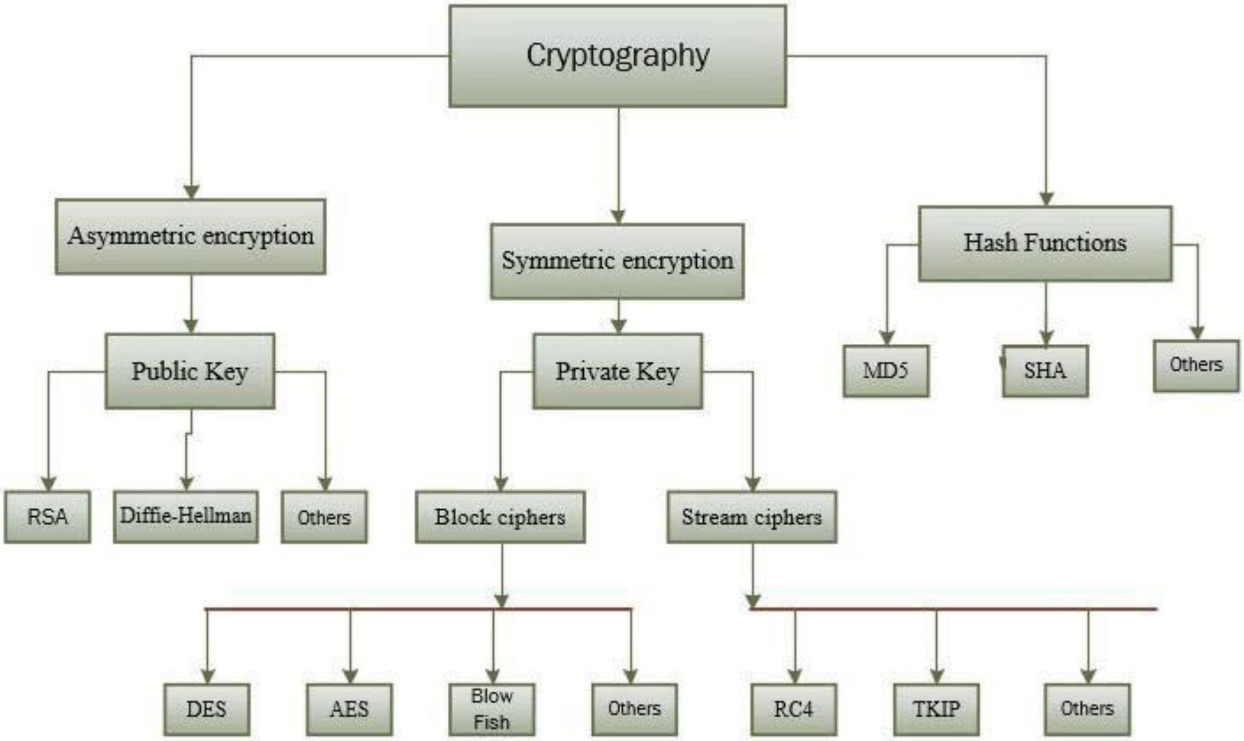
A cryptanalyst's is trying to break an encryption

Breakable Encryption

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

<u>Classification of Cryptography</u>

- Number of keys used
  - Hash functions: no key
  - Symmetric encryption (Private Key): one key
  - Asymmetric encryption (Public Key): two keys - public, private
- Type of encryption operations used
  - substitution / transposition / product
- Way in which plaintext is processed
  - block / stream

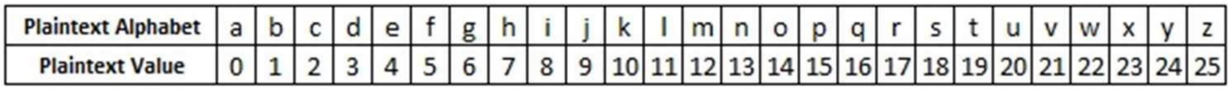


The Caesar Cipher

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 + 3

suppose that the key e is chosen to be the permutation which maps each letter to the one which is four positions to its right, as shown in example below



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

Ex1:

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

Enter the message: HELLOWORLD
Encrypted message: LIPPSASVPH →

Decryption

Message to decrypt: LIPPSASVPH
Decrypted message: HELLOWORLD

Ex2 with key:

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

Ex3: encrypt the following message using Caesar cipher:

Plain: meet me after the toga party

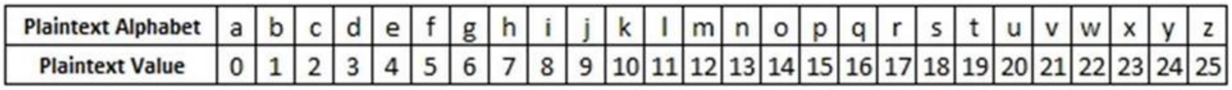
Cipher: PHHW PH DIWHU WKH WRJD SDUWB

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:

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: 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



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

Then the algorithm can be expressed as follows. For each plaintext letter *p*, substitute the ciphertext letter *C*:

We define *a* mod *n* to be the remainder when *a* is divided by *n*. For example, 11mod 7 = 4

$\boldsymbol{C = \mathrm{E}(3, p) = (p + 3) \bmod 26}$

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

$\boldsymbol{C = \mathrm{E}(k, p) = (p + k) \bmod 26}$

where *k* takes on a value in the range 1 to 25. The decryption algorithm is simply

$\boldsymbol{p = \mathrm{D}(k, C) = (C - k) \bmod 26}$

M=12, 12+3 mod 26= 15=P

E=4,4+3 mod 26= 7=H

Y=24,24+3 mod 26= 27 mod 26=1=B

Ex4: decrypt the following message (**NHBZRUG**) using Caesar cipher:

p = (C - k) mod 26

p_1=N (13-3) mod 26=10=k
p_2=H (7-3) mod 26=4=e
p_3= B (1-3) mod 26=24= y
p_4= Z (25-3) mod 26=22=w
p_5= R (17-3) mod 26=14=o
p_6= U (20-3) mod 26=17=r
p_7= G (6-3) mod 26=3=d
plaintext is **keyword**

Terminology

1. **Cryptography**: is probably the most important aspect of communications security and is becoming increasingly important as a basic building block for computer security.
2. **Cryptography: - Study of encryption principles/methods**
3. **Cryptology** is the science and study of systems for secret communications. **Cryptography methods** applied by authorized information sharers to design and develop encryption schemes in order to ensure confidentiality of information.
4. **Crypt-Analysis** (mathematical and statistical attempts by unauthorized persons to break cipher in order to reveal the meaning of the underlying protected data).
5. **Confidentiality** is the concealment of information or resources.
6. **Authenticity** is the identification and assurance of the origin of information.
7. **Integrity** refers to the trustworthiness of data or resources in terms of preventing improper and unauthorized changes.
8. **Availability** refers to the ability to use the information or resource desired.
9. **Plaintext:** This is the original intelligible message or data that is fed into the algorithm as input
10. **Plaintext: - Original message**
11. **Ciphertext:** This is the scrambled message produced as output.
12. **Ciphertext: - Coded message**
13. **Secret key:** The secret key is also input to the encryption algorithm.
14. **Block Cipher**: processes the input one block of elements at a time, producing an output block for each input block.
15. **Stream Cipher:** processes that encrypt a digital data stream one bit or one byte at a time.
16. **Encryption algorithm:** The encryption algorithm performs various substitutions and transformations on the plaintext.
17. **Decryption algorithm:** This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

18. **Cipher: - Algorithm for transforming plaintext to ciphertext**
19. **Key: - Info used in cipher known only to sender/receiver**
20. **Encrypt: - Converting plaintext to ciphertext**
21. **Decrypt: - Recovering ciphertext from plaintext**
22. **Cryptology: -Field of both cryptography and cryptanalysis**
23. **Cryptanalysis (codebreaking): - Study of principles/ methods of deciphering ciphertext without knowing key**