

UNIT 4

UNIT 4

CYRPTOGRAPHY

Cryptology Terminology –
Cipher methods –
Cryptographic Algorithms –
Cryptographic tools –
Attacks on cryptosystems –
Physical Security.

- Cryptography is the study and practice of techniques for **secure communication** in the presence of **third parties** called **adversaries**.
- It deals with **developing and analyzing protocols** which prevents malicious third parties from retrieving information being shared between two entities thereby following the various aspects of information security.
- **Secure Communication** refers to the scenario where the message or data shared between two parties can't be accessed by an adversary.
- In Cryptography, an Adversary is a **malicious entity**, which aims to retrieve precious information or data thereby undermining the principles of information security.

Who are adversaries in cyber security?

- In its most simplistic definition, a cyber adversary is someone or a group that intends to perform malicious actions against other cyber resources

Principles of modern-day cryptography

Data Confidentiality, Data Integrity, Authentication and Non-repudiation are core

1. **Confidentiality** refers to certain **rules and guidelines** usually executed under confidentiality agreements which ensure that the information is restricted to certain people or places.
2. **Data integrity** refers to maintaining and making sure that the **data stays accurate and consistent** over its entire life cycle.
3. **Authentication** is the process of making sure that the piece of data being **claimed** by the user belongs to it.
4. **Non-repudiation** refers to ability to make sure that a person or a party associated with a contract or a communication cannot **deny the authenticity of their signature** over their document or the sending of a message.

- Consider two parties **Alice and Bob**.
- Now, Alice wants to send a message **m** to Bob over a secure channel.
- So, what happens is as follows.
- The sender's message or sometimes called the Plaintext, is converted into an **unreadable form** using a **Key k**.
- The resultant text obtained is called the **Ciphertext**.
- This process is known as **Encryption**.
- At the time of receipt, the Ciphertext is converted back into the plaintext using the same Key k, so that it can be read by the receiver.
- This process is known as **Decryption**.

Alice (Sender) Bob (Receiver)

$C = E(m, k)$ -----> $m = D(C, k)$

$M \rightarrow$ Text

$C \rightarrow$ Ciphertext

$E \rightarrow$ Encryption algorithms

$D \rightarrow$ Decryption algorithms

- Let's consider the case of **Caesar Cipher** or **Shift Cipher** as an example.
- As the name suggests, in **Caesar Cipher** each character in a word is replaced by another **character** under some defined rules.
- Thus, if A is replaced by D, B by E and so on.
- **ABCDEFGHIJKLMNOPQRSTUVWXYZ**
- Shift 3 ---remove **ABC**
- **ABC** ----- **DEFGHIJKLMNOPQRSTUVWXYZ**
- Then, each character in the word would be shifted by a position of 3.
- For example:

```
Plaintext : Geeksforgeeks
Ciphertext : Jhhnvirujhhnv
```


- Note that even if the adversary knows that the cipher is based on Caesar Cipher, it cannot predict the plaintext as it doesn't have the key in this case which is to shift the characters back by three places.

Cryptology Terminology

- Cryptography is an important aspect when we deal with **network security**.
- ‘**Crypto**’ means **secret or hidden**.
- **Cryptography** is the science of **secret writing** with the intention of keeping the data secret.
- **Cryptanalysis**, on the other hand, is the science or sometimes the **art of breaking cryptosystems**.
- These both terms are a **subset** of what is called as **Cryptology**.

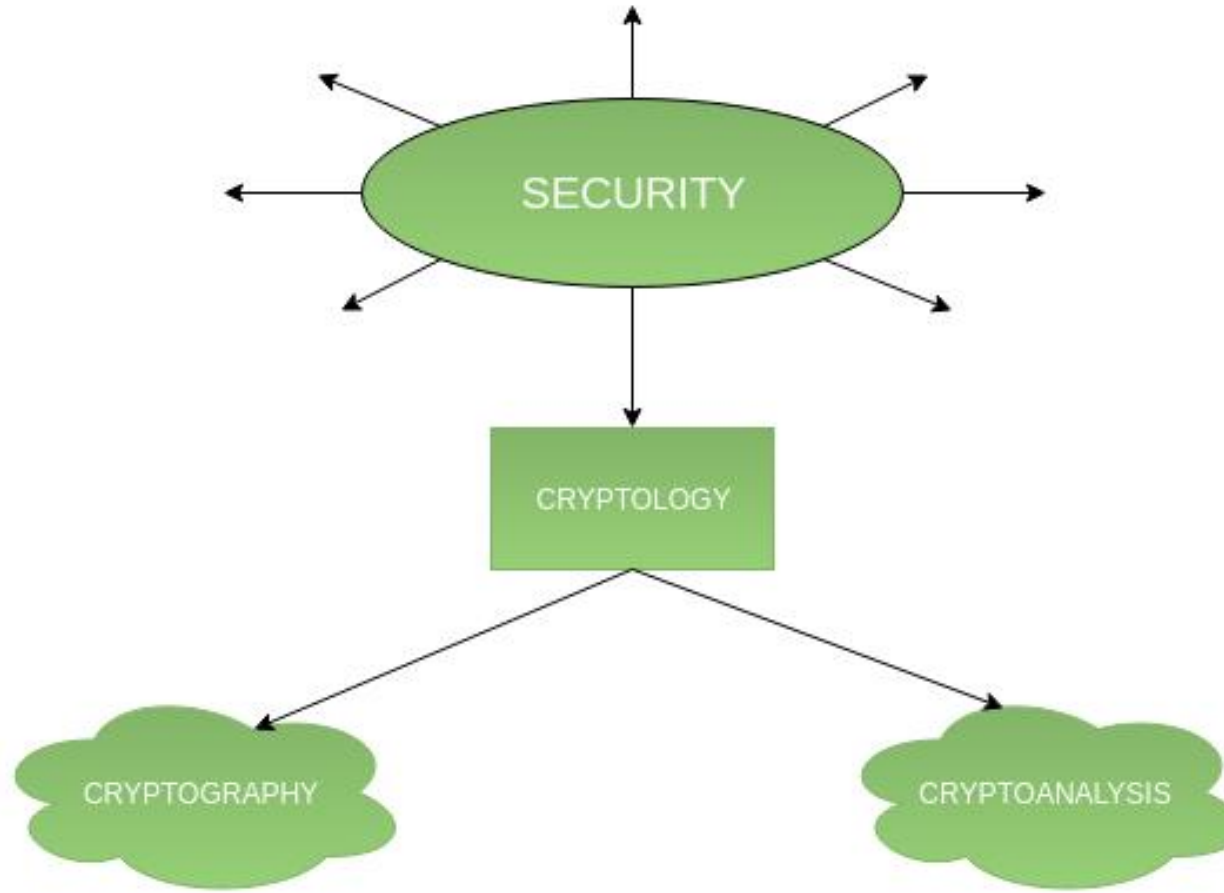
Cryptology Terminology

- Classification –
- The flowchart depicts that cryptology is only one of the factors involved in securing networks.
- **Cryptology** refers to **study of codes**, which involves both writing (cryptography) and solving (cryptanalysis) them.
- **CRYPTOLOGY --- cryptography + cryptanalysis**
- Below is a classification of the crypto-terminologies and their various types.

Cryptology Terminology

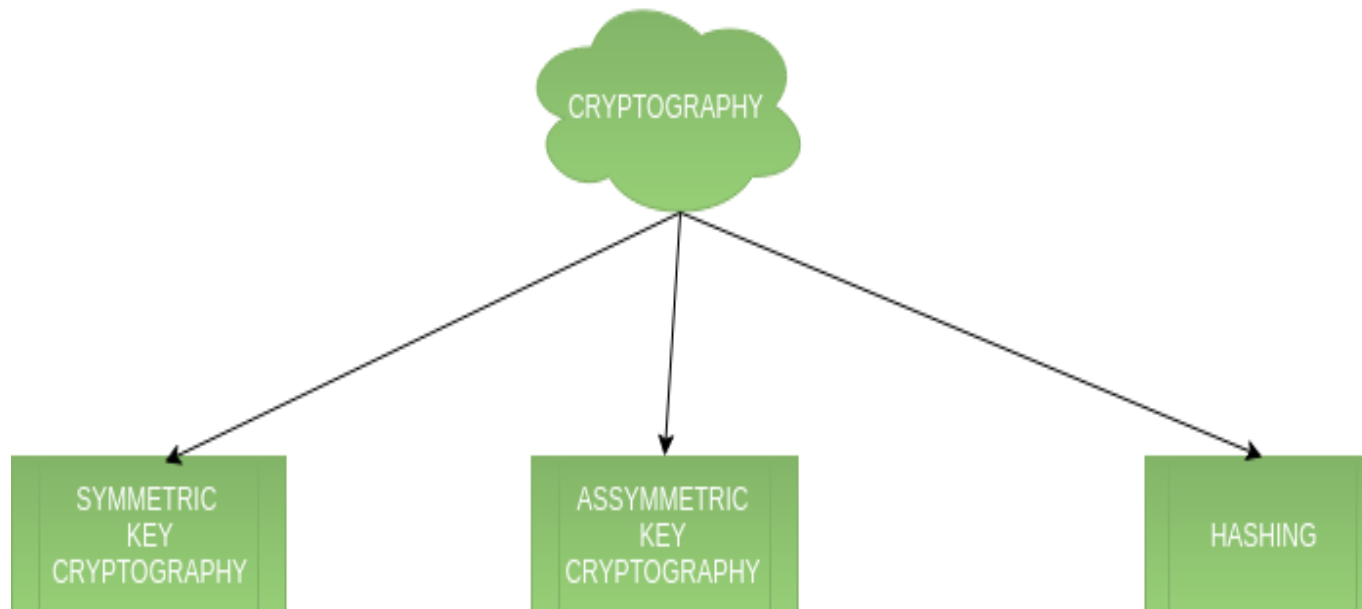
- Algorithm
- Cipher or cryptosystems
- Cipher text or Cryptogram
- Code
- Decipher
- Encipher
- Key or Cryptovariable
- Keyspace
- Link encryption
- Plain text or clear text
- Steganography
- Work factor

Cryptology Terminology



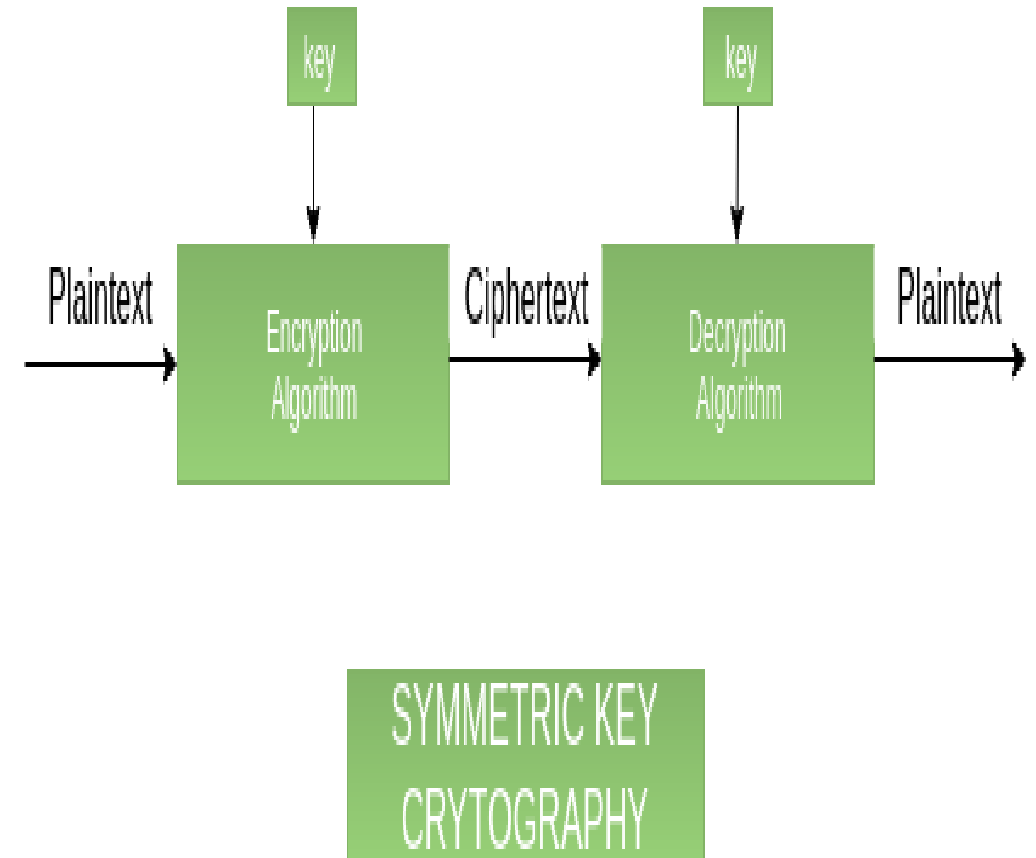
Cryptology Terminology

- 1. Cryptography –Cryptography is classified into symmetric cryptography, asymmetric cryptography and hashing.
- Below are the description of these types.



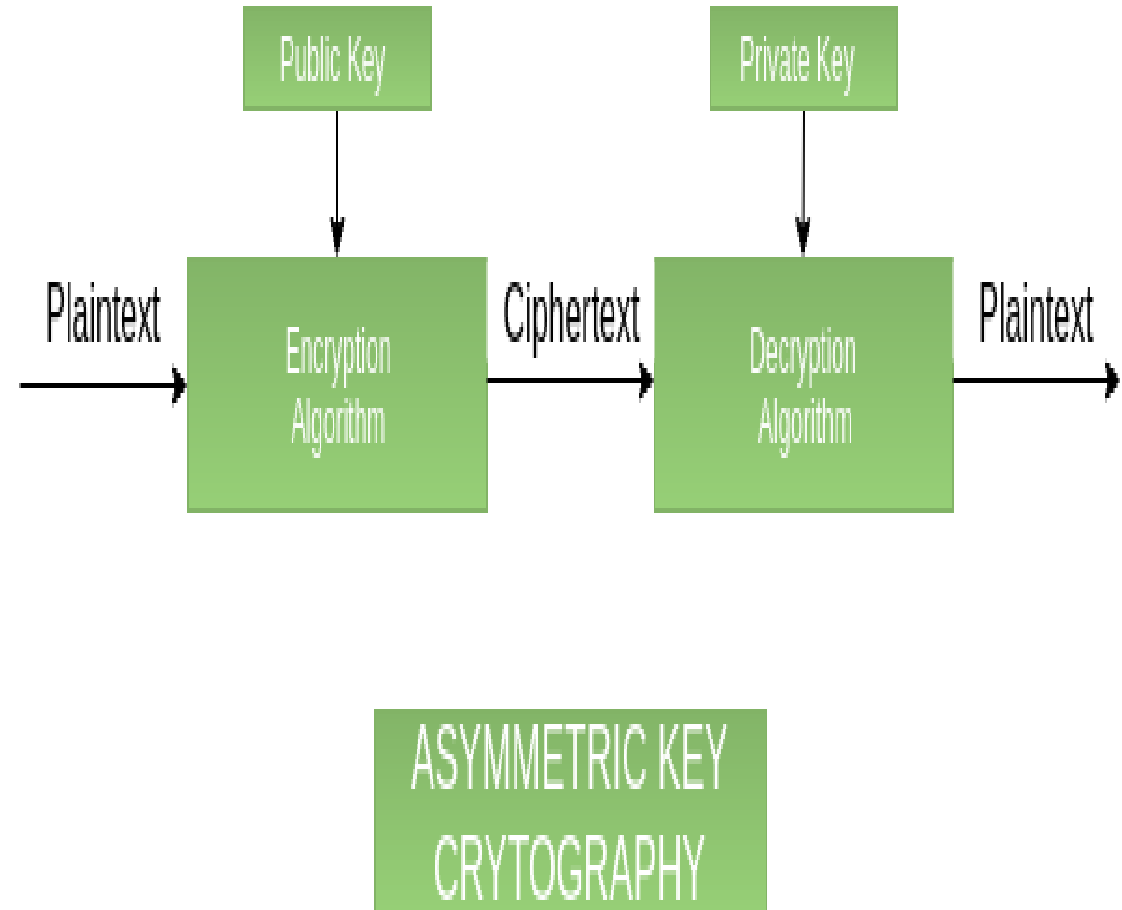
Symmetric key cryptography

- It involves usage of **one secret key** along with encryption and decryption algorithms which help in securing the contents of the message.
- The strength of symmetric key cryptography depends upon the **number of key bits**.
- It is relatively **faster** than asymmetric key cryptography.
- There arises a **key distribution problem** as the key has to be transferred from the sender to receiver through a secure channel.



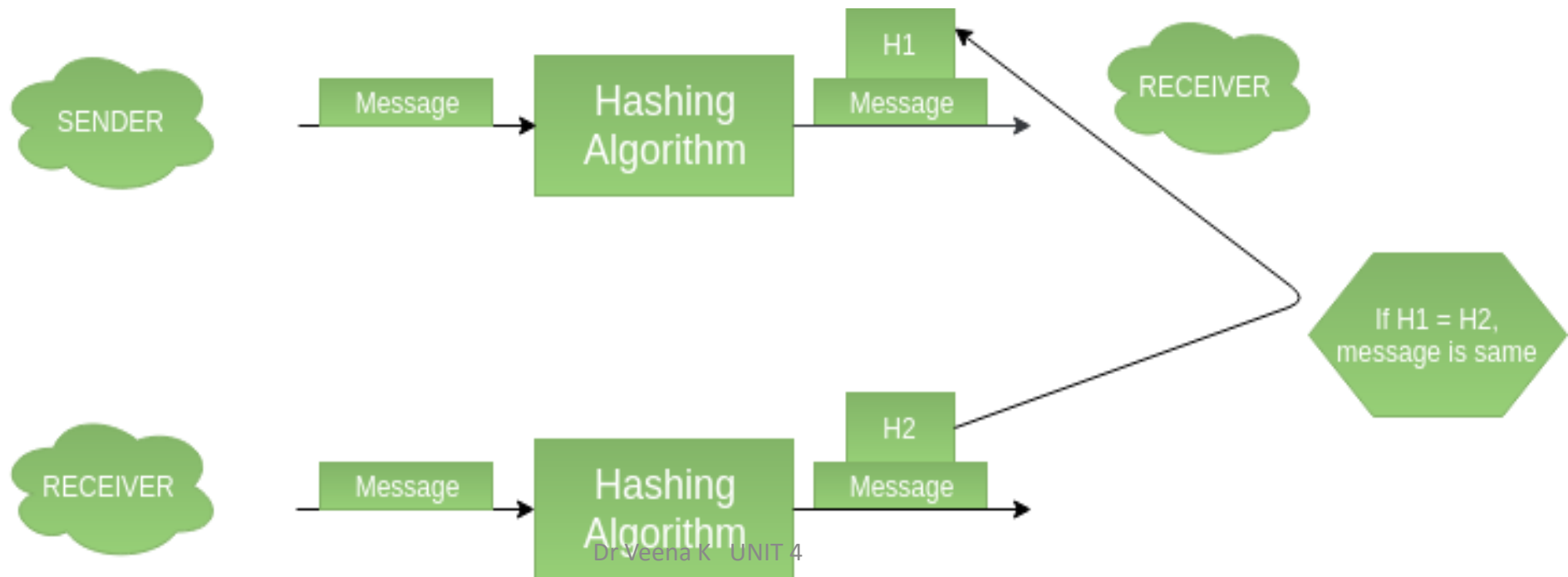
Asymmetric key cryptography

- It is also known as public key cryptography because it involves usage of a public key along with secret key.
- It solves the problem of key distribution as both parties use different keys for encryption/decryption.
- It is not feasible to use for decrypting bulk messages as it is very slow compared to symmetric key cryptography.



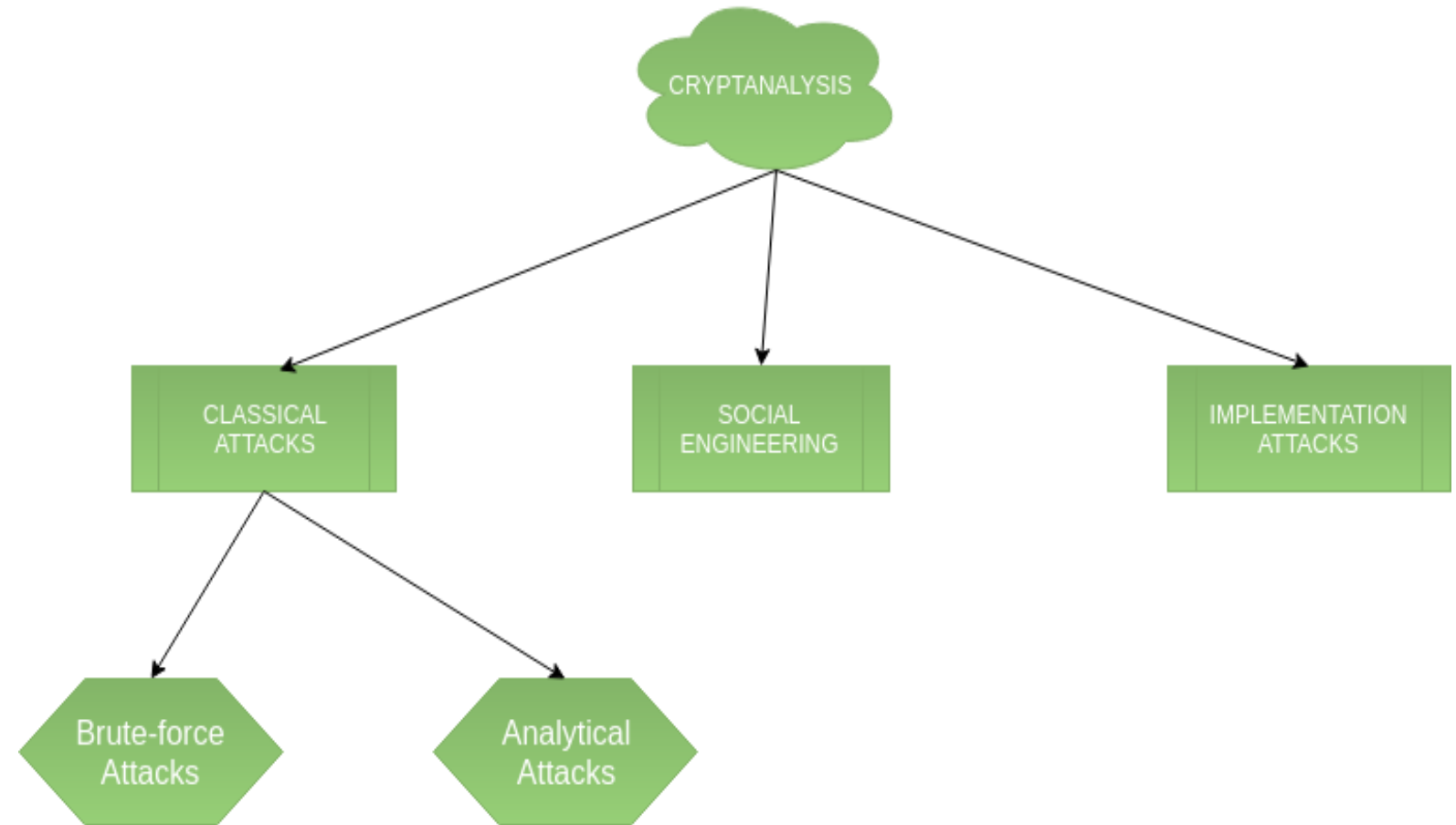
Hashing

- It involves taking the **plain-text** and **converting** it to a **hash value of fixed size by a hash function**.
- This process ensures integrity of the message as the hash value on both, sender\'s and receiver\'s side should match if the message is unaltered.



Cryptanalysis

1. Classical attacks
2. Social Engineering attack
3. Implementation attacks



Classical attacks

It can be divided into

- a) Mathematical analysis and
- b) Brute-force attacks.

Brute-force attacks runs the encryption algorithm for all possible cases of the keys until a match is found. Encryption algorithm is treated as a black box.

Analytical attacks are those attacks which focuses on breaking the cryptosystem by analysing the internal structure of the encryption algorithm.

Social Engineering attack

- It is something which is dependent on the human factor.
- **Tricking** someone to reveal their passwords to the attacker or allowing access to the restricted area comes under this attack.
- People should be cautious when revealing their passwords to any third party which is not trusted.

Implementation attacks

- Implementation attacks such as **side-channel analysis** can be used to obtain a secret key.
- They are relevant in cases where the attacker can obtain physical access to the cryptosystem.

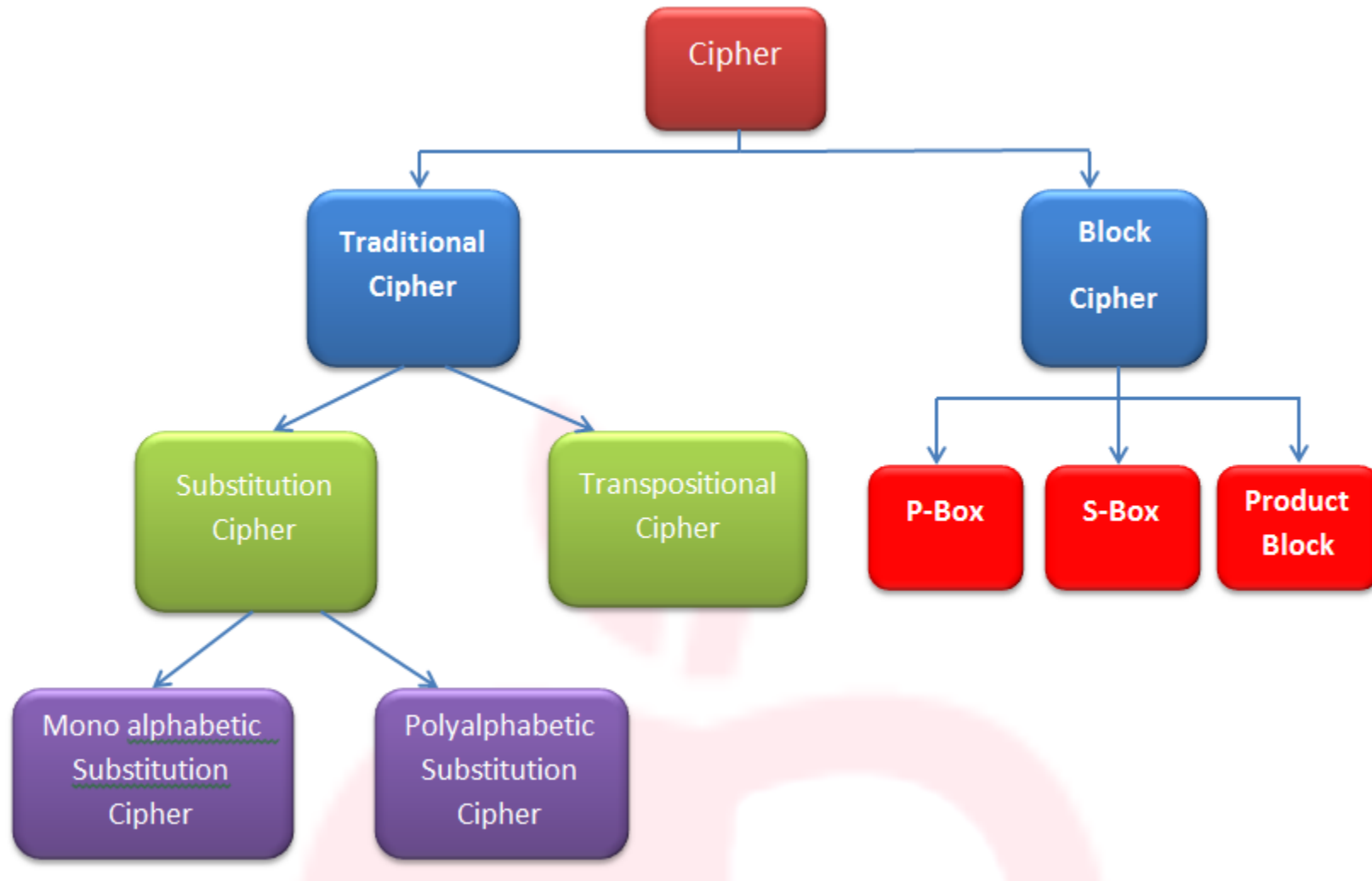
Cipher methods

- Ciphers, also called encryption algorithms, are systems for encrypting and decrypting data.
- A cipher converts the original message, called plaintext, into ciphertext using a key to determine how it is done.

Cipher Methods (As per syllabus)

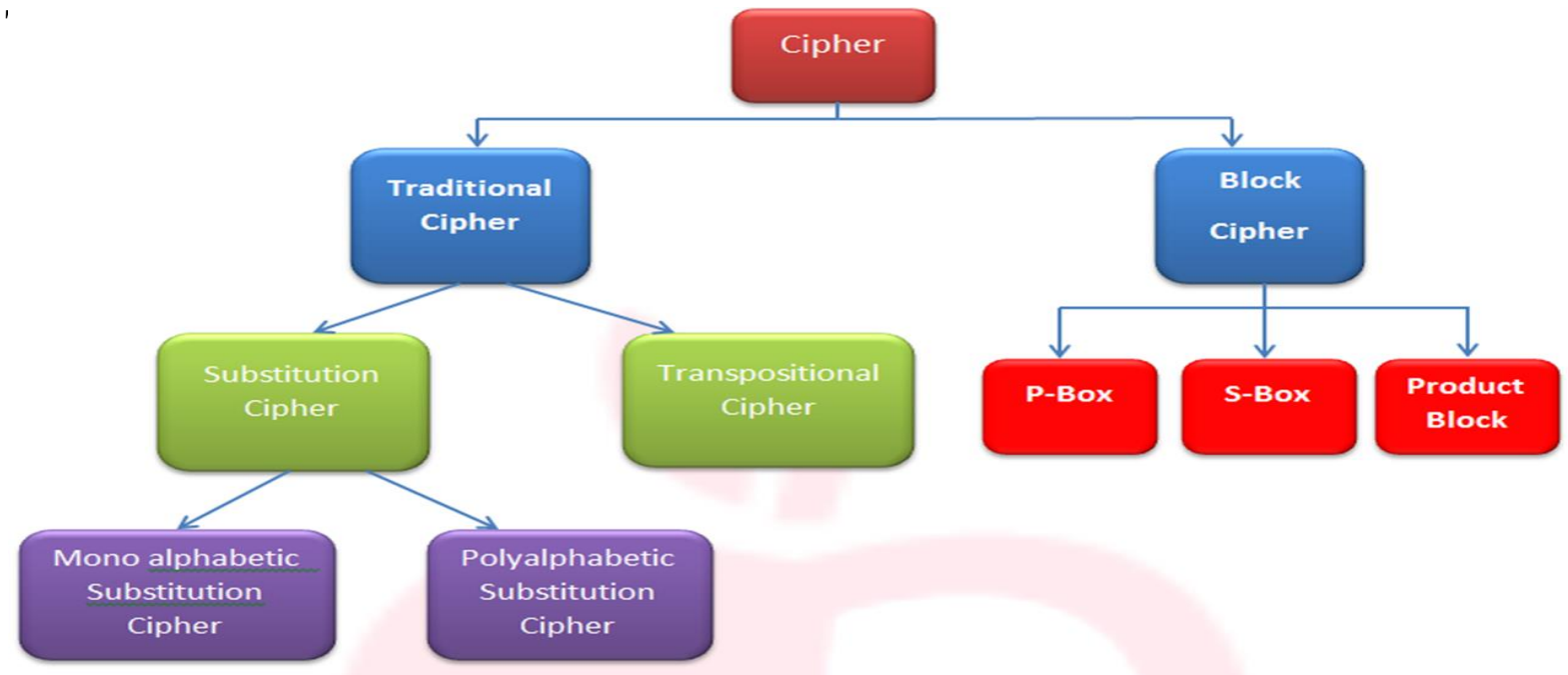
- Substitution Cipher
- Transposition cipher
- Exclusive OR
- Vernam Cipher
- Book or Running key cipher
- Hash Function

Cipher methods



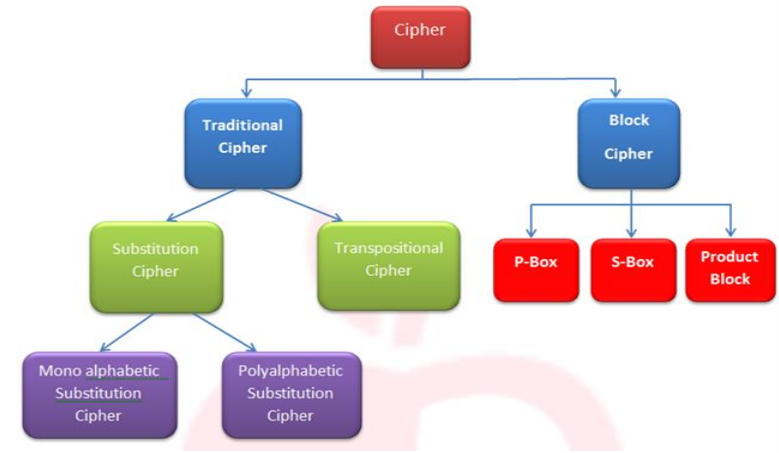
Cipher methods

- Types of Ciphers:
- There are mainly Two Types of Ciphers in Cryptography:
- 1. Traditional Cipher
 - Traditional Cipher – It is the earliest and simplest type of cipher in which a single character considers as the unit of data to encrypt. '



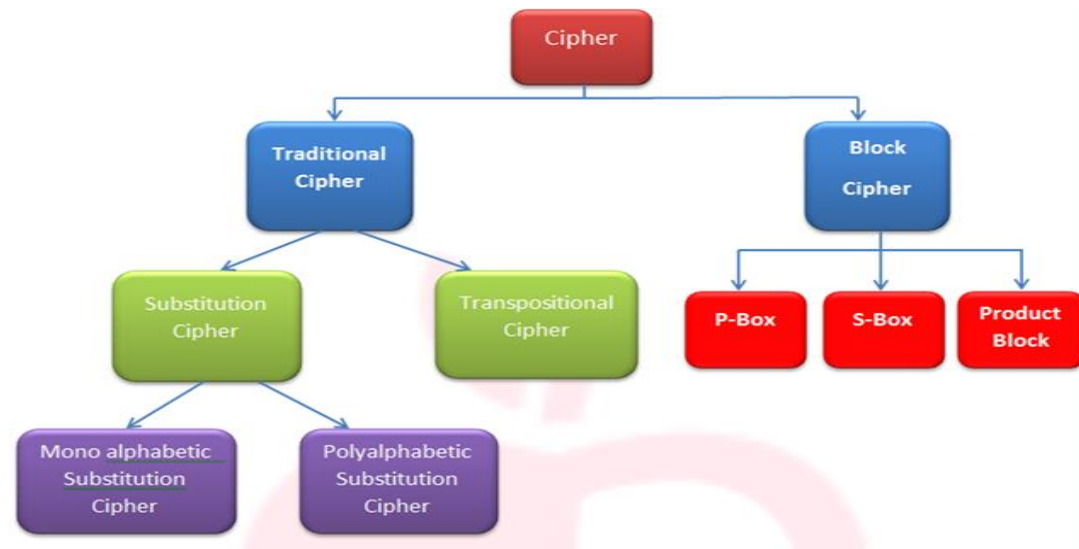
Cipher methods

- Types of Substitution Cipher:
 - In Substitution Cipher, each character is replaced by another character.
 - It is again of two types:
 - Monoalphabetic Substitution Cipher – In this cipher, a character in plain text is always replaced by a fixed character in the ciphertext irrespective of the position of the character in the plain text.
 - Polyalphabetic Substitution Cipher – In this cypher, a character in the plain text is replaced by another character in the ciphertext depending on the position of the original character in the plain text.
- In this case, the relationship between a plain text character and a ciphertext character is one-to-many.



Cipher methods

- Transposition Cipher –
- In Transposition Cipher, the characters retain their plain text form but change their position to create the ciphertext.
- The organized text in a two-dimensional table and a key is used for interchanging the columns.



Cipher methods

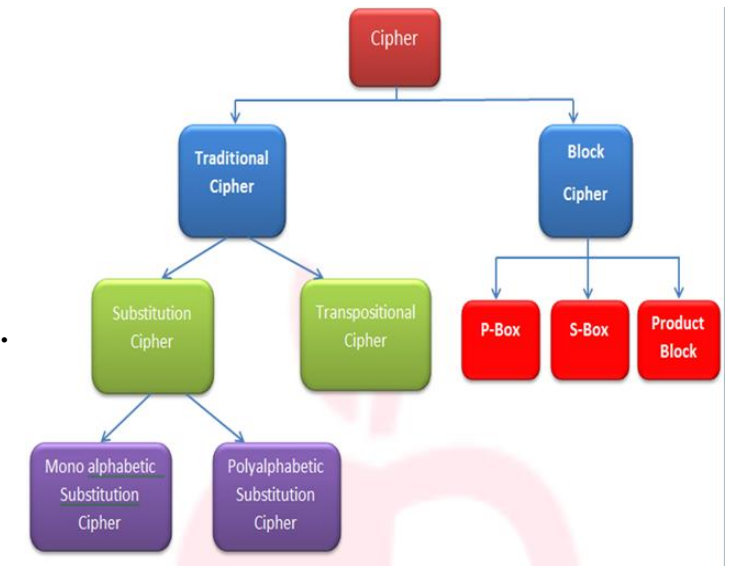
- Types of Block Ciphers:

- i. P-Box – It stands for Permutation Box. It performs transposition at the bit level.

It transposes blocks of bits within the plain text to form the ciphertext.

The total number of 1's and 0's are the same in both plain text and ciphertext.

- ii. S-Box – It stands for Substitution Box. It performs substitution at the bit level. It substitutes one decimal digit with another. An S-Box contains a decoder and a P-Box and an encoder. The decoder converts n -bit input into $2n$ -bit output. The P-Box then permutes the output of the decoder forming $2n$ -bit output. After that the encoder converts $2n$ -bit input n -bit output again. But this n -bit output differs from the original n -bit input.
- iii. Product Block – The P-Box and S-Box can combine to form a more complex block, it says Product Block.



Cipher Methods

- Substitution Cipher
- Hiding some data is known as encryption. When plain text is encrypted it becomes unreadable and is known as ciphertext.
- In a Substitution cipher, any character of plain text from the given fixed set of characters is substituted by some other character from the same set depending on a key. For example with a shift of 1, A would be replaced by B, B would become C, and so on.
- Note: Special case of Substitution cipher is known as Caesar cipher where the key is taken as 3.

Cipher Methods

- Substitution Cipher
- Mathematical representation
- The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,..., Z = 25.
- Encryption of a letter by a shift n can be described mathematically as.

$$E_n(x) = (x + n) \bmod 26$$

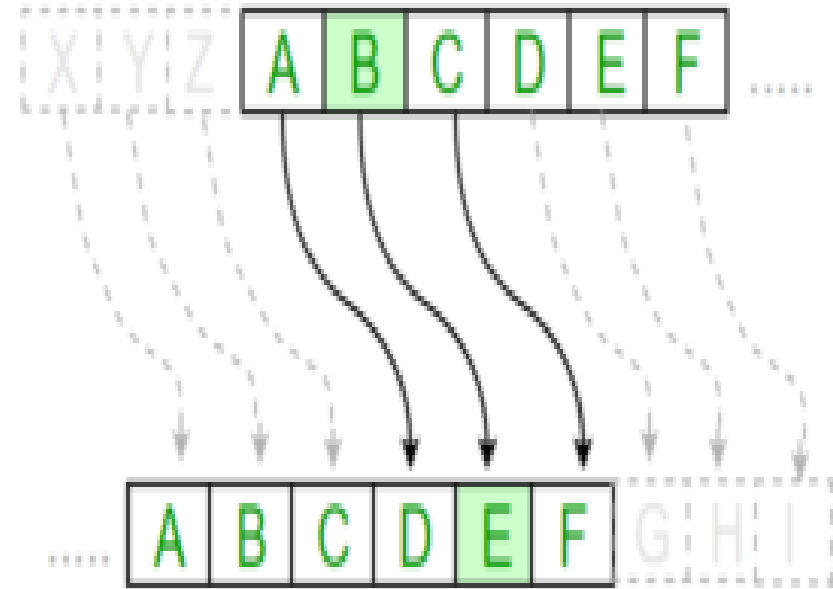
(Encryption Phase with shift n)

Cipher Methods

- Substitution Cipher

$$D_n(x) = (x - n) \bmod 26$$

(Decryption Phase with shift n)



Cipher Methods

- Substitution Cipher Examples:
 - Plain Text: I am studying Data Encryption
 - Key: 4
 - Output: M eq wxyhCmrk Hexe IrgvCtxmsr
-
- Plain Text: ABCDEFGHIJKLMNOPQRSTUVWXYZ
 - Key: 4
 - Output: EFGHIJKLMNOPQRSTUVWXYZabcd

Cipher Methods

- Substitution CipherExamples:
- Algorithm for Substitution Cipher:
- Input:
- A String of both lower and upper case letters, called PlainText.
- An Integer denoting the required key.

Cipher Methods

- Substitution Cipher
- Procedure:
 - Create a list of all the characters.
 - Create a dictionary to store the substitution for all characters.
 - For each character, transform the given character as per the rule, depending on whether we're encrypting or decrypting the text.
 - Print the new string generated.

Cipher Methods

- Transposition cipher
- In cryptography, a transposition cipher is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext.

Cipher Methods

- Columnar Transposition Cipher
- Given a plain-text message and a numeric key, cipher/de-cipher the given text using Columnar Transposition Cipher
- The Columnar Transposition Cipher is a form of transposition cipher just like Rail Fence Cipher.
- Columnar Transposition involves writing the plaintext out in rows, and then reading the ciphertext off in columns one by one.

Cipher Methods-

Columnar Transposition Cipher

- Encryption
- Input : Geeks for Geeks
- Key = HACK
- Output : e kefGsGsrekoe_
- Decryption
- Input : e kefGsGsrekoe_
- Key = HACK
- Output : Geeks for Geeks

- Encryption
- Input : Geeks on work
- Key = HACK
- Output : e w_eoo_Gs kknr_
- Decryption
- Input : e w_eoo_Gs kknr_
- Key = HACK
- Output : Geeks on work

Cipher Methods- Columnar Transposition Cipher

- **Encryption**

In a transposition cipher, the order of the alphabets is re-arranged to obtain the cipher-text.

1. The message is written out in rows of a fixed length, and then read out again column by column, and the columns are chosen in some scrambled order.
2. Width of the rows and the permutation of the columns are usually defined by a keyword.
3. For example, the word HACK is of length 4 (so the rows are of length 4), and the permutation is defined by the alphabetical order of the letters in the keyword. In this case, the order would be “3 1 2 4”.
4. Any spare spaces are filled with nulls or left blank or placed by a character (Example: _).
5. Finally, the message is read off in columns, in the order specified by the keyword.

Cipher Methods- Columnar Transposition Cipher

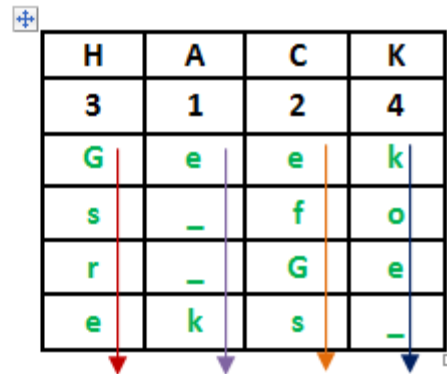
Encryption

Given text = Geeks for Geeks

Keyword = HACK

Length of Keyword = 4 (no of rows)

Order of Alphabets in HACK = 3124



H	A	C	K
3	1	2	4
G	e	e	k
s	_	f	o
r	_	G	e
e	k	s	_

Print Characters of column 1,2,3,4

Encrypted Text = e kefGsGsreko_e_

Cipher Methods- Columnar Transposition Cipher

- Decryption
- To decipher it, the recipient has to work out the column lengths by dividing the message length by the key length.
- Then, write the message out in columns again, then re-order the columns by reforming the key word.

Cipher Methods

- Exclusive OR
- XOR Encryption is an encryption method used to encrypt data and is hard to crack by brute-force method, i.e generating random encryption keys to match with the correct one.
- The concept of implementation is to first define XOR – encryption key and then to perform XOR operation of the characters in the String with this key which you want to encrypt.
- To decrypt the encrypted characters we have to perform XOR operation again with the defined key.
- Here we are encrypting the entire String.

Cipher Methods

- Exclusive OR

$$A \oplus 0 = A,$$

$$A \oplus A = 0,$$

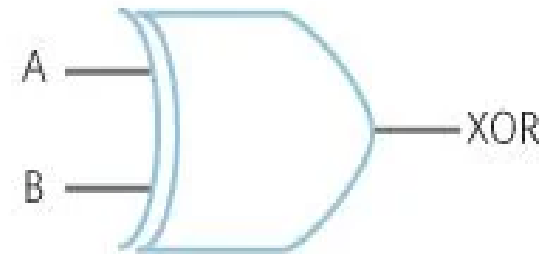
$$A \oplus B = B \oplus A,$$

$$(A \oplus B) \oplus C = A \oplus (B \oplus C),$$

$$(B \oplus A) \oplus A = B \oplus 0 = B,$$

where \oplus denotes the **exclusive disjunction (XOR)** operation.¹

$$X = A \oplus B$$



A	B	XOR
0	0	0
0	1	1
1	0	1
1	1	0

Cipher Methods

- Exclusive OR

For example, the string "Wiki" (01010111 01101001 01101011 01101001 in 8-bit ASCII) can be encrypted with the repeating key 11110011 as follows:

$$\begin{array}{r} 01010111 \ 01101001 \ 01101011 \ 01101001 \\ \oplus 11110011 \ 11110011 \ 11110011 \ 11110011 \\ \hline = 10100100 \ 10011010 \ 10011000 \ 10011010 \end{array}$$

And conversely, for decryption:

$$\begin{array}{r} 10100100 \ 10011010 \ 10011000 \ 10011010 \\ \oplus 11110011 \ 11110011 \ 11110011 \ 11110011 \\ \hline = 01010111 \ 01101001 \ 01101011 \ 01101001 \end{array}$$

Cipher Methods

- Exclusive OR
- <http://sticksandstones.kstrom.com/appen.html>
- **(ASCII - Binary Character Table)**

Cipher Methods - Exclusive OR

ASCII - Binary Character Table

Letter	ASCII Code	Binary	Letter	ASCII Code	Binary
a	097	01100001	A	065	01000001
b	098	01100010	B	066	01000010
c	099	01100011	C	067	01000011
d	100	01100100	D	068	01000100
e	101	01100101	E	069	01000101
f	102	01100110	F	070	01000110
g	103	01100111	G	071	01000111
h	104	01101000	H	072	01001000
i	105	01101001	I	073	01001001
j	106	01101010	J	074	01001010
k	107	01101011	K	075	01001011
l	108	01101100	L	076	01001100
m	109	01101101	M	077	01001101
n	110	01101110	N	078	01001110
o	111	01101111	O	079	01001111
p	112	01110000	P	080	01010000
q	113	01110001	Q	081	01010001

l	108	01101100	L	076	01001100
m	109	01101101	M	077	01001101
n	110	01101110	N	078	01001110
o	111	01101111	O	079	01001111
p	112	01110000	P	080	01010000
q	113	01110001	Q	081	01010001
r	114	01110010	R	082	01010010
s	115	01110011	S	083	01010011
t	116	01110100	T	084	01010100
u	117	01110101	U	085	01010101
v	118	01110110	V	086	01010110
w	119	01110111	W	087	01010111
x	120	01111000	X	088	01011000
y	121	01111001	Y	089	01011001
z	122	01111010	Z	090	01011010

Cipher Methods

- Exclusive OR
- The basic idea behind XOR – encryption is, if you don't know the XOR-encryption key before decrypting the encrypted data, it is impossible to decrypt the data.
- For example, if you XOR two unknown variables you cannot tell what the output of those variables is.
- Consider the operation $A \text{ XOR } B$, and this returns true.
- Now if the value of one of the variable is known we can tell the value of another variable.
- If A is True then B should be False or if A is False then B should be true according to the properties of the boolean XOR operation.
- Without knowing one of the value we can not decrypt the data and this idea is used in XOR – encryption.

Cipher Methods - Exclusive OR

// C++ program to implement XOR -
Encryption

```
#include<bits/stdc++.h>
```

// The same function is used to encrypt and
// decrypt

```
void encryptDecrypt(char inpString[])  
{
```

```
    // Define XOR key
```

```
    // Any character value will work
```

```
    char xorKey = 'P';
```

```
    // calculate length of input string
```

```
    int len = strlen(inpString);
```

```
    // perform XOR operation of key
```

```
    // with every character in string
```

```
    for (int i = 0; i < len; i++)
```

```
    {
```

```
        inpString[i] = inpString[i] ^ xorKey;
```

```
        printf("%c",inpString[i]);
```

```
    }
```

```
}
```

```
~~~~~
```

// Driver program to test above
function

```
int main()
```

```
{
```

```
    char sampleString[] =
```

```
    "GeeksforGeeks";
```

```
    // Encrypt the string
```

```
    printf("Encrypted String: ");
```

```
    encryptDecrypt(sampleString);
```

```
    printf("\n");
```

```
    // Decrypt the string
```

```
    printf("Decrypted String: ");
```

```
    encryptDecrypt(sampleString);
```

```
    return 0;
```

```
}
```

Output:

Encrypted String:

55;#6?"55;#

Decrypted String:

GeeksforGeeks

Cipher Methods

- Vernam Cipher
- **Vernam Cipher** is a method of encrypting alphabetic text.
- It is one of the Transposition techniques for converting a plain text into a cipher text.
- In this mechanism we assign a number to each character of the Plain-Text, like (a = 0, b = 1, c = 2, ... z = 25).
- **Method to take key:**

In Vernam cipher algorithm, we take a key to encrypt the plain text which length should be equal to the length of the plain text.

Cipher Methods

- Vernam Cipher
- Encryption Algorithm:
 - Assign a number to each character of the plain-text and the key according to alphabetical order.
 - Add both the number (Corresponding plain-text character number and Key character number).
 - Subtract the number from 26 if the added number is greater than 26, if it isn't then leave it.
- Example:
 - Plain-Text: RAMSWARUPK
 - Key: RANCHOBABA

Cipher Methods- Vernam Cipher

Now according to our encryption algorithm we assign a number to each character of our plain-text and key.

```
PT:  R A M S W A R U P K
NO:  17 0 12 18 22 0 17 20 15 10

KEY: R A N C H O B A B A
NO:  17 0 13 2 7 14 1 0 1 0
```

Now add the number of Plain-Text and Key and after doing the addition and subtraction operation (if required), we will get the corresponding Cipher-Text character number.

```
CT-NO: 34 0 25 20 29 14 18 20 16 10
```

In this case, there are two numbers which are greater than the 26 so we have to subtract 26 from them and after applying the subtraction operation the new Cipher text character numbers are as follow:

```
CT-NO: 8 0 25 20 3 14 18 20 16 10
```

New Cipher-Text is after getting the corresponding character from the number.

```
CIPHER-TEXT: I A Z U D O S U Q K
```

Note:

For the *Decryption* apply the just reverse process of encryption.

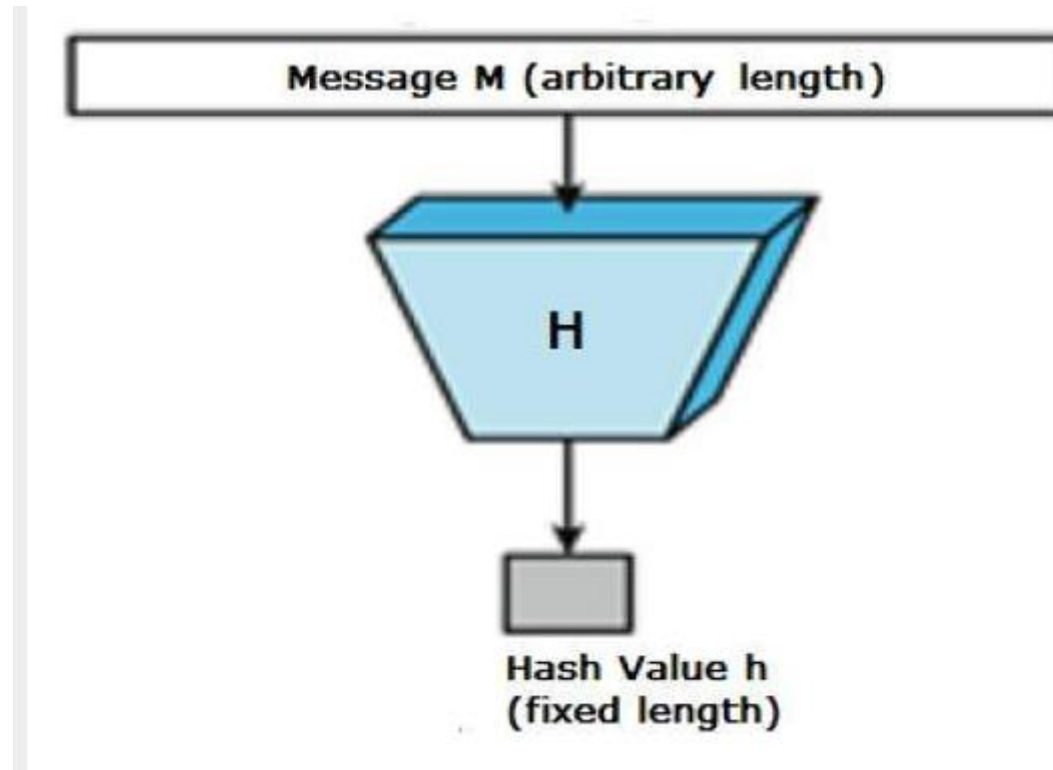
Cipher Methods- Book or Running key cipher

- The Running Key cipher has the same internal workings as the Vigenere cipher.
- The difference lies in how the key is chosen; the Vigenere cipher uses a short key that repeats, whereas the running key cipher uses a long key such as an excerpt from a book.
- This means the key does not repeat, making cryptanalysis more difficult.
- The cipher can still be broken though, as there are statistical patterns in both the key and the plaintext which can be exploited.
- If the key for the running key cipher comes from a statistically random source, then it becomes a 'one time pad' cipher. One time pads are theoretically unbreakable ciphers, because every possible decryption is equally likely.
- <http://practicalcryptography.com/ciphers/running-key-cipher/>

Cipher Methods- Hash Function

- Hash functions are extremely useful and appear in almost all information security applications.
- A hash function is a mathematical function that converts a numerical input value into another compressed numerical value. The input to the hash function is of arbitrary length but output is always of fixed length.
- Values returned by a hash function are called **message digest** or simply **hash values**. The following picture illustrated hash function –

Cipher Methods- Hash Function



Cipher Methods- Hash Function

- **Features of Hash Functions**

- The typical features of hash functions are –
- Fixed Length Output (Hash Value)
- Hash function converts data of arbitrary length to a fixed length. This process is often referred to as hashing the data.
- In general, the hash is much smaller than the input data, hence hash functions are sometimes called compression functions.
- Since a hash is a smaller representation of a larger data, it is also referred to as a digest.
- Hash function with n bit output is referred to as an n -bit hash function. Popular hash functions generate values between 160 and 512 bits.

Cryptographic Algorithms

- According to NIST, cryptographic algorithms that are either FIPS-approved or NIST-recommended must be used if cryptographic services are needed.
- These algorithms have undergone extensive security analysis and are continually tested to ensure that they provide adequate security.
- Cryptographic algorithms will usually use cryptographic keys and when these algorithms need to be strengthened, it can often be done by using larger keys.

Cryptographic Algorithms

- Symmetric Encryption
- Asymmetric Encryption
- Encryption key size

Cryptographic Algorithms

Types Of Cryptography:

In general there are three types Of cryptography:

1. Symmetric Key Cryptography:

It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system is Data Encryption System(DES).

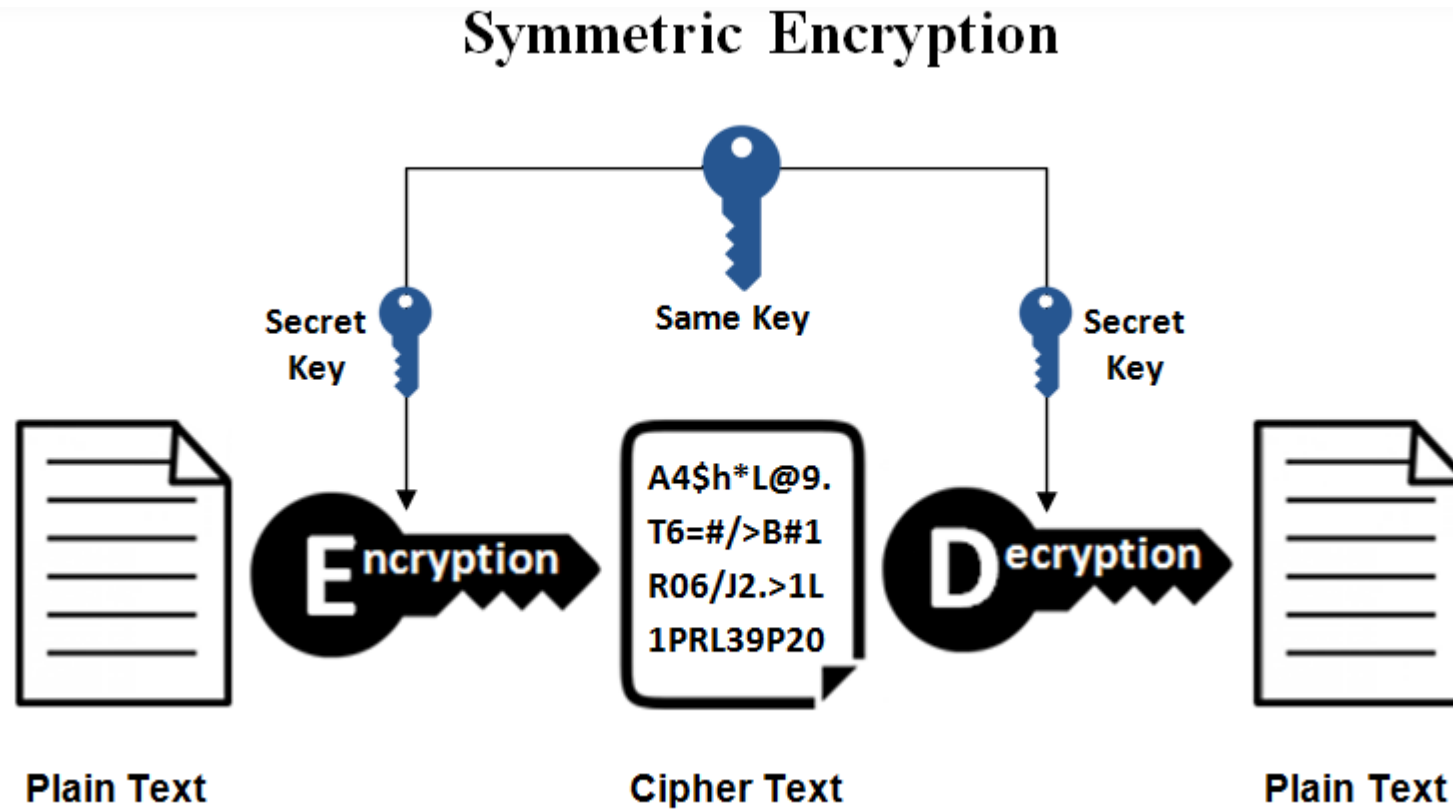
2. Hash Functions:

There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.

3. Asymmetric Key Cryptography:

Under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows the private key.

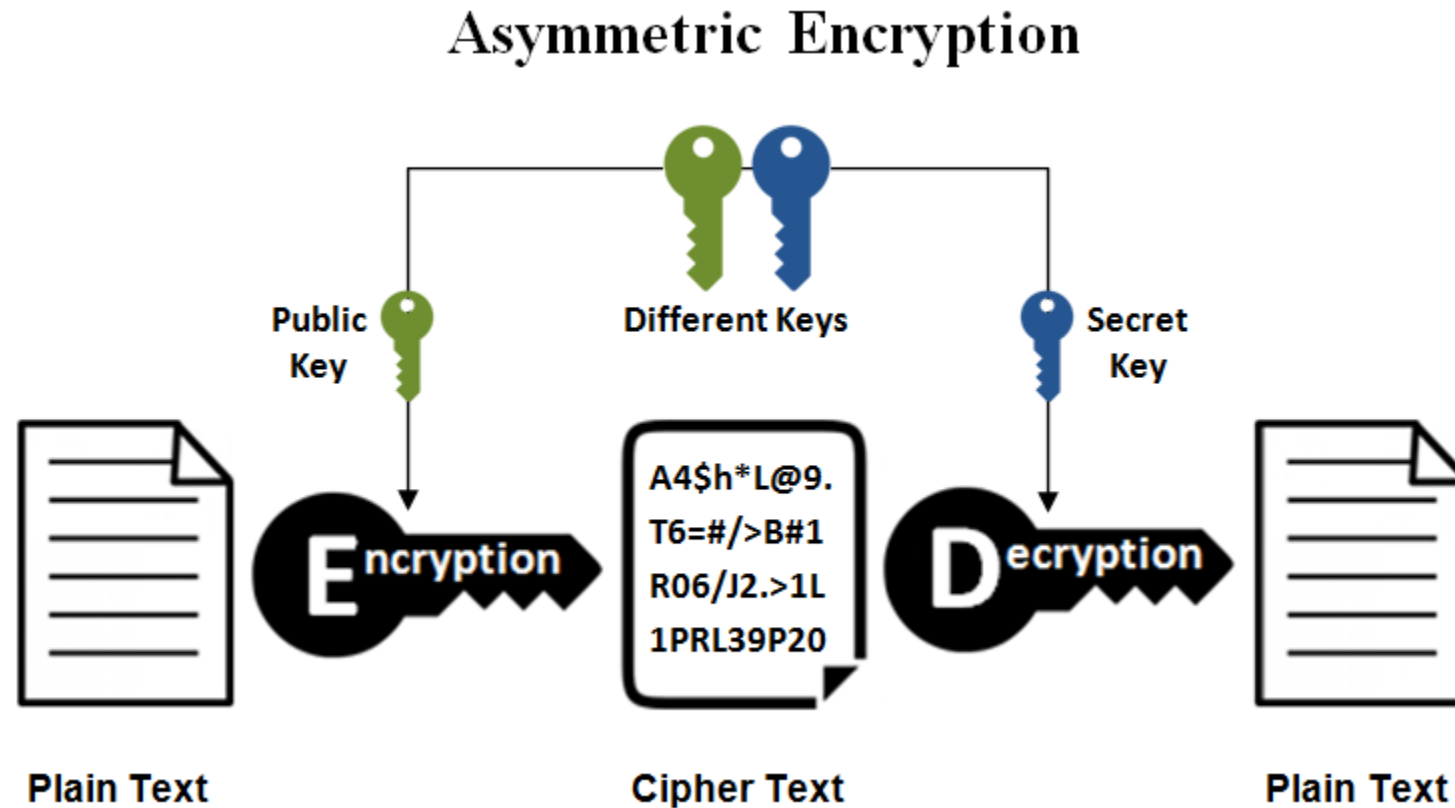
Cryptographic Algorithms- Symmetric Encryption



Cryptographic Algorithms- Symmetric Encryption

- This is the simplest kind of encryption that involves only one secret key to cipher and decipher information.
- Symmetric encryption is an old and best-known technique.
- It uses a secret key that can either be a number, a word or a string of random letters.
- It is blended with the plain text of a message to change the content in a particular way.
- The sender and the recipient should know the secret key that is used to encrypt and decrypt all the messages.
- Blowfish, AES, RC4, DES, RC5, and RC6 are examples of symmetric encryption.
- The most widely used symmetric algorithm is AES-128, AES-192, and AES-256.
- The main disadvantage of the symmetric key encryption is that all parties involved have to exchange the key used to encrypt the data before they can decrypt it.

Cryptographic Algorithms- Asymmetric Encryption



Cryptographic Algorithms- Asymmetric Encryption

- Asymmetric encryption is also known as public key cryptography, which is a relatively new method, compared to symmetric encryption.
- Asymmetric encryption uses two keys to encrypt a plain text.
- Secret keys are exchanged over the Internet or a large network.
- It ensures that malicious persons do not misuse the keys.
- It is important to note that anyone with a secret key can decrypt the message and this is why asymmetric encryption uses two related keys to boosting security.
- A public key is made freely available to anyone who might want to send you a message.
- The second private key is kept a secret so that you can only know.

Cryptographic Algorithms- Asymmetric Encryption

- A message that is encrypted using a public key can only be decrypted using a private key, while also, a message encrypted using a private key can be decrypted using a public key.
- Security of the public key is not required because it is publicly available and can be passed over the internet.
- Asymmetric key has a far better power in ensuring the security of information transmitted during communication.
- Asymmetric encryption is mostly used in day-to-day communication channels, especially over the Internet.
- Popular asymmetric key encryption algorithm includes ElGamal, RSA, DSA, Elliptic curve techniques, PKCS.

Cryptographic Algorithms-Encryption key size

- Advanced Encryption Standard (AES) keys are symmetric keys that can be three different key lengths (128, 192, or 256 bits).
- AES is the encryption standard that is recognized and recommended by the US government.
- The 256-bit keys are the longest allowed by AES.

Cryptographic Algorithms-Encryption key size

How does key size affect encryption?

- Encryption strength is often described in terms of the size of the keys used to perform the encryption:
- in general, longer keys provide stronger encryption.
- Key length is measured in bits.

Cryptographic tools

- Public Key infrastructure
- Digital Signature
- Digital Certificates
- Hybrid Cryptography Systems
- Steganography

Cryptographic tools- Public Key infrastructure

- The most distinct feature of Public Key Infrastructure (PKI) is that it uses a pair of keys to achieve the underlying security service.
- The key pair comprises of private key and public key.
- Since the public keys are in open domain, they are likely to be abused.
- It is, thus, necessary to establish and maintain some kind of trusted infrastructure to manage these keys.

Cryptographic tools- Public Key infrastructure

- There are two specific requirements of key management for public key cryptography.
- **Secrecy of private keys.** Throughout the key lifecycle, secret keys must remain secret from all parties except those who are owner and are authorized to use them.
- **Assurance of public keys.** In public key cryptography, the public keys are in open domain and seen as public pieces of data. By default there are no assurances of whether a public key is correct, with whom it can be associated, or what it can be used for. Thus key management of public keys needs to focus much more explicitly on assurance of purpose of public keys.
- The most crucial requirement of ‘assurance of public key’ can be achieved through the public-key infrastructure (PKI), a key management systems for supporting public-key cryptography.

Cryptographic tools- Public Key infrastructure

- Public Key Infrastructure (PKI)
- PKI provides assurance of public key. It provides the identification of public keys and their distribution. An anatomy of PKI comprises of the following components.
- Public Key Certificate, commonly referred to as ‘digital certificate’.
 - Private Key tokens.
 - Certification Authority.
 - Registration Authority.
 - Certificate Management System.

Cryptographic tools- Digital Signature

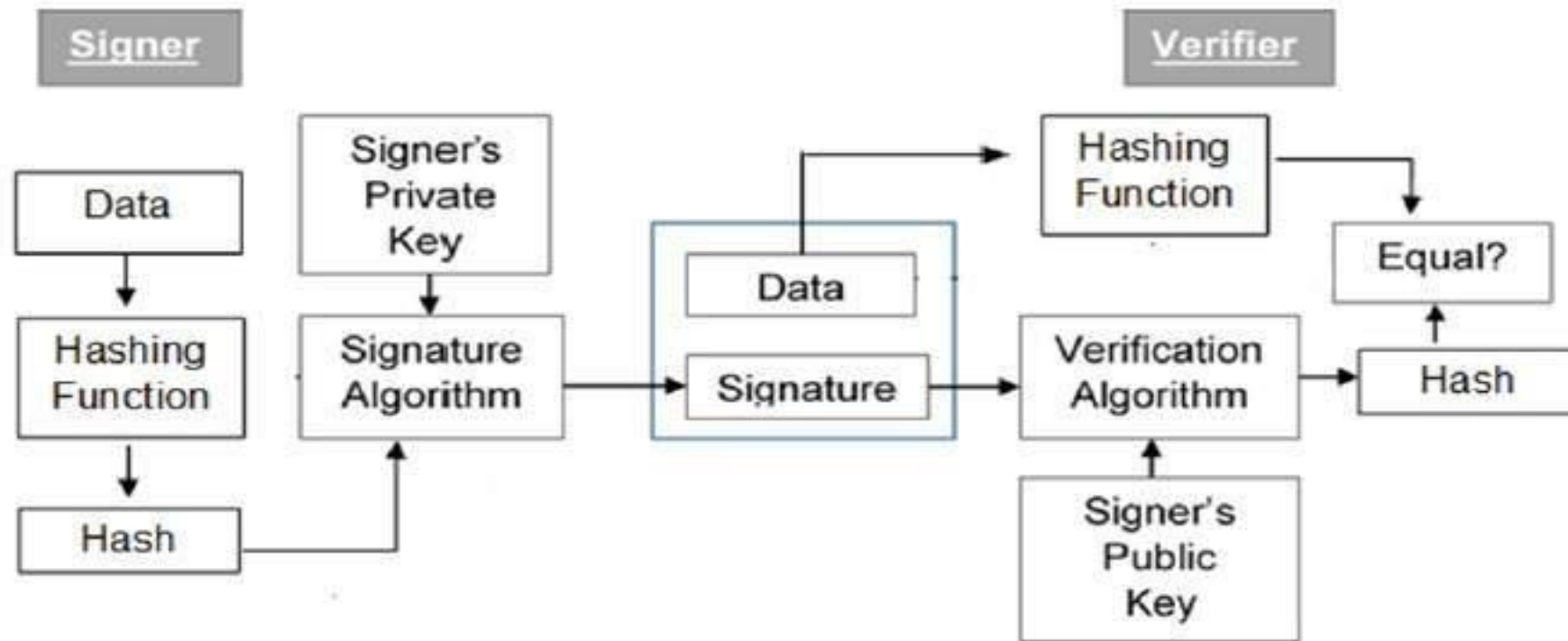
- Digital signatures are the public-key primitives of message authentication.
- In the physical world, it is common to use handwritten signatures on handwritten or typed messages.
- They are used to bind signatory to the message.
- Similarly, a digital signature is a technique that binds a person/entity to the digital data.
- This binding can be independently verified by receiver as well as any third party.
- Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer.
- In real world, the receiver of message needs assurance that the message belongs to the sender and he should not be able to repudiate the origination of that message.
- This requirement is very crucial in business applications, since likelihood of a dispute over exchanged data is very high.

Cryptographic tools- Digital Signature

- **Model of Digital Signature**
- As mentioned earlier, the digital signature scheme is based on public key cryptography.
- The model of digital signature scheme is depicted in the following illustration –

Cryptographic tools- Digital Signature

- **Model of Digital Signature**



Cryptographic tools- Digital Signature

- **Model of Digital Signature**
- Each person adopting this scheme has a public-private key pair.
- Generally, the key pairs used for encryption/decryption and signing/verifying are different.
- The private key used for signing is referred to as the signature key and the public key as the verification key.
- Signer feeds data to the hash function and generates hash of data.
- Hash value and signature key are then fed to the signature algorithm which produces the digital signature on given hash.
- Signature is appended to the data and then both are sent to the verifier.
- Verifier feeds the digital signature and the verification key into the verification algorithm.
- The verification algorithm gives some value as output.

Cryptographic tools- Digital Signature

- **Model of Digital Signature**
- Verifier also runs same hash function on received data to generate hash value.
- For verification, this hash value and output of verification algorithm are compared. Based on the comparison result, verifier decides whether the digital signature is valid.
- Since digital signature is created by ‘private’ key of signer and no one else can have this key; the signer cannot repudiate signing the data in future.
- It should be noticed that instead of signing data directly by signing algorithm, usually a hash of data is created. Since the hash of data is a unique representation of data, it is sufficient to sign the hash in place of data. The most important reason of using hash instead of data directly for signing is efficiency of the scheme

Cryptographic tools- Digital Signature

- **Model of Digital Signature**
- Let us assume RSA is used as the signing algorithm. As discussed in public key encryption chapter, the encryption/signing process using RSA involves modular exponentiation.
- Signing large data through modular exponentiation is computationally expensive and time consuming. The hash of the data is a relatively small digest of the data, hence signing a hash is more efficient than signing the entire data.

Cryptographic tools- Digital Certificates

- Digital certificates are used in public key cryptography functions most commonly for initializing Secure Sockets Layer (SSL) connections between web browsers and web servers.
- Digital certificates are also used for sharing keys used for public key encryption and authentication of digital signatures.

Cryptographic tools- Digital Certificates

- All major web browsers and web servers use digital certificates to provide assurance that unauthorized actors have not modified published content and to share keys for encrypting and decrypting web content.
- Digital certificates are also used in other contexts, online and offline, for providing cryptographic assurance and data privacy.

Cryptographic tools- Digital Certificates

- **How are digital certificates used?**
- Digital certificates are used in the following ways:
- Credit and debit cards use chip-embedded digital certificates that connect with merchants and banks to ensure that the transactions performed are secure and authentic.
- Digital payment companies use digital certificates to authenticate their automated teller machines, kiosks and point-of-sale equipment in the field with a central server in their data center.
- Websites use digital certificates for domain validation to show they are trusted and authentic.

Cryptographic tools- Digital Certificates

- **How are digital certificates used?**
- Digital certificates are used in secure email to identify one user to another and may also be used for electronic document signing.
- The sender digitally signs the email, and the recipient verifies the signature.
- Computer hardware manufacturers embed digital certificates into cable modems to help prevent the theft of broadband service through device cloning.
- As cyberthreats increase, more companies are considering attaching digital certificates to all of the IoT devices that operate at the edge and within their enterprises.

Cryptographic tools- Hybrid Cryptography Systems

- In cryptography, a hybrid cryptosystem is one which combines the convenience of a public-key cryptosystem with the efficiency of a symmetric-key cryptosystem.
- Public-key cryptosystems are convenient in that they do not require the sender and receiver to share a common secret in order to communicate securely.
- However, they often rely on complicated mathematical computations and are thus generally much more inefficient than comparable symmetric-key cryptosystems.
- In many applications, the high cost of encrypting long messages in a public-key cryptosystem can be prohibitive.
- This is addressed by hybrid systems by using a combination of both.

Cryptographic tools- Hybrid Cryptography Systems

- A hybrid cryptosystem can be constructed using any two separate cryptosystems:
 - a key encapsulation mechanism, which is a public-key cryptosystem, and
 - a data encapsulation scheme, which is a symmetric-key cryptosystem.
- The hybrid cryptosystem is itself a public-key system, whose public and private keys are the same as in the key encapsulation scheme.
- Note that for very long messages the bulk of the work in encryption/decryption is done by the more efficient symmetric-key scheme, while the inefficient public-key scheme is used only to encrypt/decrypt a short key value.

Cryptographic tools- Hybrid Cryptography Systems

- All practical implementations of public key cryptography today employ the use of a hybrid system.
- Examples include the TLS protocol and the SSH protocol, that use a public-key mechanism for key exchange (such as Diffie-Hellman) and a symmetric-key mechanism for data encapsulation (such as AES).
- The OpenPGP file format and the PKCS #7 file format are other examples.
- Hybrid Public Key Encryption is a modern standard for generic hybrid encryption.
- HPKE is used within multiple IETF protocols, including MLS and TLS Encrypted Hello.
- Envelope encryption is an example of a usage of hybrid cryptosystems in cloud computing.
- In a cloud context, hybrid cryptosystems also enable centralized key management.

Cryptographic tools - Steganography

- Steganography is the practice of concealing a message within another message or a physical object.
- In computing/electronic contexts, a computer file, message, image, or video is concealed within another file, message, image, or video.
- The word steganography comes from Greek steganographia, which combines the words steganós (meaning "covered or concealed", and -graphia meaning "writing".)

Cryptographic tools - Steganography

- The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny.
- Plainly visible encrypted messages, no matter how unbreakable they are, arouse interest and may in themselves be incriminating in countries in which encryption is illegal.
- Whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent and its contents.

Cryptographic tools - Steganography

- Steganography includes the concealment of information within computer files.
- In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program, or protocol.
- Media files are ideal for steganographic transmission because of their large size.
- For example, a sender might start with an innocuous image file and adjust the color of every hundredth pixel to correspond to a letter in the alphabet.
- The change is so subtle that someone who is not specifically looking for it is unlikely to notice the change.

Attacks on cryptosystems

- A cryptosystem is a structure or scheme consisting of a set of algorithms that converts plaintext to ciphertext

Types of Attack On cryptosystems

- Man in the Middle Attack
- Correlation attacks
- Dictionary Attacks
- Timing Attacks
- Defending against attack

Attacks on cryptosystems - Man in the Middle Attack

Man in Middle Attack (MIM) – The targets of this attack are mostly public key cryptosystems where key exchange is involved before communication takes place.

- Host A wants to communicate to host B , hence requests public key of B .
- An attacker intercepts this request and sends his public key instead.
- Thus, whatever host A sends to host B , the attacker is able to read.
- In order to maintain communication, the attacker re-encrypts the data after reading with his public key and sends to B .
- The attacker sends his public key as A 's public key so that B takes it as if it is taking it from A .

Attacks on cryptosystems - Correlation attacks

- In cryptography, correlation attacks are a class of known plaintext attacks for breaking stream ciphers whose key stream is generated by combining the output of several linear-feedback shift registers (LFSRs) using a Boolean function.
- Correlation attacks exploit a statistical weakness that arises from certain choices of the Boolean function.
- The cipher is not inherently insecure if there is a choice of the Boolean function that avoids this weakness.
- It is essential to consider susceptibility to correlation attacks when designing stream ciphers of this type.

Attacks on cryptosystems - Dictionary Attacks

- **Dictionary Attack** – This attack has many variants, all of which involve compiling a ‘dictionary’. In simplest method of this attack, attacker builds a dictionary of ciphertexts and corresponding plaintexts that he has learnt over a period of time. In future, when an attacker gets the ciphertext, he refers the dictionary to find the corresponding plaintext.

Attacks on cryptosystems - Timing Attacks

- **Timing Attacks** – They exploit the fact that different computations take different times to compute on processor. By measuring such timings, it is possible to know about a particular computation the processor is carrying out. For example, if the encryption takes a longer time, it indicates that the secret key is long.

Attacks on cryptosystems - Defending against attack

- In a public-key cryptosystem, the encryption key is in open domain and is known to any potential attacker.
- Using this key, he can generate pairs of corresponding plaintexts and ciphertexts.

Physical Security

- Physical Access Controls
 - Walls , fencing and gates
 - Guards
 - Dogs
 - ID Cards and Badges
 - Locks and keys
 - Mantraps
 - Electronic Monitoring
 - Alarms and Alarm Systems
 - Computer rooms and wiring closets
 - Interior walls and doors

Physical Security- Physical Access Controls

Walls , fencing and gates

- Walls, Fencing, and Gates Some of the oldest and most reliable elements of physical security are walls, fencing, and gates.
- While not every organization needs to implement external perimeter controls, walls and fences with suitable gates are an essential starting point for organizations whose employees require access to physical locations the organization owns or controls.
- These types of controls vary widely in appearance and function, ranging from chain link or privacy fences that control where people should park or walk, to imposing concrete or masonry barriers designed to withstand the blast of a car bomb.
- Each exterior perimeter control requires expert planning to ensure that it fulfills the security goals and that it presents an image appropriate to the organization.

Physical Security- Physical Access Controls

- Guards

- Controls like fences and walls with gates are static, and are therefore unresponsive to actions, unless they are programmed to respond with specific actions to specific stimuli, such as opening for someone who has the correct key.
- Guards, on the other hand, can evaluate each situation as it arises and make reasoned responses.
- Most guards have clear standard operating procedures (SOPs) that help them to act decisively in unfamiliar situations.
- In the military, for example, guards are given general orders (see the Offline on guard duty), as well as special orders that are particular to their posts.

Physical Security

- Physical Access Controls

- Dogs

- If an organization is protecting valuable resources, dogs can be a valuable part of physical security if they are integrated into the plan and managed properly.
 - Guard dogs are useful because their keen sense of smell and hearing can detect intrusions that human guards cannot, and they can be placed in harm's way when necessary to avoid risking the life of a person.

Physical Security- Physical Access Controls

- ID Cards and Badges
- An identification (ID) card is typically concealed, whereas a name badge is visible. Both devices can serve a number of purposes.
- First, they serve as simple forms of biometrics in that they use the cardholder's picture to authenticate his or her access to the facility.
- The cards may be visibly coded to specify which buildings or areas may be accessed.
- Second, ID cards that have a magnetic strip or radio chip that can be read by automated control devices allow an organization to restrict access to sensitive areas within the facility.
- ID cards and name badges are not foolproof, however; and even the cards designed to communicate with locks can be easily duplicated, stolen, or modified.
- Because of this inherent weakness, such devices should not be an organization's only means of controlling access to restricted areas.

Physical Security- Physical Access Controls

- **ID Cards and Badges**
- Another inherent weakness of this type of physical access control technology is the human factor.
- As depicted in this chapter's opening vignette, tailgating occurs when an authorized person presents a key to open a door, and other people, who may or may not be authorized, also enter.
- Launching a campaign to make employees aware of tailgating is one way to combat this problem.
- There are also technological means of discouraging tailgating, such as mantraps or turnstiles.
- These extra levels of control are usually expensive, in that they require floor space and/or construction, and are inconvenient for those required to use them.
- Consequently, anti-tailgating controls are only used where there is significant security risk from unauthorized entry.

Physical Security- Physical Access Controls

- Locks and keys
- There are two types of lock mechanisms: mechanical and electromechanical.
- The mechanical lock may rely on a key that is a carefully shaped piece of metal, which is rotated to turn tumblers that release secured loops of steel, aluminum, or brass (as in, for example, brass padlocks).
- Alternatively, a mechanical lock may have a dial that rotates slotted discs until the slots on multiple disks are aligned, and then retracts a securing bolt (as in combination and safe locks).
- Although mechanical locks are conceptually simple, some of the technologies that go into their development are quite complex.
- Some of these modern enhancements have led to the creation of the electromechanical lock.
- Electromechanical locks can accept a variety of inputs as keys, including magnetic strips on ID cards, radio signals from name badges, personal identification numbers (PINs) typed into a keypad, or some combination of these to activate an electrically powered locking mechanism

Physical Security- Physical Access Controls

- **Locks and keys**
- Locks can also be divided into four categories based on the triggering process: manual, programmable, electronic, and biometric.
- Manual locks such as padlocks and combination locks, are commonplace and well understood.
- If you have the key (or combination) you can open the lock.
- These locks are often preset by the manufacturer and therefore unchangeable.
- In other words, once manual locks are installed into doors, they can only be changed by highly trained locksmiths.
- Programmable locks can be changed after they are put in service, allowing for combination or key changes without a locksmith and even allowing the owner to change to another access method (key or combination) to upgrade security.
- Many examples of these types of locks are shown
- Mechanical push button locks, show are popular for securing computer rooms and wiring closets, as they have a code that can be reset and don't require electricity to operate.

Physical Security- Physical Access Controls

- **Locks and keys**

- Electronic locks can be integrated into alarm systems and combined with other building management systems.
- Also, these locks can be integrated with sensors to create various combinations of locking behavior.
- One such combination is a system that coordinates the use of fire alarms and locks to improve safety during alarm conditions (i.e., fires).
- Such a system changes a location's required level of access authorization when that location is in an alarm condition.

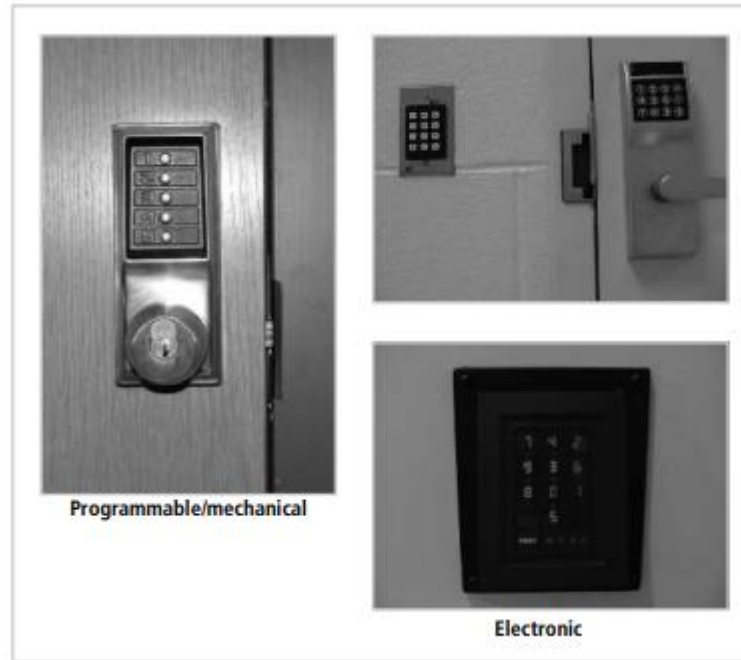
Physical Security- Physical Access Controls

- **Locks and keys**

- Another example is a combination system in which a lock is fitted with a sensor that notifies guard stations when that lock has been activated.
- Another common form of electronic locks are electric strike locks, which usually require people to announce themselves before being “buzzed” through a locked door. In general, electronic locks lend themselves to uses where they can be activated or deactivated by a switch controlled by an agent, usually a secretary or guard.
- Electronic push button locks, like their mechanical cousins, have a numerical keypad over the knob, requiring the individual user to enter a personal code and open the door. These locks usually use battery backups to power the keypad in case of a power failure.

Physical Security- Physical Access Controls

- **Locks and keys**

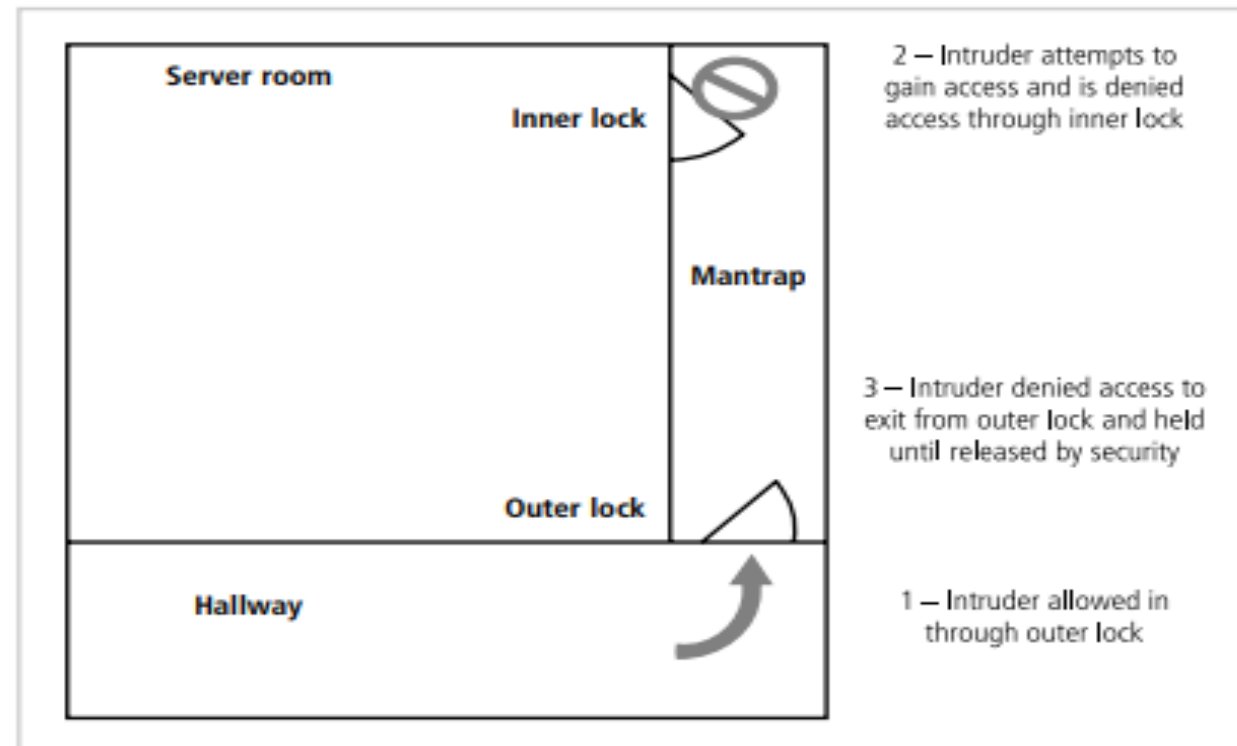


Physical Security

- Physical Access Controls
 - Mantraps
 - A common enhancement for locks in high security areas is the mantrap.
 - A mantrap is a small enclosure that has separate entry and exit points.
 - To gain access to the facility, area, or room, a person enters the mantrap, requests access via some form of electronic or biometric lock and key, and if confirmed, exits the mantrap into the facility.
 - Otherwise the person cannot leave the mantrap until a security official overrides the enclosure's automatic locks.
 - Figure 9-2 provides an example of a typical mantrap layout.

Physical Security

- Physical Access Controls
 - Mantraps



Physical Security

Physical Access Controls

- **Alarms and Alarm Systems**

- Closely related to monitoring are the alarm systems that notify people or systems when a predetermined event or activity occurs.
- Alarms, which are similar to the IDPSs can detect a physical intrusion or other untoward event.
- This could be a fire, a break-in, an environmental disturbance such as flooding, or an interruption in services such as a loss of power.
- One example of an alarm system is the burglar alarm commonly found in residential and commercial environments.
- Burglar alarms detect intrusions into unauthorized areas and notify either a local or remote security agency to react.
- To detect intrusions, these systems rely on a number of different types of sensors: motion detectors, thermal detectors, glass breakage detectors, weight sensors, and contact sensors.

Physical Security- **Physical Access Controls**

Alarms and Alarm Systems

- Motion detectors detect movement within a confined space and are either active or passive.
- Some motion sensors emit energy beams, usually in the form of infrared or laser light, ultrasonic sound or sound waves, or some form of electromagnetic radiation. If the energy from the beam projected into the area being monitored is disrupted, the alarm is activated.
- Other types of motion sensors are passive in that they constantly measure the energy (infrared or ultrasonic) from the monitored space and detect rapid changes in this energy.
- The passive measurement of these energies can be blocked or disguised and is therefore fallible.

Physical Security

- Physical Access Controls
 - Computer rooms and wiring closets
 - Computer rooms and wiring and communications closets require special attention to ensure the confidentiality, integrity, and availability of information.
 - For an outline of the physical and environmental controls needed for computer rooms, read the Technical Details box entitled “Physical and Environmental Controls for Computer Rooms.”

Physical Security

- Physical Access Controls
 - Interior walls and doors
 - The security of information assets can sometimes be compromised by the nature of the construction of the walls and doors of the facility.
 - The walls in a facility are typically of two types: standard interior and firewall.
 - Building codes require that each floor have a number of firewalls, or walls that limit the spread of damage should a fire break out in an office.
 - Between the firewalls, standard interior walls compartmentalize the individual offices.
 - Unlike firewalls, these interior walls reach only part way to the next floor, which leaves a space above the ceiling but below the floor of the next level up.
 - This space is called a plenum, and is usually one to three feet to allow for ventilation systems that can inexpensively collect return air from all the offices on the floor

Physical Security

- Physical Access Controls
 - Interior walls and doors
 - As a result, all high-security areas, such as computer rooms and wiring closets, must have firewall-grade walls surrounding them.
 - This provides physical security not only from potential intruders, but also from fires.