8-Block Security System for Digital Envelope

[1]Homer Benny Bandela, [2]G Samuel Vara Prasad Raju

[1]Assistant Professor, Department of Computer Science and Engineering, Sir C R R College of Engineering, Eluru,
[2]Professor, Department of Computer science and Engineering, Visakhapatnam,
Email: [1]homer.benny@gmail.com, [2]gsvprajudr9@gmail.com

Abstract— The sensitive information stored on computers and transmitted over the Internet need to ensure information security and safety measures. Without our knowledge, the Intruders sneak into the systems, misuse it and even create back doors to our computer systems. System contains valuable information which should not be in hands of anti-social elements. There is a possibility to hack the systems in network. It can be server or any peer in network. Thus, there must not be any compromise in securing our resources. Hence, Cryptography is mainly used to ensure secrecy. Various security measures are in force in order to protect the sensitive data from intruders, most of them need a strong cryptographic base. Cryptography provide solutions for four different security areas confidentiality, authentication, integrity and control of interaction between different parties involved in data exchange ultimately which tend to the security of information. Digital Envelopes are secured and promises user authentication and non repudiation. Digital Envelopes are made using a combination of Symmetric key Cryptography and Asymmetric key Cryptography. In this paper we present a new technique for data encryption and RSA algorithm for making a Digital Envelope.

Index Terms— Digital Envelope, Symmetric key, public key, private key, Networks.

I. INTRODUCTION

In this era E-Commerce has become very prominent. At the same time security for the transactions through these E-Commerce tools also became important. These tools are globally connected to one another by means of inter networking. Question is whether the data being transferred through the internet is secured against unauthorized access or not.

II. PROBLEM

A. Principles of security

A durable set of security principles are to be satisfied for the data being protected.

- Confidentiality
- Integrity
- Authentication
- Non Repudiation

If one of the above is compromised, data is lost to intruders.

- The principle of Confidentiality specifies that only the sender and the intended recipient should be able to access the contents of message.
- Integrity means that data cannot be modified undetectably.
- Authentication mechanisms help in the establishment of proof of identities.
- Non Repudiation implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction.

B. Methods of attack

Depending on security parameters and the access control policy Attack methods are categorized into:

- Interception
- Fabrication
- Modification

III. LITERATURE STUDY

A. Wireless Multichannel Multipoint Broadcast Service for Mobile Stations

In wireless Multicast Broadcast Service (MBS), the common channel is used to multicast the MBS content to the Mobile Stations (MSs) on the MBS calls within the coverage area of a Base Station (BS), which causes interference to the dedicated channels serving the traditional calls, and degrades the system capacity. The MBS zone technology is proposed in Mobile Communications Network (MCN) standards to improve system capacity and reduce the handoff delay for the wireless MBS calls. In the MBS zone technology, a group of BSs form an MBS zone, where the macro diversity is applied in the MS, the BSs synchronize to transmit the

MBS content on the same common channel, interference caused by the common channel is reduced, and the MBS MSs need not perform handoff while moving between the BSs in the same MBS zone. However, when there is no MBS MS in a BS with the MBS zone technology, the transmission on the common channel wastes the bandwidth of the BS. It is an important issue to determine the condition for the MBS Controller (MBSC) to enable the MBS zone technology by considering the Quality of Services (QoS) for traditional calls and MBS calls are used to reduce the dependency over the common channel and also it is going to reduce the delay over the network. By enabling Dynamic Channel Allocation (DCA) and Enhance Dynamic Channel Allocation (EDCA) we are going to overcome these problems.

No security aspect in the paper.

B. Overcome of Router/ Gateway Problems in Wireless Networks

In world, main communication media is Networks. A computer network, or simply a network, is a collection of computers and other hardware interconnected by communication channels that allow sharing of resources and information. Where we can setup communication in between a small office, offices, towns, cities and any geographic place in world. Fast way of communicating is by Networks. Even though we are using sophisticated devices to achieve target goal but there are some minor problems which are under finger tip. Under magnified glass there are big and irritating. In this paper we will study about Computer Networks, problems related to router and solutions related to router. These days, having access to wireless broadband is an absolute necessity for home offices and small businesses. And after more than a decade of innovations, you would think that the standard wireless gateway/router would be a picture-perfect product by now. While many routers offer good features, most still come with flaws that can make life a lot harder, such as confounding setups or limited security. In paper we follow some problems and suggest some solutions to the problems.

This paper does not discuss about the security aspects.

C. Forced Protection Security Wall for Web Server on Network Attacks

The term web server can refer to either the hardware (the computer) or the software (the computer application) that helps to deliver web content that can be accessed through the Internet. Here we deal with software of the server. The most common use of web servers is to host websites, but there are other uses such as gaming, data storage or running enterprise applications. When they are active in network, there is a possibility to attack server by attackers. They can steal valuable information from the server or they can corrupt your system or some may overwrite falls information on existing data. They are also called as hackers. Black hats are meant to damage or do illegal operations on system. Once attacker enters into your server and nobody can stop them. This paper deals with the things that make you aware of such things. Possibly it gives some solutions to the problems which may prevent attackers to attack.

This paper gives brief information related to networks but does not deal with network security. Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

IV. PROPOSED SYSTEM

Various techniques are used to solve the attacks on system and to implement the security policies. These techniques differ from one another by the way of implementation and the application. Developing a digital envelope itself provides security for the data by

- Authentication
- Data Encryption

A. Digital Envelope Mechanism

Both asymmetric key cryptography and symmetric key cryptography does not solve all the problems in a practical security infrastructure individually. It would be very effective, if we combine both cryptographic mechanisms. This concept leads to the development of digital envelope. Digital envelopes are very efficient security solutions. Both the asymmetric key algorithms and symmetric key algorithms are used for data encryption. But in digital envelopes symmetric key algorithms are used to encrypt the data using a session key or one time symmetric key and the asymmetric key algorithms are used to encrypt the session key or one time symmetric key.

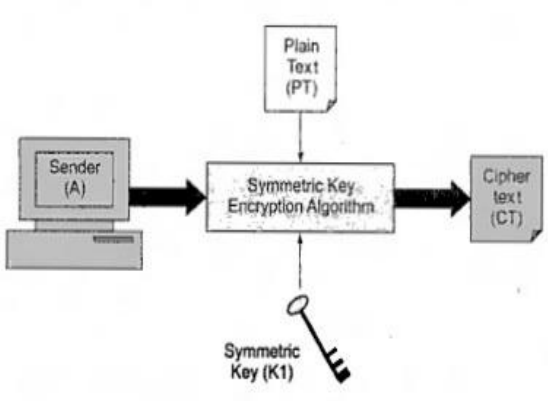


Figure 1: Encryption of plain text

Fig [1] shows the encryption of message sent by the sender (A) using a symmetric key encryption algorithm with symmetric key (k1). The resultant is the cipher text.

The symmetric key (k1) is encrypted by receiver (B) public key (k2) using a public key cryptographic encryption algorithm as shown in fig [2].

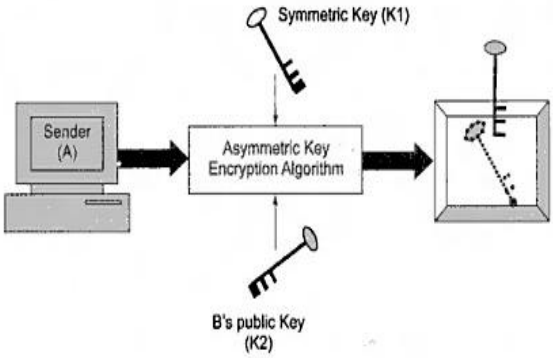


Figure 2: Encryption of Symmetric key

The resultant encrypted symmetric key is wrapped along with the cipher text (CT) to form a digital envelope as shown in fig [3]. This method is called key wrapping. The digital envelope is sent to the receiver (B) over the network.

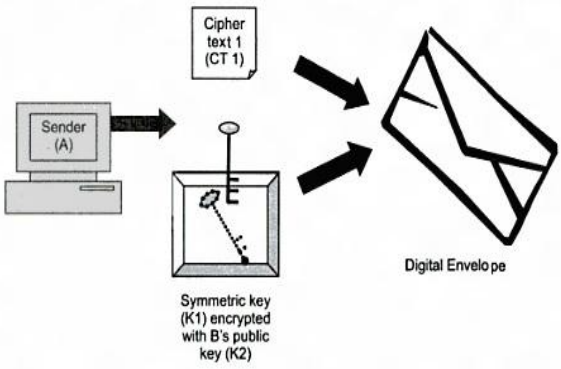


Figure 3: Generating a digital envelope

Upon receiving the digital envelope receiver (B) separates the cipher text (CT) and the encrypted one time symmetric key. Receiver uses his corresponding private key (k3) to decrypt the encrypted symmetric key as shown in fig [4].

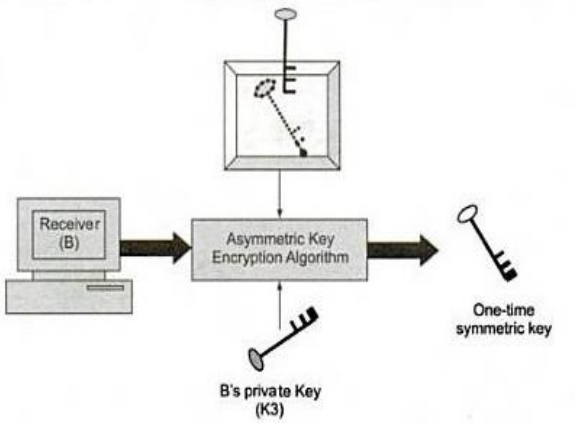


Figure 4: Retrieval of wrapped key

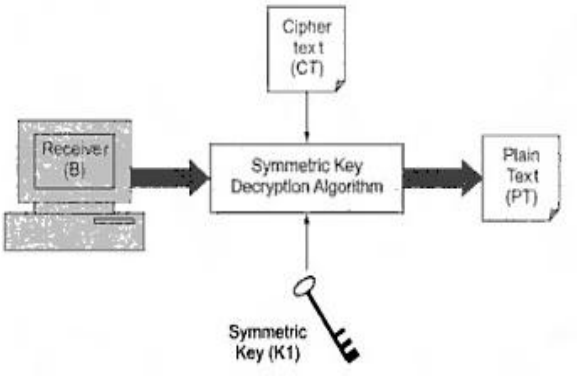


Figure 5: Decryption of Cipher text

Receiver (B) uses the symmetric key (k1) to decrypt the cipher text to get the original message sent by sender (A) as shown in fig [5].

In this paper we present a new technique for symmetric key encryption and decryption algorithm called "8-block cipher technique", and RSA algorithm as asymmetric key encryption algorithm.

V. DESIGN AND IMPLEMENTATION OF SYSTEM

8-block cipher technique is a combination of substitution and transposition techniques, which consists of 8 major blocks. Each major block is in turn divided into 256-bit sub blocks. Symmetric key length is 512-bits. The symmetric key is generally a one time usable key which is generated differently for each session. So this symmetric key can also be called as session key.

The session key and the data to be encrypted undergo several substitutions and transpositions. These are done in different phases. The algorithm is divided in to two parts.

- Sub key generation

- Data encryption

A. Sub key generation

- The session key generated of 512-bits is divided into equal halves i.e., 256-bits each say key1 and key2.
- Key 1 and key 2 are XOR-ed with each other to form a final key.
- The final key is left circularly shifted 32-bits for each major block which is used as a new final key for each major block.

B. Data Encryption

- The data is read as bytes and converted into hexadecimal codes.
- Hexadecimal codes are substituted by a set of predefined values.
- Reverse the whole data after the substitution.
- Divide the data into two equal halves, half 1 and half 2. The length of each half should be divisible by 256 else right padding is done until it is divisible by 256.
- XOR the half 1 with key 2 and half 2 with key 1.
- Combine the two halves half 1 and half 2 which gives an intermediate cipher.
- Split up the intermediate cipher into 8 major blocks. If necessary right padding should be done to divide into 256-bit sub blocks.
- Each major block is XOR-ed with final keys generated.
- All the encrypted major blocks are combined back to form the cipher text, i.e., data of file is encrypted.

The detailed flow chart representation is shown in fig [6].

C. RSA encryption of session key

The session key is encrypted based on the public key of the receiver. We use 512-bit RSA key pairs for encryption and decryption purposes as the session key is of length 512-bits.

D. Decryption

Firstly the session key is decrypted using the receiver's private key. Reverse process of encryption is applied to get plain text using the session key.

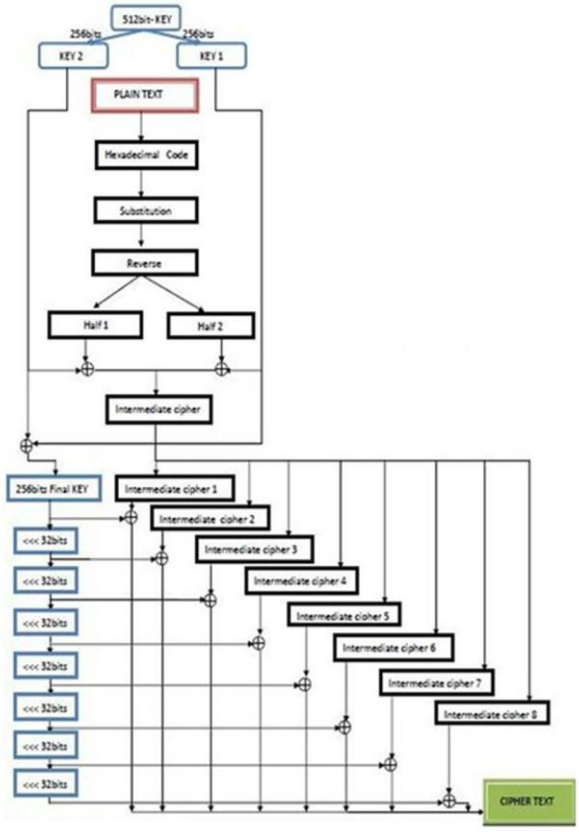


Figure 6: 8-block cipher technique encryption algorithm flow chart.

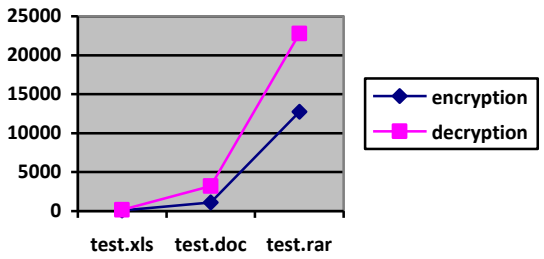
VI. RESULT

The desired technique has been successfully implemented using java programming language and various files have been experimented with varying file sizes.

The decryption time is doubled because of the encrypted file size being doubled. The reason is, during the hexadecimal code conversion a byte of data occupies two bytes of hexadecimal code. So finally the encrypted file size is doubled. However this doesn't reflect on the standards of the encryption. The encryption and decryption times are tabulated along with the file sizes.

Type	Original Size	Encrypted Size	Encryption Time (millisec)	Decryption Time (millisec)
test.xls	21KB	42KB	63	152
test.pdf	93KB	186KB	189	484
test.jpg	255KB	511KB	683	1290
test.doc	603KB	1.17MB	1094	3213
test.mp3	3.88MB	7.76MB	9081	18936
test.rar	4.67MB	9.36MB	12750	22774

Table 1: Encryption/Decryption times.



Graph depicting file size Vs encryption and decryption times from the table [1]

VII. CONCLUSION

The proposed technique has been implemented for text files, image files, audio and video files. It is being executed efficiently for all file formats and on various operating systems. Due to the hexadecimal conversion the file size is being doubled which doesn't have effect on the encryption standards. The predefined substitution of values in place of hexadecimal codes provide greater chances for protection because it is difficult to find which value is substituted for which hexadecimal code and also the values are encrypted during the encryption process. For different sessions different keys are generated in random and security is further enhanced by wrapping up of the key in encrypted form.

REFERENCES

[1] "Forced Protection Security Wall for Web Server on Network Attacks" By Homer Benny Bandela[1], Dr. G Samuel Vara Prasad Raju[2], T R S Prasad Babu[3]

[2] "Wireless Multichannel Multipoint Broadcast Service for Mobile Stations" By Homer Benny Bandela, K Chaitanya Deepthi, Prathipati Ratna Kumar

[3] "Overcome of Router/ Gateway Problems in Wireless Networks" Homer Benny Bandela, Chodagam Suresh Kumar, Donavalli Venkata Vidya Deepthi, Sala Krishna Rao, Dr. G Samuel Vara Prasad Raju

◈◈◈