Proceedings of the Second International Conference on Research in Intelligent and Computing in Engineering pp. 335–339
DOI: 10.15439/2017R48
ACSIS, Vol. 10 ISSN 2300-5963

Symmetric Key Encryption With Many Secret Keys

Vijaya Kumar S
Assistant Professor in MCA Dept
Saintgits College of Engineering
Pathamuttom, Kottayam, Kerala
vksudev@gmail.com

***Abstract*—One of the essential practices in the field of secured communication between two people is Cryptography. It confirms features like availability, authenticity, integrity and confidentiality of information. Also it enhances the mechanism of data security. For the purpose of encryption and decryption, in cryptography we have symmetric and asymmetric cryptography. Out of these, symmetric is the simplest and used widely due to its speed and feasibility in decrypting bulk messages, and requirement of limited computer resources. Symmetric key technique uses one secret key for cryptography, which opens the door for different kinds of security attacks. Through this paper I would like to introduce a Novel Symmetric key encryption and decryption using multiple secret keys. Here in this approach I am using different secret keys to encrypt different original texts.**

***Index Terms*—Symmetric and asymmetric cryptography, Information security, secret keys, block cipher.**

I. Introduction

Inoformation security is one of the key feature which requires due diligence and care to ensure the information security from various activities like unauthenticated access, modification, destruction, disclosure and use. Information security has the responsibility to make sure the security of the information throughout its life cycle, which means from the generation/creation of the information through its disposal. Irrespective of the state of the information it should be secured. If the access to information is protected then that kind of data should be restricted to a certain set of authorized persons who has enough access to that. In such cases, if the secured information is inside some device, say for example inside a computer, then proper security measurements should be applied to that computer device as well. In other words, some control access mechanism is required for those cases.

Encryption is the technique which transforms the original usable data to another form of the same data, which is not usable to unauthorized persons. Likewise the decryption is the process of transforming the encrypted data into its normal form through the help of a secret key, which can be done only by authorized users.

Basic types of cryptography are Symmetric key and asymmetric key cryptography. Same secret keys will be used in the Symmetric key cryptography; where as a private and public key is used in case of asymmetric key cryptography. Almost the entire encryption algorithm is based on the replacement technique, in which each letter will be mapped with another element.

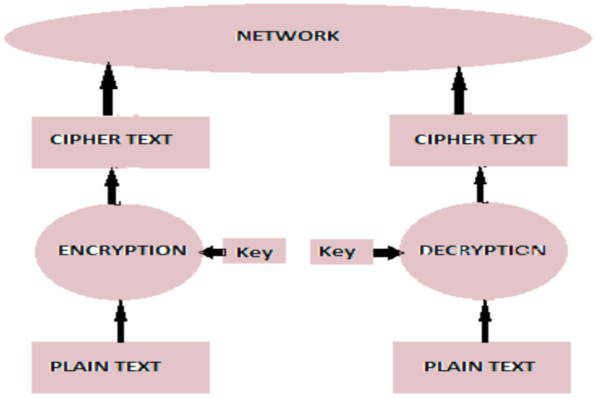


Fig 1:- Simple Cryptography Model.[7]

Asymmetric key or public key cryptography has a pair of keys, one public and one private. Both keys are used for the encryption and decryption purposes. Private Key is a secret key, which will not be shared with anybody. It is the owner's responsibility to keep this key safe. In Public key cryptography, the key will be accessible to all the users using that system. The advantage of Asymmetric key is its convenience and increased security. In this case, the private key will be kept as secret and will not be shared with anyone, while the public key will be used for encryption purpose. Disadvantage of the asymmetric key encryption is its slowness and the low feasibility for bulk message decryptions.

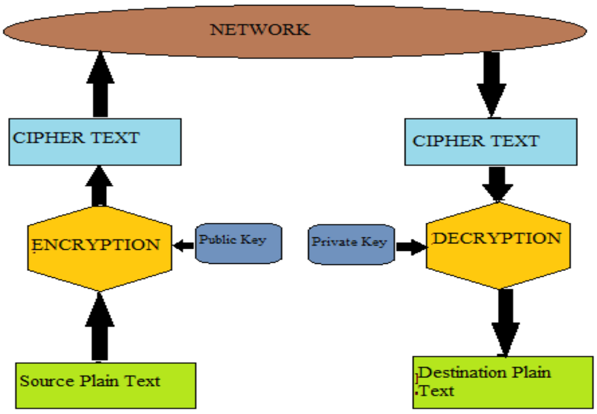


Fig 2:- Asymmetric Cryptography Model.[7]

Secret key is used in secret key encryption for encrypting & sending the plain text to the receiver end. The same key will be used at the receiving end for decrypting the cipher text. Other name of secret key encryption is symmetric key encryption because the same key is used on both the sides. The mandatory rule for this cryptography is that the secret key should be known to both the sides of the cryptography. The advantages of symmetric key encryption are feasibility and the speed in cryptography and also it's a feasible way to decrypt bulk messages. When comparing with asymmetric key cryptography, symmetric key cryptography is vulnerable to chosen plain text attacks, since the same secret key is shared among both sides.

In this paper I have tried to introduce the Novel Symmetric Key Cryptography, where multiple random keys will be in use to encrypt different message blocks. This paper is organized in the following order: symmetric key cryptography description, key distribution in the existing and the proposed symmetric key cryptography, symmetric key algorithm, the results and the conclusion of this study.

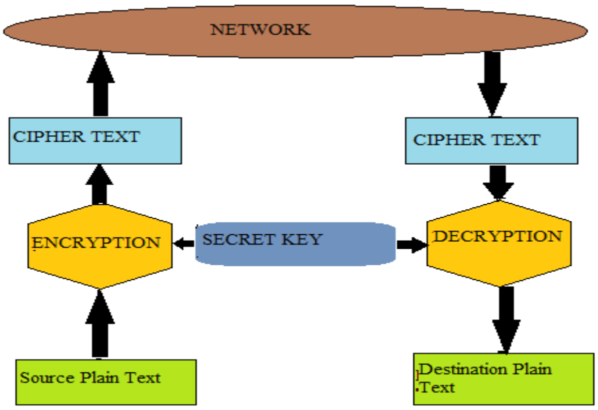


Fig 3:- Symmetric Cryptography Model.[7]

II. System Study

A. Symmetric Cryptography

The symmetric key cryptography can be categorized into two: block cipher and stream cipher. As the name implies, the stream buffer transforms one bit at a time, and different keys will be generated for each bit. Two types of stream ciphers are there: synchronous stream buffer and self synchronizing stream buffer. In self synchronizing stream buffers, each bit is calculated as a function of the previous n-bits in the key stream. While in Synchronous stream buffer, the key stream generated by it will be independent of the message stream but will be using the same key stream functions on both the sides. This will not propagate any transmission errors and is also periodic in nature, so there are possibilities to repeat the key stream.

TABLE I. Stream Cipher Encryption

Plain Text P:	Encryption E:	Secret Key K:	Cipher Text C:
P1	Ⓔ	K1	C1
P2	Ⓔ	K2	C2
P3	Ⓔ	K3	C3
P4	Ⓔ	K4	C4
P5	Ⓔ	K5	C5
P6	Ⓔ	K6	C6
P7	Ⓔ	K7	C7
P8	Ⓔ	K8	C8

In block cipher, the same key will be used by each of the blocks. In a block cipher, the same plain text will be encrypted in to the same cipher text. There are four types of block cipher. They are Output Feedback, Cipher block Chaining, Electronic Code Book and Cipher Feedback Mode. Data Encryption Standard or DES is one of the common secret key cryptography methods used in the recent days. DES operates on 64-bit blocks, and employs 56-bit key. Software side implementation is slow while the hardware side implementation is faster. Some of the common secret key cryptography algorithms are TwoFish, CAST-128, RC2 and RC5.

TABLE II. Block Cipher Encryption

Plain Text P:	Encryption E:	Secret Key K:	Cipher Text C:
P1P2	Ⓔ	K1	C1C2
P3P4	Ⓔ	K2	C3C4
P5P6	Ⓔ	K3	C5C6
P7P8	Ⓔ	K4	C7C8
P9P10	Ⓔ	K5	C9C10
P11P12	Ⓔ	K6	C11C12
P13P14	Ⓔ	K7	C13C14
P15P16	Ⓔ	K8	C15C16

B. Key Distribution

Existing System

Key distribution technique is the key strength of any cryptographic system. Key distribution technique is defined as the technique that delivers a key for those parties who wish to exchange the data, without revealing the key to each other. If three parties are involved in a network, and if there is a requirement to transfer the data between the first two parties, then we can achieve this by employing an encrypted connectivity between the first two parties, so that the third party won't be able to see the data that is being exchanged between first two parties.

Two kinds of keys are required for this: Session key and Permanent key. Session key is used for the cryptographic functions like encryption/decryption of user data during the communication between two parties. For the distribution of the session keys, permanent key is used. The configuration consists of the following elements: Key distribution Center and Front-end Processor. The former is used to grant the permission for the systems for establishment of connection and for providing the one time session key for the specific function. The latter provides the end to end encryption and obtains the session key on behalf of the host / terminal.

If one host needs to establish a connection with another host, then the system transmits a connection-request packet. At that time, the front end processor receives the packet, saves and confirms the KDC for permission to establish the connection. FEP to KDC communication is encrypted using the master shared key. On approval of the connection request at the KDC, a session key will be generated and delivered to the two front end processors. Also it will make sure that a unique permanent key will be there for each front end. Hence the requesting front end processor can release the connection request packet, along with a connection setup between two end systems. Using the session key, the front end processor encrypts the data during the exchange of data.

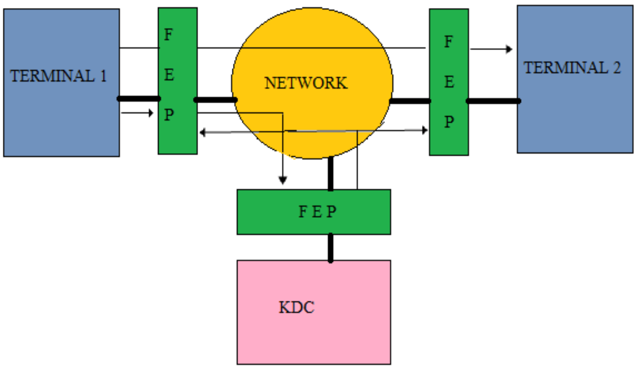


Fig 4:- Existing system's key distribution.

Steps involved in the existing key distribution system are:

1. Terminal1 sends a packet, to request the connection.
2. Front end buffer packets, requests the KDC for the session key.
3. KDC shares the session key with both the front end buffers.
4. Transmitting the encrypted packet.

Proposed System

In the proposed system, the connection establishment is almost same as that of the existing system. The key difference between the existing and proposed system is the difference in the key distribution center. The former system is using the Key Distribution Center (KDC), and the latter is using Random Key distribution center.

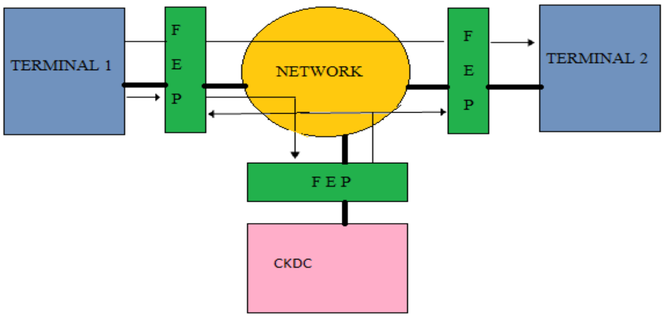


Fig 5:- Proposed system's Key Distribution

1. Terminal1 sends a packet, to request the connection.
2. Front end buffer packets, requests the KDC for the session key.
3. CKDC shares the session key with both the front end buffers.
4. Transmitting the encrypted packet.

COMPOUND RANDOM SECRET KEYS

In the symmetric key cryptography, same key is used at the source and the destination end systems. In this case anybody who can identify the key and the encryption algorithm can capture the message and decrypt the information exchanged between the end systems. But, if the secret key is different for the source and destination, the problem of symmetric cryptography can be resolved. To accomplish these random keys should be generated each time, and used in each message transactions.

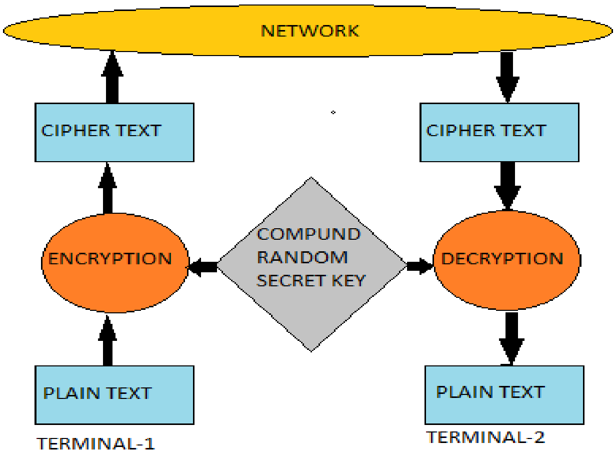


Fig 6: Proposed model for the cryptography

If a terminal wishes to establish a connection with another terminal, it will send a connection request packet to the CKDC. When the connection request is approved, it will send the message which is encrypted on both the terminals. Four values will be there in that encrypted message, namely x, y, m and c. Sizes of the x, y, and c are of the equal size. The value of m will vary from 1 to 9. With the above 4 values, we need to generate compound secret keys using the key generation algorithm. The equations used to generate the compound secret key are

$$z = y + x$$
$$x = mx + c$$

z is the compound secret key that we are generating. We need to execute the above two statements repeatedly for each and every message exchange. For each message exchange the value of x and z will also change, but the length of the item should be equivalent to the secret key length. New secret keys should be generated each time message transfer occurs in the system. The advantage of this technique is its easiness in finding out the missing packets in the message transfer if any.

PROPOSED ALGORITHMS

Encryption Algorithm

The steps involved in the encryption procedure are:

1. Map the secret key with the characters in the input string.
2. Find out the ASCII character value for the input string.
3. Find out the sum of each ASCII value and the secret key digit.
4. Find out the modulus of the sum of the above value with the digit 128.
5. Find out the respective character for the above ASCII value.

The result we obtain from the step 5 will be out cipher text.

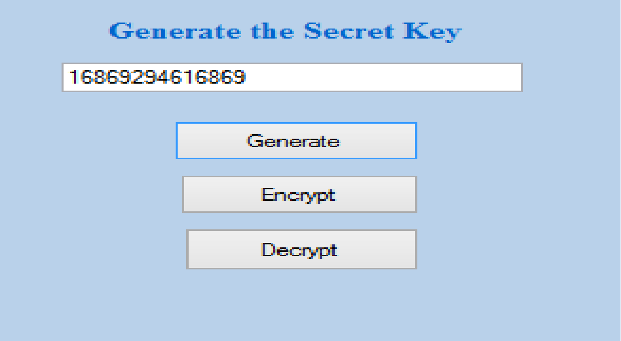
Decryption Algorithm

The secret key will be the same as that we used in the encryption algorithm. The steps involved in the decryption process are as follows.

1. Map the cipher text characters with the secret key numbers.
2. Get the ASCII value of each character in the cipher text.
3. Deduct the secret key numbers from the above numbers.
4. Get the modulus result by using the value 128.
5. Convert the result to the characters.

III. RESULTS

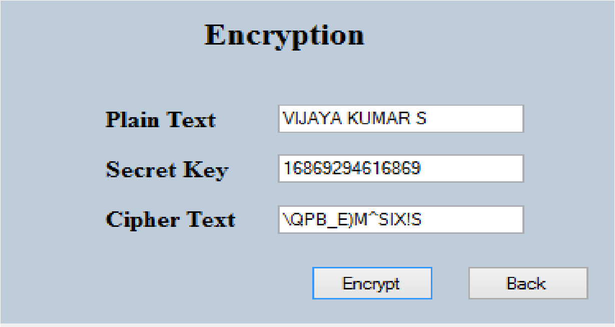
I implemented the proposed algorithm as a Windows application by using Microsoft Visual Studio – 2013. The symmetric key encryption and decryption are shown in the below figures.



Generate the Secret Key

16869294616869

Fig 7: Key Generation Page: Test 1



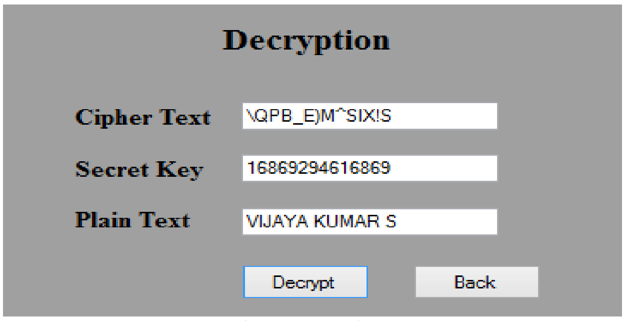
Encryption

Plain Text VIJAYA KUMAR S

Secret Key 16869294616869

Cipher Text \QPB_E)M^SIX!S

Fig 8: Encryption: Test 1



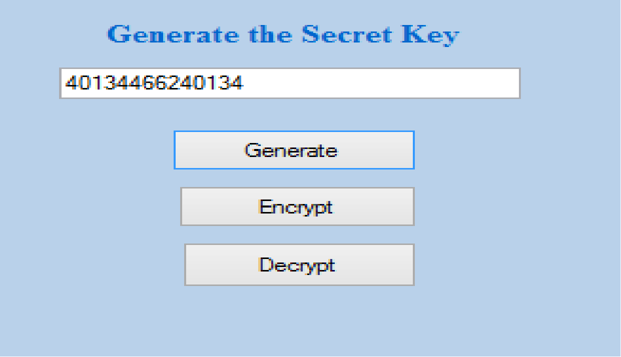
Decryption

Cipher Text \QPB_E)M^SIX!S

Secret Key 16869294616869

Plain Text VIJAYA KUMAR S

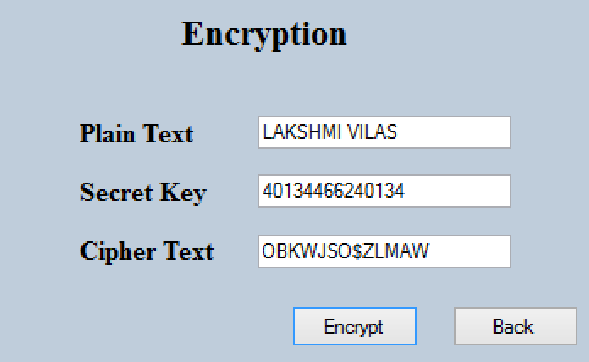
Fig 9: Decryption: Test 1



Generate the Secret Key

40134466240134

Fig 10: Key Generation: Test 2

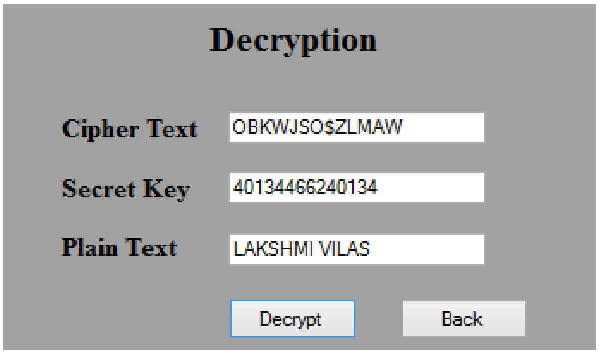


Plain Text: LAKSHMI VILAS

Secret Key: 40134466240134

Cipher Text: OBKWJSO$ZLMAW

Fig 11: Encryption: Test 2



Cipher Text: OBKWJSO$ZLMAW

Secret Key: 40134466240134

Plain Text: LAKSHMI VILAS

Fig 12: Decryption: Test 2

VI. CONCLUSION

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper; use the scroll down window on the left of the MS Word Formatting toolbar.

REFERENCES

[1] S. William, Cryptography and Network Security: Principles and practice 2nd edition, Prentice-Hall, Inc., 1999 pp 23-50.

[2] Aamer Nadeem, Dr M. Younus Javed, "A Performance Comparison of Data Encryption Algorithms", First International Conference on IEEE Information and Communication Technologies (ICICT), Vol 1, Issue 6, 27-28 Aug. 2005, pp 84-89.

[3] S.Soni, H. Agrawal, M. Sharma, "Analysis and comparison between AES and DES Cryptographic Algorithm", International Journal of Engineering and Innovative Technology, Vol 2, Issue 6, December 2012, pp.362-365.

[4] E.Surya and C.Diviya, "A Survey on Symmetric Key Encryption Algorithm s", International Journal of Computer Science & Communication Networks,Vol 2(4), 475-477.

[5] Prakash Kuppuswamy, Dr.C.Chandrasekar, "Enrichment Of Security Through Cryptographic Public Key Science Algorithm Based On Block Cipher" Indian Journal of Computer and Engineering (IJCSE), Vol. 2 No. 3 Jun - Jul.2011.

[6] Steve Burnett & Stephen Paine RSA Security's Official Guide to Cryptography, Tata McGrawHill.

[7] Behrouz A. Forouzan,Cryptography & Network Security,Tata McGraw Hill..

[8] http://williamstallings.com/Crypto3e.html.

[9] http://www.cacr.math.uwaterloo.ca/hac

Vijaya Kumar S, MCA., ME (CSE), has completed MCA in 2003 from Periyar University, Salem and ME in Computer Science and Engineering in 2016 from Anna University Salem. He has 9 years of Industrial experience and around 2 years of teaching experience. Now he is working as Assistant Professor in MCA, Saintgits College of Engineering, Kottayam, Kerala.