gradeup

Network Security

Prep Smart. Stay Safe. go Gradeup

gradeup.co

Network Security

Content :

CRYPTOGRAPHY

The study of various ways to disguise messages in order to avoid the interception from an authorized interceptor is known as cryptography.

ENCIPHER AND ENCRYPTY

The terms encipher and encrypt correspond to the message transformations performed at the transmitter in order to disguise the message.

DECIPHER AND DECRYPT

The terms decipher and decrypt correspond to the inverse transformations performed at the receiver in order to recover the original message back.

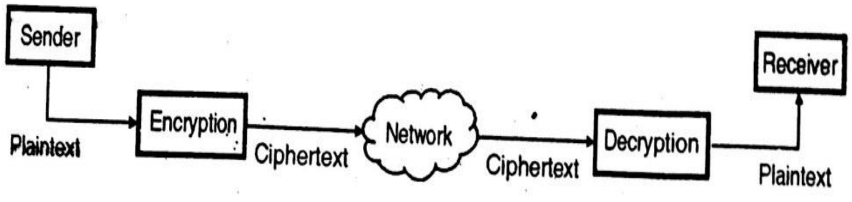
REASONS FOR USING CRYPTOSYSTEMS

The three major reasons for using the cryptosystems are:

1. To maintain privacy and to prevent an unauthorized person from extracting information from the communication channel. The process of extracting information from the channel is called eavesdropping.
2. To enable authentication for preventing unauthorized persons from injecting information into the channel. The process of injecting information is called spoofing.
3. Sometimes it is essential to provide the electronic equivalent of a written signature in order to avoid or settle any dispute between the transmitter and the receiver about what transmitted message is.

CRYPTOGRAPHY COMPONENTS

Cryptography is Greek word which means “secret writing” below figure shows the cryptography components.



PLAINTEXT

The original message produced by the sender is known as plaintext. It is data before transmission.

CIPHERTEXT

The plaintext is transformed into cipher text. The encryption grogram coverts the plaintext into cipher text.

DECRYPTION

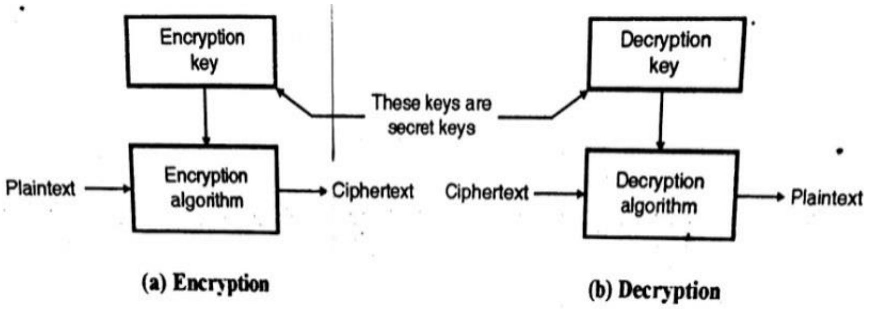
It is a process which is exactly opposite to encryption. The decryption algorithm at the receiver transforms the cipher text back to plain text.

CIPHERS

- The encryption and decryption algorithms together are referred to as ciphers. This term is also used to refer to different categories of algorithms in cryptography.
- It is not necessary to have a separate cipher for each sender or receiver pair. Instead it is possible to use public ciphers with secret keys for millions of pair sender and receiver.

A KEY

- A key is a value or a number. The cipher as an algorithm operates on the key.
- For the encryption of a message we have to use an encryption algorithm, an encryption key and the plaintext at the input as shown in below figure. At the output of the encryption box we get the cipher text.
- For decryption of the cipher text, we have to use a decryption algorithm, a decryption key and the cipher text at the point input as shown in below figure.
- After deception, we get the plaintext back.



NOTE: The encryption and decryption algorithms are public and any one can use them but the encryption and decryption keys are secret.

CHARACTERS IN CRYPTOGRAPHY

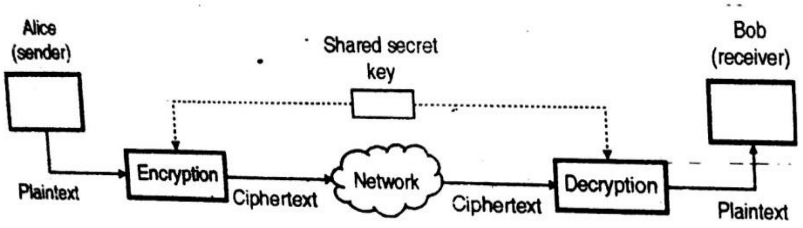
- In cryptography, generally three characters are used, namely Alice, Bob and Eve.
- Alice is a person who needs to send a secure data. Bob is a person who receives this data and Eve wants to disturb, interrupt the communication between Alice and Bob.

TYPE OF CRYPTOGRAPHY ALGORITHMS

- The cryptography algorithms can classified basically into two types as:
  1. Symmetric key or secret key cryptography algorithms and
  2. Public key or asymmetric cryptography algorithms
- Let us discuss them one by one.

SYMMETRIC KEY CRYPTOGRAPHY

- It is also called as the secret key cryptography, below figure shows the block schematic of symmetric key cryptography.



- In the symmetrical key cryptography, the same key (shared secret key) is used by the sender and receiver.
- The sender uses this key along with the encryption algorithm to encrypt the data, and the receiver uses it along with the decrypting algorithm to decrypt the data.
- The encryption algorithm makes use of a combination of addition and multiplication whereas the decryption algorithm uses a combination and division.

ADVANTAGES

1. The major advantages of symmetric key algorithm is that it is more efficient than the public key algorithms. It takes less time to encrypt a message using the symmetric key algorithm. This is because this key is of smaller size (length).

2. Hence symmetric key algorithms are used encryption and decryption of long messages.

DISADVANTAGES

1. The first disadvantages in that the sender and receiver both should have a unique symmetric key. So a large number of keys are required when the number of users increases.

2. The disadvantages of keys between two users can be difficult.

TRADITIONAL CIPHERS

- Traditional cipher are the earliest and simplest types of ciphers in which a character is used as a unit of data to be encrypted.
- The traditional ciphers are of two types:
  1. Substitution ciphers
  2. Transposition ciphers.

SUBSTITUTION CIPHERS

- This cipher operates on the principle of substitution of substitution of one symbol with the other.
- If the symbols in the plaintext are alphanumeric characters (such as A, B etc), then some of such characters are replaced by another characters.
- For example A can be replaced by C or B by Z etc. the symbols in the digit form (0, 1, 2, …) also can be replaced by another digits.

TYPES OF SUBSTITUTION

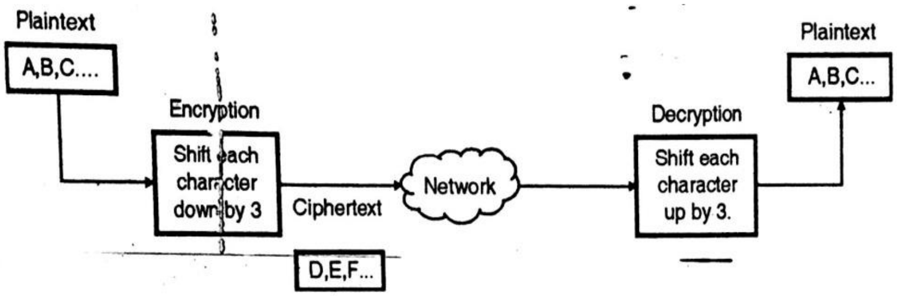
Substitution can be of one of the following two types:

1. Mon alphabetic substitution.

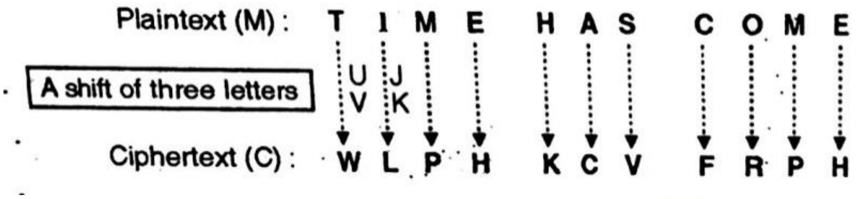
2. Polyalphabetic substitution.

MONOALPHABETIC SUBSTITUTION

- In this type of substitution, a character in the plaintext is always substituted by some other character in the cipher text regardless of its position in the text.
- For example if the encryption algorithm states that A in the plaintext is to be changed to F, then every A in the plaintext will be changed to F regardless of its position in the plaintext.
- The oldest recorded cipher is called the Caesar Cipher in which each character is shifted down by 3 as shown in below figure.



- Note that in encryption block each plaintext character is shifted down by 3 i.e. A is replaced by D, B is replaced by D etc.
- Below diagram shows the plaintext message "TIME HAS COME" and its corresponding cipher text. Note that each letter in the cipher text has been obtained by three end around shifting.



- The decryption block will shift each cipher text character up by 3 to obtain plaintext.
- In monoalphabetic substitution, the relationship between a character in the plaintext and that in the cipher text is always one as to one.

DISADVANTAGES

Mon alphabetic substitution is very simple. But the code can be attacked very easily. To overcome this disadvantages the polyalphabetic substitution method is used.

POLYALPBABETIC SUBSTITUTION

- In this technique each character in the plaintext is replaced by a group of character to obtain the cipher text. So the relation between a character in the plaintext to a character in the chipper text is one-to-many
- Another important point to be noted is that is that a character B can be changed to E at the beginning of the text but it may be changed to P in the middle of the text.
- In the polyalphabetic substitution, the key should tell us about which of the different possible characters can be chosen for encryption.

- Example: let encryption algorithm be defined as follows “Take the position of character in plaintext, divide it by 5, obtain the remainder and use the remainder as shift value”
- Then the character in position 1 is shifted by 1 where as that in position 8 is shifted by 3.
- An example of polyalphabetic substitution is the Vigenere cipher.

ADVANTAGES

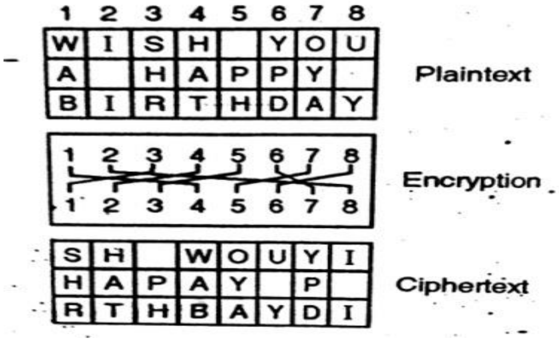
The advantages of polyalphabetic substitution is that it is difficult to attack successfully as compared to the monoalphabetic substitution.

DISADVANTAGES

However it is still possible to attack the code by trial and error.

TRANSPOSITION CIPHER

- In this type of cipher, the characters retain their plaintext form, but change their positions when cipher text is created.
- The plaintext is arranged in the form of a two dimensional table as shown in below figure and columns are interchanged as per key.



1	2	3	4	5	6	7	8
W	I	S	H		Y	O	U
A		H	A	P	P	Y	
B	I	R	T	H	D	A	Y

Plaintext

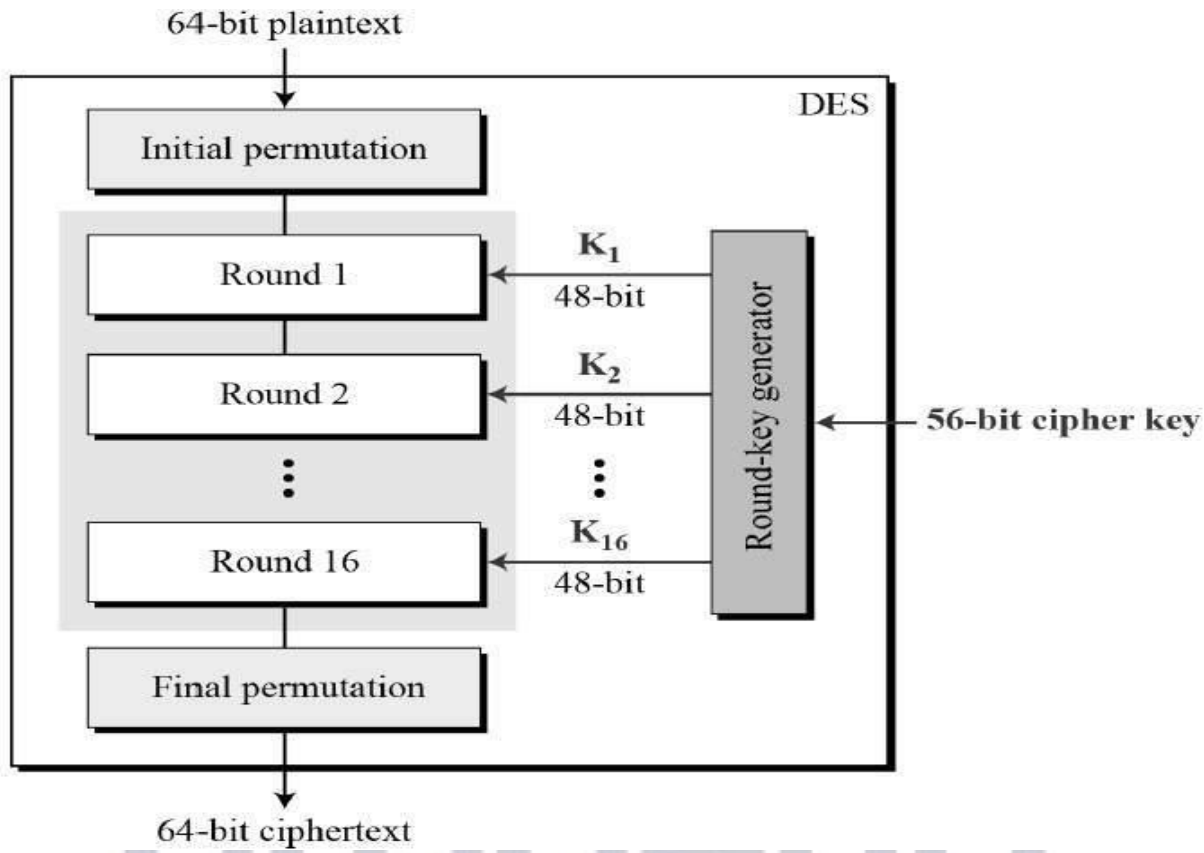
Encryption

S	H		W	O	U	Y	I
H	A	P	A	Y		P	
R	T	H	B	A	Y	D	I

Ciphertext

- But the transportation cipher is not very secure. It is still possible to attack by trial and error.
- Hence this method should be combined with the other methods for providing better security.

DATA ENCRYPTON STANDARD (DES)



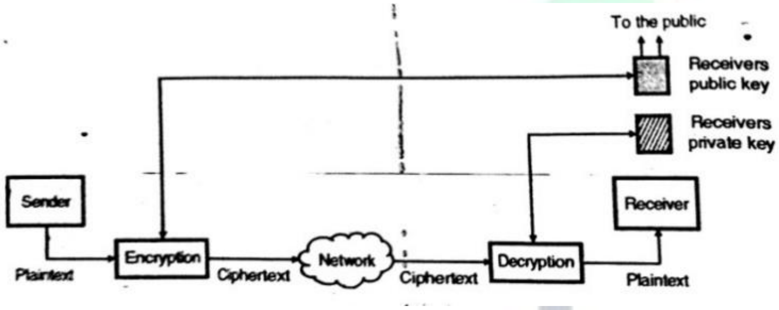
DES is developed in 1972, 56bit key is used for encryption. Steps are as follows. Below figure shows the details of operations so as to encrypt the message. Reverse steps are applied to decrypt the message to get original message.

1. Divide message to be encrypted in 64-bit blocks, say M1, M2, … Mn.
2. Initial transportation.
3. Encryption rounds 1 … 16 with keys 1 … 16 (grinding with XOR, shifting etc)
4. 32 bit swap.
5. Reverse transposition.
6. Now you get Cypher text C1, C2…

After these steps, message is sent to receiver.

PUBLIC KEY CRYPTOGRAPHY

- In the public key cryptography is also called as asymmetric key cryptography. This type of cryptography have are two keys.
  1. Private key
  2. Public key
- Out of them, the private key is kept by the received whereas the public key is announced to the public.
- Below figure shows the block schematic for public key cryptography.



- In this system the sender uses the public key to encrypt the message to be sent.
- At the receiver, this message is decrypted with the help of receivers private key.
- The public key used for encryption is different from the private key used for decryption. The public key is known to everyone but the private key is available only to an individual.

ADVANTAGES

1. There is no compulsion of using (sharing) the symmetric key by the sender and receiver.
2. The number of keys required reduces tremendously.

DISADVANTAGES

1. The algorithms used for highly complex
2. It takes a long time to calculate cipher text from plaintext.
3. It is necessary to verify the association between a sender and this public key.

Note: public key algorithm are more efficient for short message.

- One of the most commonly used public key algorithms is the RSA algorithms.

THE RSA ALGORITHM

- RSA is the most widely used public key algorithm. It is named after its creators - Rivest, Shamir and Adleman.
- The principle of RSA is simple. It is based on a fact that it is easy to multiply two prime numbers but it is very difficult to factor the product and get them back.
- The algorithm is as follows:
  1. Take two very large prime number A and B of equal lengths and obtain their product (N).

     $$\therefore N = A \times B$$

  2. Subtract 1 from A as well as B and take the product T.

     $$\therefore T = (A - 1)\ (B - 1)$$

  3. Choose the public key (E) which is a randomly chosen number such that it has to common factors with T.
  4. Obtain the private key (D) as follows

     $$D = E^{-1} \bmod T$$

  5. The rule for encryption of a block of plaintext M into cipher text (C) is as follows:

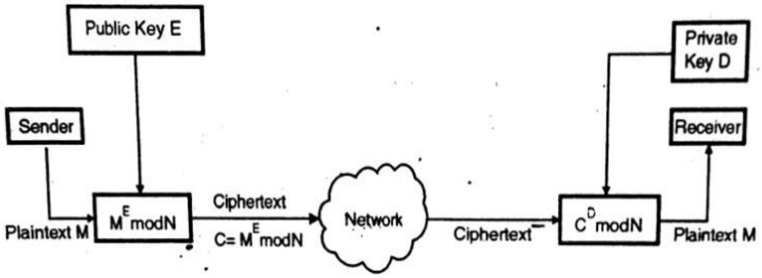
$$C = M^E \bmod N$$

That means the plaintext M is raised to the power of E (public key) and then divided by N. The mod term in above Equation indicates that the remainder of this division is sent as the cipher text C as shown in below figure.

6. The received message C at the receiver is decrypted to obtain the plaintext back by using the following rule

$$M = C^D \bmod N$$

The encryption and decryption process using the RSA algorithm is illustrated diagrammatically in below figure.



SECURITY OF RSA

- The security of RSA is decided by the ability of the hacker computer to factorize numbers.
- RSA provide a very good security because it uses very large prime numbers A and B their product is also large that an attempt to break the code using even the fastest computer will need a few years.
- But as the computers improved all the time, the time required to break the code will also reduce and one has to sue large keys. But then the time required for encryption and decryption also will increase.
- A key size of 768 bits is recommended for the personal use, 1024 bits for the corporate use and 2048 bits for extremely valuable keys.
- The user's key should be changed regularly in order to enhance security.

Example: If N = 119, public key E = 5, and private key D = 77 then demonstrate how to send the character F using RSA.

Solution: The character F is the sixth character in alphabets. So we can represent it by 6.

So as per RSA, the encryption is given below,

$$C = M^{E} \text{ mod } N$$

$$= 6^{5} \text{ mod } 119$$

The process of getting C is as follow

$$6^{5} = 7776$$

$$\therefore \quad C = 7776 \div 119$$

Since the quotient of this division is 65 and remainder is 41 we take C = 41.

This number is sent to the receiver as cipher text.

The receiver uses the decryption algorithm to get the plaintext M back as follows:

$$M = C^{D} \text{ mod } N$$

$$= 41^{77} \text{ mod } 119$$

$$6 \quad \text{… which is the original number}$$

APPLICATIONS OF CRYPTOGRAPHY

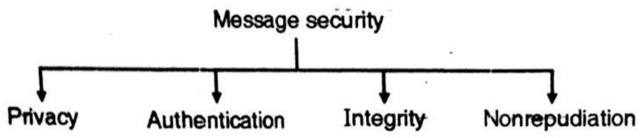
Some of the important applications of cryptography are:

1. Message security

2. User authentication.
3. Key management.

MESSGE SECURITY

Here, we will discuss the security measures applied to each single message. The security provides four services as shown in below figure.



1. **Privacy**
   - The transmitted message be such that only the intended receiver should be able to read it. No one else should be able to read it.
   - The privacy is achieved by means of using the encryption. We can use the symmetric key encryption and decryption.
   - It is also possible to use public key encryption to achieve the privacy.
2. **Message authentication:**
   - In message authentication, the receiver needs to be sure about the sender’s identity.
   - Digital signature is used for the providing the message authentication.
3. **Integrity**
   - We can define the meaning of integrity as the data arriving at the receiver exactly as it was sent. There should not be changed absolutely.
   - The digital signature can provide message integrity.
4. **Non-repudiation**
   - The meaning of nonrepudiation is that the receiver should be able to prove that , the message it has received has come from a specific sender.
   - The digital signature can provide the nonrepudiation.

ATTACKS ON SECURITY

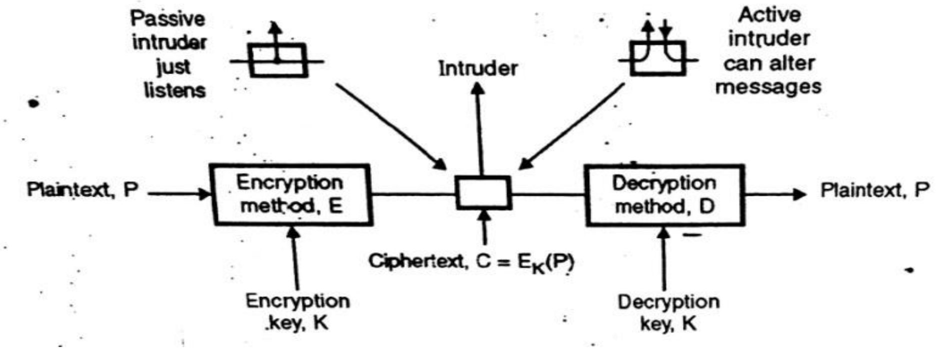
Security attacks can be classified in the following two categories depending on the nature of the attacker and below figure show Attacks and Encryption model.

PASSIVE ATTACT

The attack can only eavesdrop or monitor the network traffic. Typically this is the easiest form of attack and it can be performed without difficulty in many of the networking environments, examplebroadcast type networks such as wireless networks and Ethernet.

ACTIVE ATTACKS

The attacker is not only able to listen to the transmission but is also able to actively alter or obstruct it. Furthermore depending on the attackers actions, the following subcategories can be used to cover the majority of attacks.



EVAESDROPPING

This attack is used to gain knowledge of the transmitted data. This is a passive attack which is easily performed in many networking environments. However this attack can easily be prevented by using an encryption scheme to protect the transmitted data.

TRAFFIC ANALYSIS

The mail goal of this attack is not to gain direct knowledge about the transmitted data, but to extract information from characteristics of the transmission, example identity of the communicating nodes, amount of data transmitted etc. this information may allow the attacker to deduce thesensitive information, e.g. role of the communicating nodes, their position etc. unlike previously described attacks this one is more difficult to prevent.

IMPERSONATION

In this type the attacker uses the identity of another node to gain unauthorized access to a resource or data. This attack is often used as a prerequisite to eavesdropping. By impersonating the legitimate node the attacker can try to gain access to the encryption key used to protect the transmitted data. Once this key is known by the attacker, she can successfully perform the eavesdropping attack.

MODIFICATION

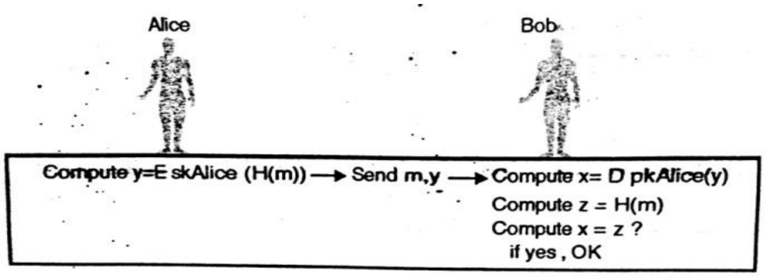
This attack modifies data during the transmission between the communication nodes, implying that the communicating nodes do not share the same view of the transmitted data. Example could be when the transmitted data represents a financial transaction where the attacker has modified the transactions value.

INSERTION

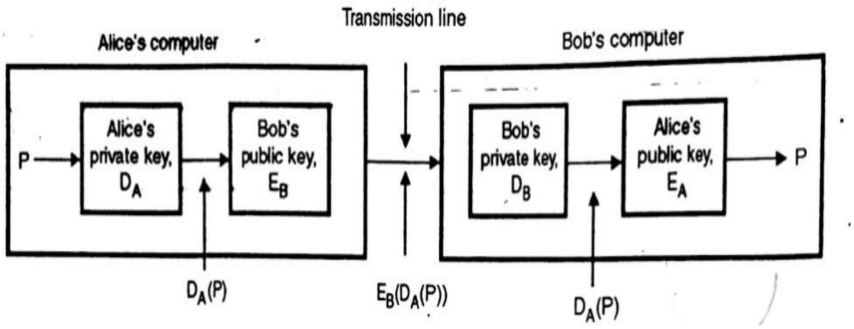
Insertion involves an unauthorized party, who inserts new data claiming that it originates from a legitimate party. This attack is related to that of impersonation.

DIGITAL SIGNATURE

- A digital signature is a data structure that provides proof of origin, i.e. Authentication and integrity, and depending on how it is used, it can also provide non-repudiation. Below figure illustrate how a digital signature is used.


Alice
Bob
Compute y=E skAlice (H(m)) → Send m,y → Compute x= D pkAlice(y)
Compute z = H(m)
Compute x = z ?
if yes , OK

- Alice wants to send a message to Bob, however she doesn't want it to be modified during transmission and Bob wants to be sure that the message really came from Alice.
- What Alice does is that she computes a hash digest (Digest H(m) is finger print of large message like CRCs) of the message which she encrypts with her private key skAlice.
- She then sends both the message and the encrypted digest which is here signature. Bob can then verify the signature of computing the hash digest of the message he received and comparing it with the digest he gets when decrypting the signature using Alice's public key pkAlice.
- If the digests are equal Bob knows that Alice sent the message and that it has not been modified since she signed it. (E-encryption, D-decryption).



- In above figure, signature by Alice is ensured, but anybody can decrypt using Alice public key which is available to every body. Below figure, (P = m message = plaintext)
- Not only ensures signature by Alice but also decryption by Bob since document is also encrypted by Bob’s public key. One more thing, we would like to reveal that in former figure that, not whole document.