Enhancing Data Security by Adapting Network Security and Cryptographic Paradigms

Pushpa B R

Lecturer, Department of Computer Science
Amrita Vishwa Vidyapeetham,
Mysore Campus, Karnataka, India

***Abstract*— Network security is one of the significant aspects of information security. Network security is involved in various business organizations, enterprises, and other types of institutions and it has become a pivotal function in building and maintaining today's modern high-growth networks. Cryptography is a technology used to provide of information security by encoding the data. It provides a high secured data transmission by encrypting the data that cannot be accessed by a third party. This paper encompasses the basics of network security and types of symmetric algorithms and new approach for symmetric encryption algorithm for encryption and decryption of data and the merits of the new proposed algorithm.**

***Keywords*— Network Security Cryptography Symmetric and Asymmetric keys, Block Ciphers.**

I. Introduction

Network security involves securing a computer network infrastructure in which the network security issues are handled by a network administrator or system administrator who implements the security policy, network software and hardware which is needed to protect a network and the resources from the unauthorized access. Cryptography involves securing a data over the wireless communication. There was a real need of security as the computer application was developed for transforming the confidential data. There was a chance for intruder to capture the information as they travel from the client machine to the sever. So it is necessary to make use of cryptography techniques to provide the data security by providing user id and password which authenticate a user and other method is by encoding the information.

II. Cryptography

Cryptography is a technique that transforms plain text into an unreadable format (encrypt) called cipher text, then converting back the cipher text (decrypt) to plain text. Two people can communicate securely by encrypting the messages sent between them and by making use of keys shared by sender and receiver the decryption can be achieved.

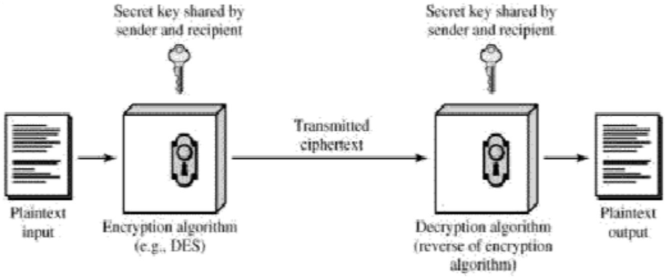
Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Fig. 1 The Block Diagram of Cryptosystem

A. Principles of Security—the CIA Model

The CIA provides a measurement tool for security implementations. These principles are applicable across the entire spectrum of security analysis.

Confidentiality prevents unauthorized access of sensitive information. It ensures that the necessary level of secrecy is enforced .Cryptography and encryption methods are examples of attempts to ensure the confidentiality of data transferred from one computer to another. Cryptography provides a secure transmission protecting the sensitive data traversing across the shared medium.

Integrity prevents unauthorized modification of data, systems, and information, thereby providing assurance of the accuracy of information and systems. A common type of a security attack is man-in-the-middle. In this type of attack, an intruder intercepts data in transfer and makes changes to it.

Availability is the prevention of loss of access to resources and information to ensure that information is available for use when it is needed. Denial of service (DoS) is one of several types of security attacks that attempts to deny access to the appropriate user, often for the sake of disruption of service.

III. Symmetric and Asymmetric key Cryptography

A. Asymmetric key cryptography

Public-key cryptography, also known as asymmetric cryptography, refers to a cryptographic algorithm which requires two separate keys, one key is used for encryption and other key is used for decryption. Although different, the two parts of this key pair are mathematically linked. The public key is used to encrypt plaintext or to verify a digital signature, whereas the private key is used to decrypt ciphertext or to create a digital signature

In Asymmetric cryptography initially a network user receives a public and private key pair from a certificate authority. Any other user who wants to send an encrypted message can get the intended recipient's public key from a public directory. They use this key to encrypt the message, and they send it to the recipient. When the recipient gets the message, they decrypt it with their private key, which no one else should have access to.

B. Symmetric key cryptography

Symmetric Encryption is one of the oldest algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of cipher text. The keys may be identical or there may be a simple transformation to go between the two keys. These key can be a number, a word, or just a string of random letters, is applied to the text of a message to change the content in a particular way. The key is combined with a plain text for creating a cipher text and the same key is used with the cipher text for decryption.

Symmetric cryptography is split into block ciphers and stream ciphers.

A stream cipher is a symmetric key cryptography where plaintext is encrypted one byte at a time, to give a digit of the cipher text stream. The plain text is combined with a pseudorandom cipher digit stream (keystream).

A block cipher is a deterministic algorithm operating on fixed-length groups of bits, called *blocks*, with an unvarying transformation that is specified by a symmetric key.

A block cipher breaks the plaintext into equally-sized blocks. A block is simply a group of characters, such as 'cipherblock'. The most popular block size is 8 characters, or 64 bits. If the total number of characters in the plaintext is not divisible by the block size (i.e. a complete last block cannot be made), then extra characters are generally added on to the end of the plaintext until a complete last block can be formed. The problem with block cipher is repeating text, so that the same cipher text is created. This may give clue to the intruder. To overcome from this problem the chaining mode is used where the previous block of cipher text is combined with the current block, such that more security is achieved.

IV. REASONS FOR USE OF SYMMETRIC APPROACH FOR ENCRYPTION AND DECRYPTION

- Single key encryption
- It uses a less computer resources
- Simple and faster

V. AN APPROACH TO SYMMETRIC ENCRYPTION

A. Encryption algorithm:

Step 1: Select a text file which contains text, by removing blank spaces from text file.

Step 2: Convert each character of the text data into their ASCII values.

Step 3: Perform the 9's complement of each ASCII value.

Step 4: Generate equivalent 8421 binary value of each digit.[Binary value should be in 1Byte (i.e. 8bit) e.g. for decimal 65 the value should be 01100101]

Step 5: Arrange binary values into a complete string.

Step 6: From the MSB (Most Significant Bit), extract1Byte data (i.e.8bit). Take a key of 8 bit binary by performing the 9s complement of key value.

Step 7: Perform XOR operation of key and first block of plain text.

Step 8: Perform 1s complement of the result of step 5. This results in encrypting of first block.

Step 9: Perform XOR of key and cipher text and the result is XOR ed with next 8 bits of plain text. This results in encrypting of second block and the string is reversed.

Step 10: The reversed string is XORed with key and the result is XOR ed with next 8 bits of plain text. This results in encrypting of third block and the string is reversed and the process is continued till the end of the string is reached.

Step 11: Except the first and the last block all other cipher block are reversed.

B. Decryption algorithm

Step 1: Extract 1Byte from MSB of the cipher text.

Step 2: Perform XOR of cipher text and key value. Take the 1s complement.

Step 3: Perform XOR of first 8bits (MSB) and reversed next block of cipher text. Again perform XOR of result and key. This decrypts the second block of data.

Step 4: Perform XOR of second block of 8bits (MSB) and reversed next block of cipher text. Again perform XOR of result and key. This decrypts the third block of data and the process continues till the end of the string is reached.

C. Example:

Suppose the text is taken as "DATA" .Now according to the above steps we will get the following:

For Encryption:

Step 1: ASCII values of each character and their 9's complement is shown in below.

Character	D	A	T	A
ASCII value	68	65	84	65

Step 2: Perform the 9's complement of each ASCII value. Generate equivalent 8421 binary value of each digit.

```
99 99 99 99
68 65 84 65
-----------------
31 34 15 34
00110001  00110100  00010101  00110100
```

Step 3: From the MSB(most Significant Bit), extract1Byte data 00110001 . Take a key of 8 bit binary by performing the 9s complement of key value.

Key = C

ASCII value 65

```
9's complement     99
                    65
                   ---
                   32
 8421 code      00110010
```

Step 4: Perform XOR operation of 00110010 and 00110001, the result is 00000011.Perform 1s complement 11111100.

Step 5: Perform XOR of key and cipher text and the result is XOR ed with next 8 bits of plain text.

```
11111100
00110010
--------------
11001110
00110100
-------------
11111010
```

Step 6: The reversed string 01011111 is XORed with key 00110010and the result 01101101 is XOR ed with next 8 bits of plain text 00010101. This gives 01111000.

Step 7: The reversed string 00011110 is XORed with key 00110010and the result 00101100 is XOR ed with next 8 bits of plain text 00110100. This gives 00011000.

11111100 11111010 0111000 00011000

Step 8: Except the first and the last block all other cipher block are reversed.

cipher text : **11111100 01011111 00011110 00011000**

For Decryption:

Step 1: Extract 1Byte from MSB 11111100 of the cipher text and perform XOR of 11111100 and key value 00110010

```
11111100
00110010
-------------
11001110
```

Take the 1s complement- 00110001

Step 2: Perform XOR of first 8bits (MSB) 11111100 and reversed next block of cipher text 11111010 .

```
11111100
11111010
-------------
00000110
```

Again perform XOR of result 00000110 and key 00110010

```
00000110
00110010
-------------
00110100
```

Step 3: Perform XOR of second block of 8bits (MSB) 01011111 and reversed next block of cipher text 01111000.

```
01011111
01111000
-------------
00100111
```

Again perform XOR of result and key

```
00100111
00110010
---------------
00010101
```

Step 4: Perform XOR of third block of 8bits (MSB) 00011110 and next block of cipher text 00011000.

```
00011110
00011000
--------------
00000110
00110010
--------------
00110100
```

Plain text: **00110001 00110100 00010101 00110100**

31 34 15 34

D A T A

VI. CONCLUSION

The method proposed in this paper is simple and effective way for the text encryption and decryption. The simple key is used to encrypt and decrypt the file. This method is suitable for small amount of data. The proposed algorithm of symmetric encryption works better to encrypt and decrypt the file. The plain text is encrypted using key and again the same key is used for decrypting the file so that it provides better security.

REFERENCES

[1] S. William, *Cryptography and Network Security:Principles and Practice*, 2nd edition, Prentice-Hall, Inc.,1999.

[2] S. Hebert, "*A Brief History of Cryptography*", an article available athttp://cybercrimes.net/aindex.htm

[3] Sumedha Kaushik1 "*Network Security Using Cryptographic Techniques* ", *International Journal of Advanced Research in Computer Science and Software Engineering*.

[4] Atul Kahate, *Computer and Network security*.

[5] Fundamentals of Computer Security, Springer publications -Basic Cryptographic Algorithms‖, an article available at www.itsc.state.md.us/oldsite/info/InternetSecurity/Crypto/CryptoIntro.htm#Algorithms

[6] http://library.thinkquest.org/27993/crypto/dig/block2.shtml