Basics of Information and Network Security

- In daily life we use information for various purposes and use network for communication and exchange information between different parties.
- In many cases these information are sensitive so we need to take care that only authorized party can get that information.
- For maintaining such privacy we require some mechanism or physical device which ensures that it is safe. Such mechanism or physical devices are known as **security system**.
- **Computer Security:** The protection afforded to an automated information system in order to attain the applicable objectives of preserving the **integrity**, **availability**, and **confidentiality** of information system resources.
- This definition of computer security introduces three key objectives that are at the heart of computer security:
  1. **Confidentiality:** It covers two 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.
  2. **Integrity:** It covers two concepts
     Data Integrity: Assures that information and programs are changed only in a specified and authorize 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.
  3. **Availability:** Assures that systems work promptly and service is not denied to authorize user.
- **Unconditionally secure algorithm:** An algorithm or an encryption scheme is unconditionally secure if the attacker cannot obtain the corresponding plaintext from ciphertext no matter how much ciphertext is available.
- **Computationally secure algorithm:** An encryption scheme is said to be computationally secure if either of the following criteria is met:
  o The cost of breaking the cipher exceeds the value of the encrypted information.
  o The time required to break the cipher exceeds the useful lifetime of the information.
- **Threat:** A potential for violation of security, which exists when there is a circumstance, capability,

  action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit vulnerability.

Security Attacks

- **Security Attacks:** An attack is an action that comprises the information or networksecurity.
- There are two types of attacks:
  1. Passive Attack
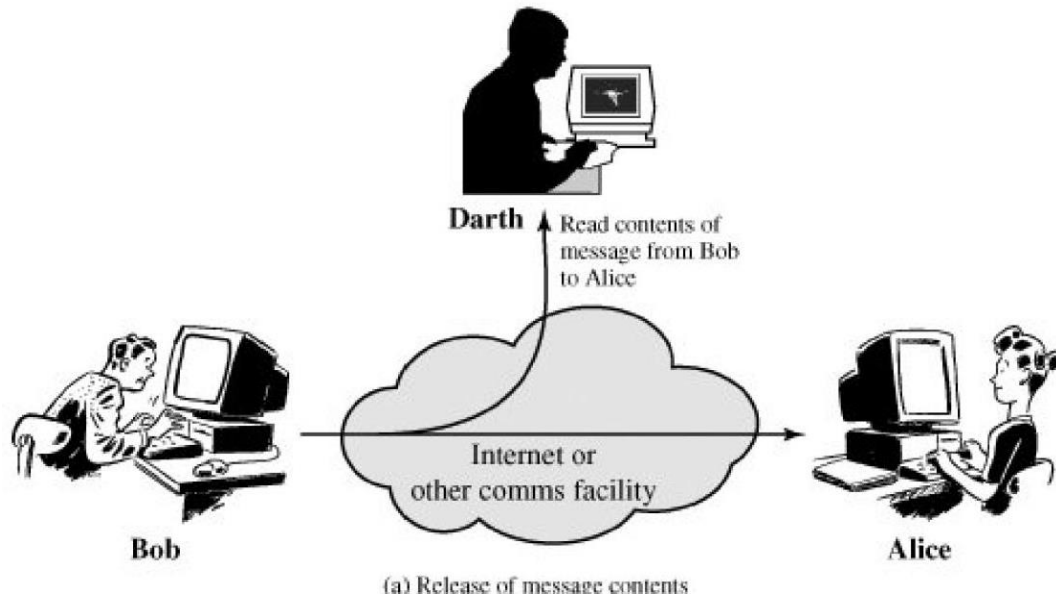 2. Active Attack

Passive Attack

- **Passive Attack:** The attacker only monitors the traffic attacking the confidentiality of the data. It

contains release of message contents and traffic analysis (in case of encrypted data).

1. **Release of message contents:**
   o The release of message contents is easily understood.
   o A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information.
   o We would like to prevent an opponent from learning the contents of these transmissions.

(a) Release of message contents

2. **Traffic analysis:**
   o A second type of passive attack, traffic analysis.
   o Suppose that we had a way of masking the contents of messages or other information.
   o Even if they captured the message, could not extract the information from the message.
   o The common technique for masking contents is encryption.
   o If we had encryption protection in place, an opponent might still be able to observe the pattern of these messages.
   o The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged.
   o This information might be useful in guessing the nature of the communication that was taking place.
   o Passive attacks are very difficult to detect because they do not involve any alteration of the data.
   o Typically, the message traffic is send and received in an apparently normal fashion and the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern.


(b) Traffic analysis
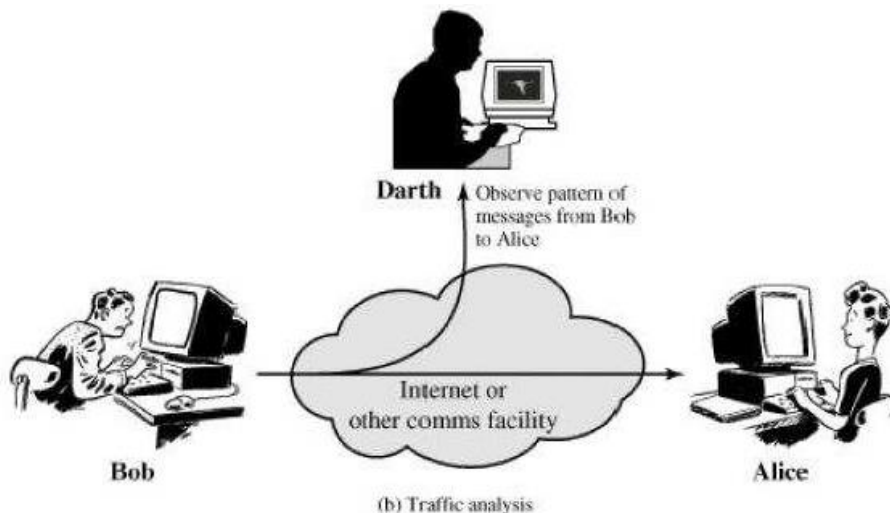
Active attack

- **Active attack:** Attacker tries to alter transmitted data. It includes masquerade, modification, replay and denial of service.
    1. **Masquerade:** A masquerade takes place when one entity pretends to be a different entity (Figure a). A masquerade attack usually includes one of the other forms of active attack.


(a) Masquerade
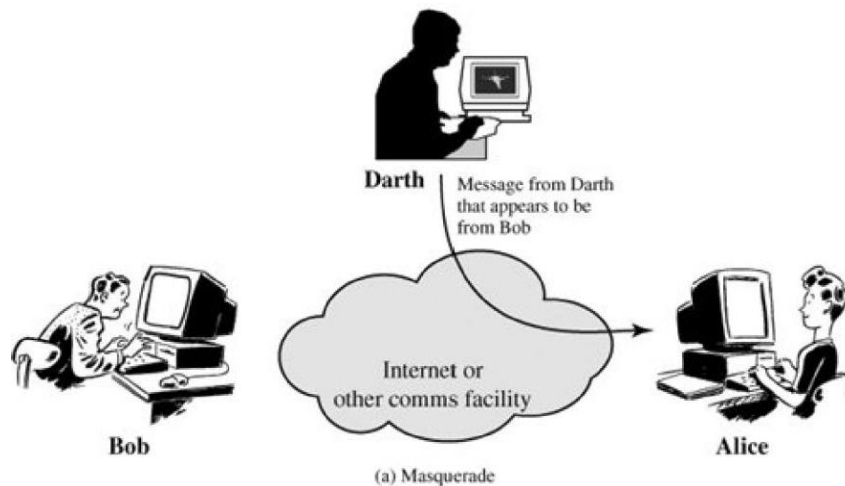
    2. **Replay:** Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

(b) Replay
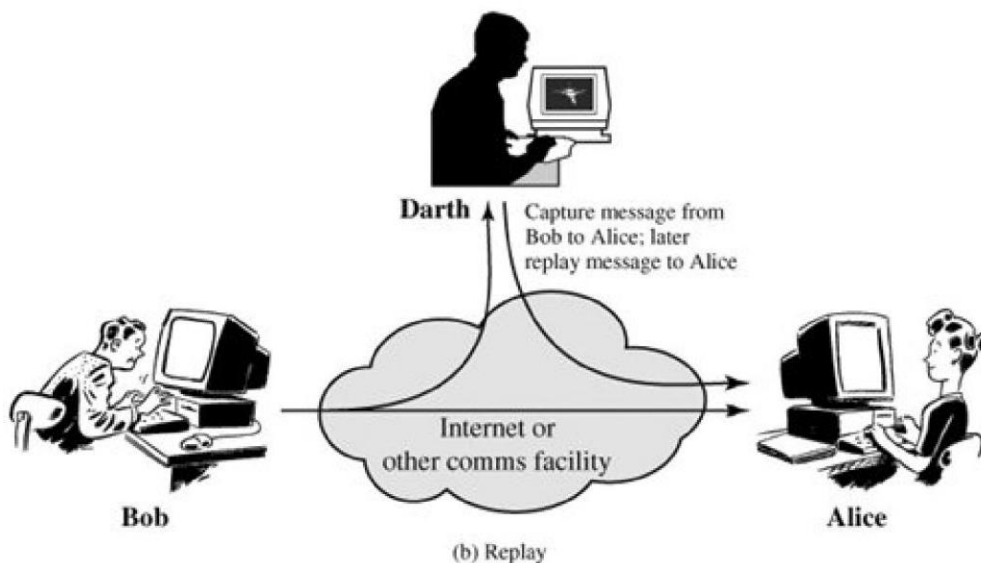
   3. **Modification of messages:**
        o Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect (Figure c).
        o For example, a message meaning "Allow John Smith to read confidential file accounts" is modified to mean "Allow Fred Brown to read confidential file accounts."

Darth modifies message from Bob to Alice

(c) Modification of messages
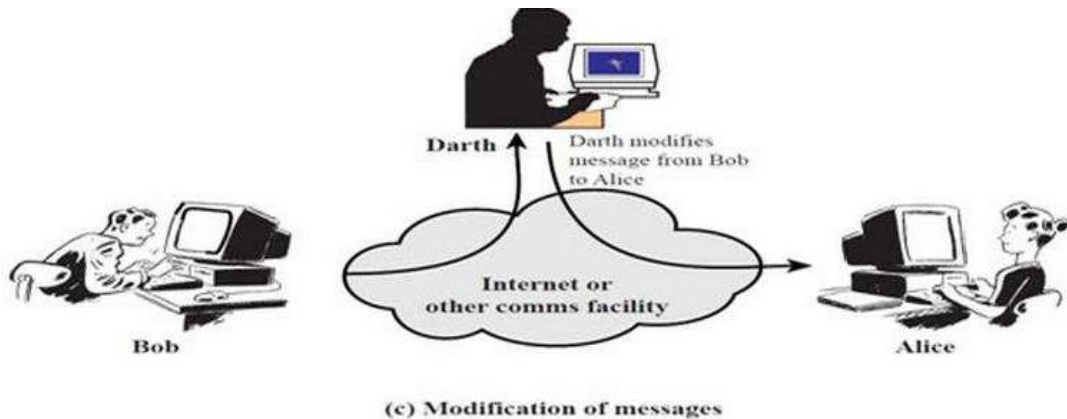
4. **Denial of service:**
   o The denial of service prevents or inhibits the normal use or management of communications facilities.
   o This attack may have   a specific target; for example, an entity may   suppress all messages directed to a particular destination (e.g., the security audit service).
   o Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.

Darth disrupts service provided by server

(d) Denial of service
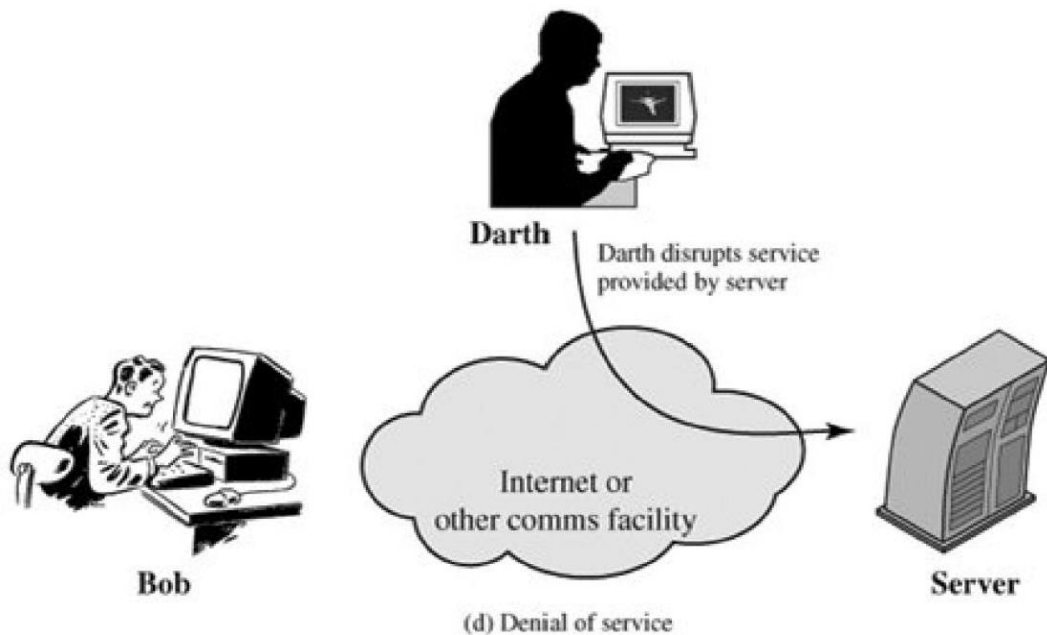
Security services

- A security service is a processing or communicating service that can prevent or detect the above-mentioned attacks. Various security services are:
  o **Authentication:** the recipient should be able to identify the sender, and verify that the sender, who claims to be the sender, actually did send the message.
  o **Data Confidentiality:** An attacker should not be able to read the transmitted data or extract data in case of encrypted data. In short, confidentiality is the protection of transmitted data from passive attacks.
  o **Data Integrity:** Make sure that the message received was exactly the message the sender sent.
  o **Nonrepudiation:** The sender should not be able to deny sending the   message.   The receiver should not be able to deny receiving the message.

Symmetric Cipher Model
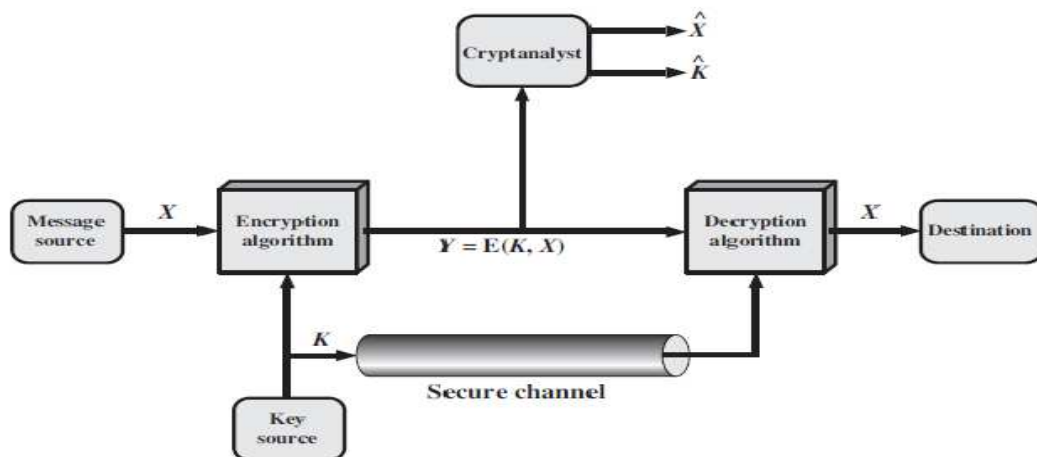
- A symmetric cipher model are broadly contains five parts.
- **Plaintext:** This is the original intelligible message.
- **Encryption algorithm:** The encryption algorithm performs various substitutions and transformations on the plaintext. It takes in plaintext and key and gives the ciphertext.
- **Secret key:** The key is a value independent of the plaintext and of the algorithm. Different keys will yield different outputs.
- **Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and the secret key.
- **Decryption algorithm:** Runs on the ciphertext and the key to produce the plaintext. This is essentially the encryption algorithm run in reverse.
- Two basic requirements of encryption are:
    1. Encryption algorithm should be strong. An attacker knowing the algorithm and having any number of ciphertext should not be able to decrypt the ciphertext or guess the key.
    2. The key shared by the sender and the receiver should be secret.
- Let the plaintext be $X = [X1, X2,…, X_M]$, key be $K = [K1, K2,…, K_J]$ and the ciphertext produced be $Y = [Y1, Y2,…, Y_N]$. Then, we can write

$$Y = E(K, X)$$

- Here E represents the encryption algorithm and is a function of plaintext X and key K.
- The receiver at the other ends decrypts the ciphertext using the key.

$$X = D(K, Y)$$

- Here D represents the decryption algorithm and it inverts the transformations of encryption algorithm.
- An opponent not having access to X or K may attempt to recover K or X or both.
- It is assumed that the opponent knows the encryption (E) and decryption (D) algorithms.
- If the opponent is interested in only this particular message, then the focus of the effort is to recover by generating a plaintext estimate $\hat{X}$.
- If the opponent is interested in being able to read future messages as well then he will attempt to recover the key by making an estimate $\hat{K}$.

Cryptography

- **Cryptography:** The area of   study containing the principles and methods of transforming an intelligible message into one that is unintelligible, and then retransforming that message back to its original form.
- Cryptographic systems are characterized along three independent dimensions.
    1. **The types of operations used for transforming plaintext to ciphertext.** All encryption algorithms are based on two general principles substitution, and transposition. Basic requirement is that no information be lost. Most systems referred to as product system, involves multiple stages of substitutions and transpositions.
    2. **The number of keys used.** If both sender and receiver use the same key, the system is referred to as **symmetric, single-key, secret-key, or conventional encryption**. If the sender and receiver use different keys the system is referred to as **asymmetric, two-key, or public-key encryption**.
    3. **The way in which the plaintext is processed.** A block cipher process a block at a time and produce an output block for each input block. A stream cipher process the input element continuously, producing output one element at a time, as it goes along.

Cryptanalysis and Brute-Force Attack

- **Cryptanalysis:** Cryptanalytic attacks rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some simple plaintext-ciphertext pairs. This type of attack finds characteristics of the algorithm to find a specific plaintext or to find key.
- **Brute-force attack:** The attacker tries every possible key on a piece of ciphertext until plaintext is obtained. On average, half of all possible keys must be tried to achieve success.
- Based on the amount of information known to the cryptanalyst cryptanalytic attacks can be categorized as:
    o **Cipher text Only Attack:** The attacker knows only cipher text only. It is easiest to defend.
    o **Known plaintext Attack:** In this type of attack, the opponent has some plaintext-cipher text pairs. Or the analyst may know that certain plaintext patterns will appear in a message. For example, there may be a standardized header or banner to an electronic funds transfer message and the attacker can use that for generating plaintext-cipher text pairs.
    o **Chosen plaintext:** If the analyst is able somehow to get the source system to insert into the system a message chosen by the analyst, then a *chosen-plaintext* attack is possible. In such a case, the analyst will pick patterns that can be expected to reveal the structure of the key.
    o **Chosen Cipher text:** In this attack, the analyst has cipher text and some plaintext-cipher text pairs where cipher text has been chosen by the analyst.
    o **Chosen Text:** Here, the attacker has got cipher text, chosen plaintext-cipher text pairs and chosen cipher text-plaintext pairs.
- Chosen cipher text and chosen text attacks are rarely used.
- It is assumed that the attacker knows the encryption and decryption algorithms.
- Generally, an encryption algorithm is designed to withstand a known-plaintext attack.

Brute-force attack

- This type of attack becomes   impractical as the key size increases as   trying all the possible

---

alternative keys for a very large key may take a huge amount of time.

- For example, for a binary key of 128 bits, 2^{128} keys are possible which would require around 5 X10^{24} years at the rate of 1 decryption per microsecond (current machine's speed).

- The Data Encryption Standard (DES) algorithm uses a 56-bit key a 128-bit key is used in AES.

- With massively parallel systems, even DES is also not secure against Brute Force attack.

- AES with its 128-bit key is secure since the time required to break it makes it impractical to try Brute-Force attack

Substitution Techniques

- Various conventional encryption schemes or substitution techniques are as under:

Caesar cipher

- The encryption rule is simple; replace each letter of the alphabet with the letter standing 3 places further down the alphabet.

- The alphabet is wrapped around so that Z follows A.

- Example:
  Plaintext: MEET ME AFTER THE PARTY
  Ciphertext: PHHW PH DIWHU WKH SDUWB

- Here, the key is 3. If different key is used, different substitution will be obtained.

- Mathematically, starting from a=0, b=1 and so on, Caesar cipher can be written as:

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

- This cipher can be broken
  - If we know one plaintext-cipher text pair since the difference will be same.
  - By applying Brute Force attack as there are only 26 possible keys.

Monoalphabetic Substitution Cipher

- Instead of shifting alphabets by fixed amount as in Caesar cipher, any random permutation is assigned to the alphabets. This type of encryption is called monoalphabetic substitution cipher.

- For example, A is replaced by Q, B by D, C by T etc. then it will be comparatively stronger than Caesar cipher.

- The number of alternative keys possible now becomes 26!.

- Thus, Brute Force attack is impractical in this case.

- However, another attack is possible. Human languages are redundant i.e. certain characters are used more frequently than others. This fact can be exploited.

- In English 'e' is the most common letter followed by 't', 'r', 'n', 'o', 'a' etc. Letters like 'q', 'x', 'j' are less frequently used.

- Moreover, digrams like 'th' and trigrams like 'the' are also more frequent.

- Tables of frequency of these letters exist. These can be used to guess the plaintext if the plaintext is in uncompressed English language.

Playfair Cipher

- In this technique multiple (2) letters are encrypted at a time.

- This technique uses a 5 X 5 matrix which is also called key matrix.

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

- The plaintext is encrypted **two letters at a time**:
  - Break the plaintext into pairs of two consecutive letters.
  - If a pair is a repeated letter, insert a filler like 'X'in the plaintext, eg. "Balloon" is treated as "ba lx lo on".
  - If both letters fall in the same row of the key matrix, replace each with the letter to its right (wrapping back to start from end), eg. "AR" encrypts as "RM".
  - If both letters fall in the same column, replace each with the letter below it (again wrapping to top from bottom), eg. "MU" encrypts to "CM".
  - Otherwise each letter is replaced by the one in its row in the column of the other letter of the pair, eg. "HS" encrypts to "BP", and "EA" to "IM" or "JM" (as desired)
- Security is much improved over monoalphabetic as here two letters are encrypted at a time and hence there are 26 X 26 =676 diagrams and hence it needs a 676 entry frequency table.
- However, it can be broken even if a few hundred letters are known as much of plaintext structure is retained in cipher text.

Hill Cipher

- This cipher is based on linear algebra.
- Each letter is represented by numbers from 0 to 25 and calculations are done m dulo 26.

- This encryption algorithm takes m successive plaintext letters and substitutes them with m cipher text letters.
- The substitution is determined by m linear equations. For m = 3, the system can be described as:

$$c_1 = (k_{11}p_1 + k_{12}p_2 + k_{13}p_3) \ \text{Nod } 26$$
$$c_2 = (k_{21}p_1 + k_{22}p_2 + k_{23}p_3) \ \text{Nod } 26$$
$$c_3 = (k_{31}p_1 + k_{32}p_2 + k_{33}p_3) \ \text{Nod } 26$$

- This can also be expressed in terms of row vectors and matrices.

$$(c_1 \ c_2 \ c_3) = (p_1 \ p_2 \ p_3) \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \ \text{Nod } 26$$

Where **C** and **P** are row vectors of length 3 representing the plaintext and cipher text, and **K** is a 3 X 3 matrix representing the encryption key

- Key is an invertible matrix K modulo 26, of size m. For example:

$$K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \qquad K^{-1} = \begin{pmatrix} 4 & 19 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

- Encryption and decryption can be given by the following formulae:

Encryption: $C = PK \ \text{Nod } 26$

Decryption: $P = CK^{-1} \bmod 26$

- The strength of the Hill cipher is that it completely hides single-letter frequencies.
- Although the Hill cipher is strong against a cipher text-only attack, it is easily broken with a known plaintext attack.
  - Collect m pair of plaintext-cipher text, where m is the size of the key.
  - Write the m plaintexts as the rows of a square matrix P of size m.
  - Write the m cipher texts as the rows of a square matrix C of size m.
  - We have that C=PK mod 26.
  - If P is invertible, then K=P^{-1}C mod 26,
  - If P is not invertible, then collect more plaintext-cipher text pairs until an invertible P is obtained.

The Vigenère cipher

- This is a type of polyalphabetic substitution cipher (includes multiple substitutions depending on the key). In this type of cipher, the key determines which particular substitution is to be used.
- To encrypt a message, a key is needed that is as long as the message. Usually, the key is a repeating keyword.
- For example, if the keyword is *deceptive*, the message "we are discovered save yourself" is encrypted as follows:
  Key: *deceptivedecept*
  Plaintext: wearediscovered
  Ciphertext: ZICVTWQNGRZGVTW
- Encryption can be done by looking in the Vigenere Table where ciphertext is the letter key's row and plaintext's column or by the following formula:

$$C_i = (P_i + K_{i \text{ Nod N}}) \text{ Nod } 26$$

- Decryption is equally simple. The key letter again identifies the row. The position of the cipher text letter in that row determines the column, and the plaintext letter is at the top of that column.
- The strength of this cipher is that there are multiple ciphertext letters for each plaintext letter, one for each unique letter of the keyword.
- Thus, the letter frequency information is obscured however, not all knowledge of the plaintext structure is lost.

Vernam Cipher

- This system works on binary data (bits) rather than letters.
- The technique can be expressed as follows:

$$C_i = P_i \oplus K_i$$

  Where
  P_i = ith binary digit of plaintext.
  K_i = ith binary digit of key.
  C_i = ith binary digit of ciphertext.
  $\oplus$ = exclusive-or (XOR) operation
- Thus, the ciphertext is generated by performing the bitwise XOR of the plaintext and the key.
- Decryption simply involves the same bitwise operation:

$$P_i = C_i \oplus K_i$$

- The essence of this technique is the means of construction of the key.
- It was produced by the use of a running loop of tape that eventually repeated the key, so that in fact the system worked with a very long but repeating keyword.

- Although such a scheme has cryptanalytic difficulties, but it can be broken with a very long ciphertext or known plaintext as the key is repeated.

One-Time Pad

- In this scheme, a random key that is as long as the message is used.
- The key is used to encrypt and decrypt a single message, and then is discarded. Each new message requires a new key of the same length as the new message.
- This scheme is unbreakable.
- It produces random output that bears no statistical relationship to the plaintext.
- Because the ciphertext contains no information whatsoever about the plaintext, there is simply no way to break the code.
- For any plaintext of equal length to the ciphertext, there is a key that produces that plaintext.
- Therefore, if you did an exhaustive search of all possible keys, you would e   d up with many legible plaintexts, with no way of knowing which the intended plaintext was.
- Therefore, the code is unbreakable.
- The security of the one-time pad is entirely due to the randomness of the key.

- The one-time pad offers complete security but, in practice, has two fundamental difficulties:
  o There is the practical problem of making large quantities of random keys. Any heavily used system might require millions of random characters on a regular basis. Supplying truly random characters in this volume is a significant task.
  o Another problem is that of key distribution and protection. For every message to be sent, a key of equal length is needed by both sender and receiver.
- Because of these difficulties, the one-time pad is used where very high security is required.
- The one-time pad is the only cryptosystem that exhibits **perfect secrecy**.

Transposition Techniques

- A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is referred to as a transposition cipher.
- The simplest such cipher is the **rail fence** technique.

Rail Fence Technique

- Encryption involves writing plaintext letters diagonally over a number of rows, then read off cipher row by row.
- For example, the text "meet me after the party" can be written (in 2 rows) as:

m e m a t r h p r y

e t e f e t e o a t

- Ciphertext is read from the above row-by-row:
  MEMATRHPRYETEFETEAT
- This scheme is very easy to cryptanalyze as no key is involved.
- Transposition cipher can be made significantly more secure by performing more than one stage of transposition. The result is a more complex permutation that is not easily reconstructed.

Difference between Symmetric and Asymmetric key cryptography

Symmetric key Cryptography	Asymmetric Key Cryptography
Symmetric key cryptography uses the same secret (private) key to encrypt and decrypt its data	Asymmetric key cryptography uses a public and a private key to encrypt and decrypt its data
The secret key must be known by both parties.	The public key is known to anyone with which they can encrypt the data but it can only be decoded by the person having the private key
In key distribution process, key information may have to be shared which decreases the security.	Here, the need for sharing key with key distribution center is eliminated.
Symmetric key encryption is faster than asymmetric key.	It is Slower than symmetric key encryption.
Basic operations used in encryption/ decryption are transposition and substitution.	It uses mathematical functions.