CYBER SECURITY & CRYPTOGRAPHY (4)

techworldthink • March 10, 2022

11. Explain Network security model with the help of a neat diagram

A Network Security Model exhibits how the security service has been designed over the network to prevent the opponent from causing a threat to the confidentiality or authenticity of the information that is being transmitted through the network.

For a message to be sent or receive there must be a sender and a receiver. Both the sender and receiver must also be mutually agreeing to the sharing of the message. Now, the transmission of a message from sender to receiver needs a medium i.e. Information channel which is an Internet service.

A logical route is defined through the network (Internet), from sender to the receiver and using the communication protocols both the sender and the receiver established communication.

Well, we are concerned about the security of the message over the network when the message has some confidential or authentic information which has a threat from an opponent present at the information channel. Any security service would have the three components discussed below:

1. Transformation of the information which has to be sent to the receiver. So, that any opponent present at the information channel is unable to read the message. This indicates the encryption of the message.

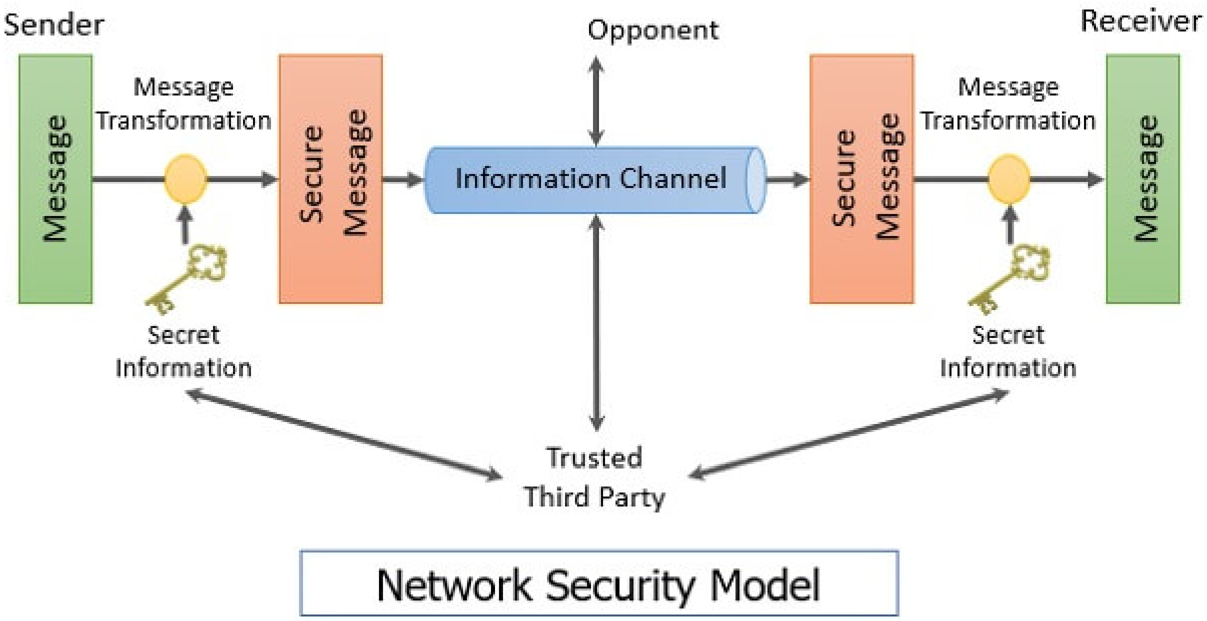
It also includes the addition of code during the transformation of the information which will be used in verifying the identity of the authentic receiver.

2. Sharing of the secret information between sender and receiver of which the opponent must not any clue. Yes, we are talking of the encryption key which is used during the encryption of the message at the sender's end and also during the decryption of message at receiver's end.

3. There must be a trusted third party which should take the responsibility of distributing the secret information (key) to both the communicating parties and

also prevent it from any opponent.

Now we will study a general network security model with the help of the figure given below:



Network Security Model

The network security model presents the two communicating parties sender and receiver who mutually agrees to exchange the information. The sender has information to share with the receiver.

But sender cannot send the message on the information cannel in the readable form as it will have a threat of being attacked by the opponent. So, before sending the message through the information channel, it should be transformed into an unreadable format.

Secret information is used while transforming the message which will also be required when the message will be retransformed at the recipient side. That's why a trusted third party is required which would take the responsibility of distributing this secret information to both the parties involved in communication.

So, considering this general model of network security, one must consider the following four tasks while designing the security model.

1. To transform a readable message at the sender side into an unreadable format, an appropriate algorithm should be designed such that it should be difficult for an opponent to crack that security algorithm.

2. Next, the network security model designer is concerned about the generation of the secret information which is known as a key.

This secret information is used in conjunction with the security algorithm in order to transform the message.

3. Now, the secret information is required at both the ends, sender's end and receiver's end. At sender's end, it is used to encrypt or transform the message into unreadable form and at the receiver's end, it is used to decrypt or retransform the message into readable form.

So, there must be a trusted third party which will distribute the secret information to both sender and receiver. While designing the network security model designer must also concentrate on developing the methods to distribute the key to the sender and receiver.

An appropriate methodology must be used to deliver the secret information to the communicating parties without the interference of the opponent.

It is also taken care that the communication protocols that are used by the communicating parties should be supporting the security algorithm and the secret key in order to achieve the security service.

Till now we have discussed the security of the information or message over the network. Now, we will discuss the network access security model which is designed to secure the information system which can be accessed by the attacker through the network.

You are well aware of the attackers who attack your system that is accessible through the internet. These attackers fall into two categories:

1. Hacker: The one who is only interested in penetrating into your system. They do not cause any harm to your system they only get satisfied by getting access to your system.

2. Intruders: These attackers intend to do damage to your system or try to obtain the information from the system which can be used to attain financial gain.

The attacker can place a logical program on your system through the network which can affect the software on your system. This leads to two kinds of risks:

a. Information threat: This kind of threats modifies data on the user's behalf to which actually user should not access. Like enabling some crucial permission in the system.

b. Service threat: This kind of threat disables the user from accessing data on the system.

Well, these kinds of threats can be introduced by launching worms and viruses and may more like this on your system. Attack with worms and viruses are the software attack that can be introduced to your system through the internet.

12. Describe the working of Playfair cipher and Hill cipher.

> *Playfair cipher*

The **Playfair cipher** was the first practical digraph substitution cipher. The scheme was invented in **1854** by **Charles Wheatstone** but was named after Lord Playfair who promoted the use of the cipher. In playfair cipher unlike traditional cipher we encrypt a pair of alphabets(digraphs) instead of a single alphabet.

It was used for tactical purposes by British forces in the Second Boer War and in World War I and for the same purpose by the Australians during World War II. This was because Playfair is reasonably fast to use and requires no special equipment.

The Playfair Cipher Encryption Algorithm:

The Algorithm consists of 2 steps:

1. **Generate the key Square(5×5):** The key square is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table (as the table can hold only 25 alphabets). If the plaintext contains J, then it is replaced by I. The initial alphabets in the key square are the unique alphabets of the key in the order in which they appear followed by the remaining letters of the alphabet in order.
2. **Algorithm to encrypt the plain text:** The plaintext is split into pairs of two letters (digraphs). If there is an odd number of letters, a Z is added to the last letter.

For example:

```
PlainText: "instruments"
After Split: 'in' 'st' 'ru' 'me' 'nt' 'sz'
```

1. Pair cannot be made with same letter. Break the letter in single and add a bogus letter to the previous letter.

Plain Text: *"hello" ,* ***After Split:*** *'he' 'lx' 'lo' , Here* ***'x'*** *is the bogus letter.*

2. If the letter is standing alone in the process of pairing, then add an extra bogus letter with the alone letter

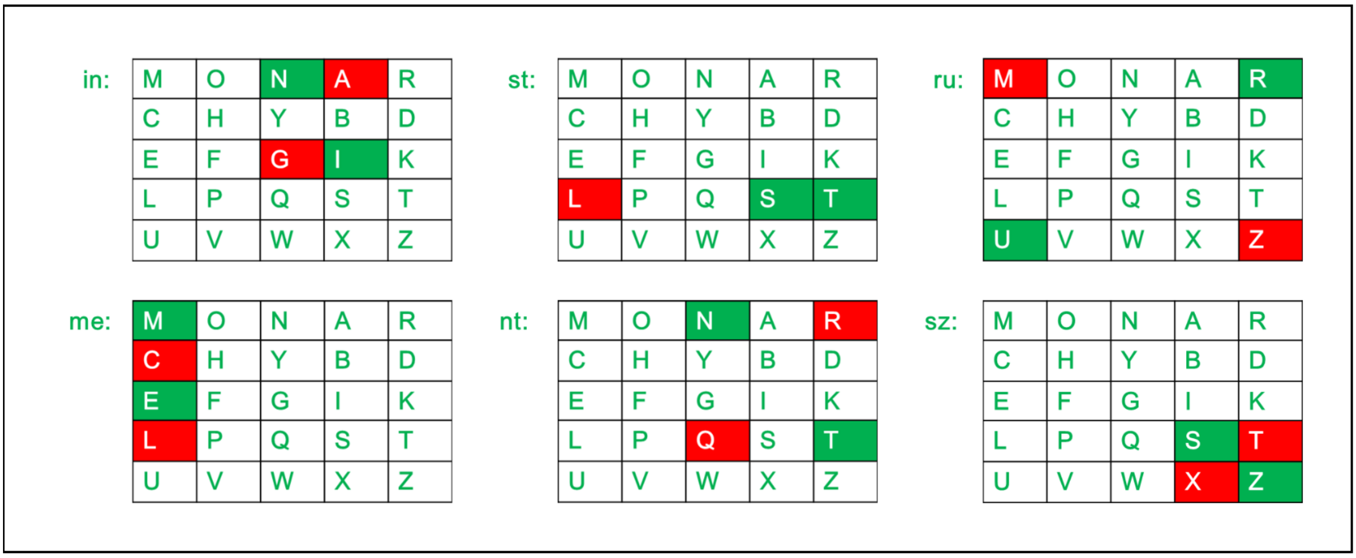
Plain Text: *"helloe" ,* ***AfterSplit:*** *'he' 'lx' 'lo' 'ez' , Here* ***'z'*** *is the bogus letter.*

Rules for Encryption:

- **If both the letters are in the same column**: Take the letter below each one (going back to the top if at the bottom).
- **If both the letters are in the same row**: Take the letter to the right of each one (going back to the leftmost if at the rightmost position).
- **If neither of the above rules is true**: Form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.

For example:

```
Plain Text: "instrumentsz"
Key : "MONARCHY"
Encrypted Text: gatlmzclrqtx
Encryption:
  i -> g
  n -> a
  s -> t
  t -> l
  r -> m
  u -> z
  m -> c
  e -> l
  n -> r
  t -> q
  s -> t
  z -> x
```



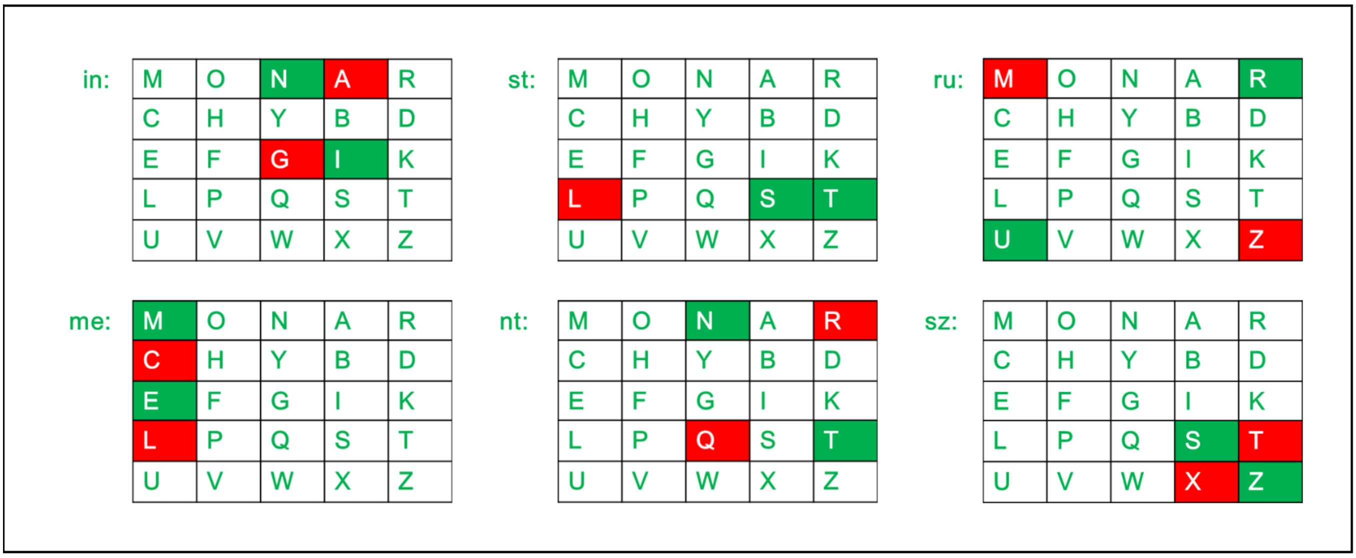
Example of encryption

Rules for Decryption:

- **If both the letters are in the same column**: Take the letter above each one (going back to the bottom if at the top).
- **If both the letters are in the same row**: Take the letter to the left of each one (going back to the rightmost if at the leftmost position).
- **If neither of the above rules is true**: Form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.

For example:

```
Plain Text: "gatlmzclrqtx"
Decrypted Text: instrumentsz
Decryption:
(red)-> (green)
  ga -> in
  tl -> st
  mz -> ru
  cl -> me
  rq -> nt
  tx -> sz
```



Example of Decryption

Hill cipher

Hill cipher is a polygraphic substitution cipher based on linear algebra.Each letter is represented by a number modulo 26. Often the simple scheme A = 0, B = 1, …, Z = 25 is used, but this is not an essential feature of the cipher. To encrypt a message, each block of n letters (considered as an n-component vector) is multiplied by an invertible n × n matrix, against modulus 26. To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.

The matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible n × n matrices (modulo 26).

Examples:

```
Input  : Plaintext: ACT
         Key: GYBNQKURP
Output : Ciphertext: POH
...................................
Input  : Plaintext: GFG
```

```
          Key: HILLMAGIC
Output : Ciphertext: SWK
```

Encryption

We have to encrypt the message ‘ACT’ (n=3).The key is ‘GYBNQKURP’ which can be written as the nxn matrix:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

Cipherkey

The message ‘ACT’ is written as vector:

$$\begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$$

message vector

The enciphered vector is given as:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} = \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} \equiv \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \pmod{26}$$

enciphered vector

which corresponds to ciphertext of 'POH'

Decryption

To decrypt the message, we turn the ciphertext back into a vector, then simply multiply by the inverse matrix of the key matrix (IFKVIVVMI in letters).The inverse of the matrix used in the previous example is:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}^{-1} \equiv \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \pmod{26}$$

inverse matrix

For the previous Ciphertext 'POH':

$$\begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \equiv \begin{bmatrix} 260 \\ 574 \\ 539 \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} \pmod{26}$$

Decrypt

which gives us back ‘ACT’.

Assume that all the alphabets are in upper case.