International Journal of Engineering &Technology, 7 (4) (2018) 6510-6514

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i4.26613
Research paper

An efficient encryption-secure communication using symmetric key

Nahida Nigar *

Department of Computer Science and Engineering, Southern University Bangladesh, Bangladesh
**Corresponding author E-mail: n.nigar.87 @ gmail.com*

Abstract

To stop unauthorized disclosure of confidential information we need to secure our data. To secure data we need to use a secure cryptographic system. The conventional systems of data security are not suitable for multimedia as well as different data types. This paper is concerned with the development of a secure communication system which will satisfy some aspects such as reliability, maintainability, security, and user-friendliness. This project is based on the conventional method of cryptography known as symmetric key encryption technique named AES and 3DES made the system faster, better immune to attacks, greater complexity, easier encryption/decryption, and much more advanced security feature included. This project work is designed and developed for secure communication on different platforms. Unlike any other application, this software can encrypt any length of a video message, audio, text, etc. using a key and then decrypts the ciphertext with the same key to see the plaintext on the receiving end. Whatever the data is encrypted the ciphertext will be in text type which will give more security to the data because the hacker cannot guess the data type to hack. Comparing with other security based application system, the proposed system can be used for any type of communication in both online and offline.

Keywords: *Cryptography; Symmetric key; AES; 3DES.*

1. Introduction

Cryptography [4] is a sophisticated, creative and mathematically challenging field of study. "Encryption is basically an indication of users' distrust of the security of the system, the owner or operator of the system, or law enforcement authorities." Encryption transforms original information, called plaintext or cleartext, into transformed information, called ciphertext, code text or simply cipher, which usually has the appearance of random, unintelligible data. The transformed information, in its encrypted form, is called the cryptogram. Information transmission in a communication system needs to be secure. That means transmitted data must maintain integrity, authenticity, and confidentiality. Cryptography is the science which provides encryption techniques for secure communication [1]. Data is encrypted before transmission and decrypted after receiving the encrypted data. Normal communication that we used to do in our everyday life on the web is potentially visible to eavesdropper anywhere along its internet path which means information is compromised at any time. For this reason, our proposed software system is concerned with the development of a secure communication system using the cryptographic technique.

The basis of Encryption involves receiving some data that is readily readable and to encrypt this data into a new format, that is gibberish to all but those for whom it is intended. This data can be mostly decoded only by those who contain relevant information needed for the decryption. The initially received data is referred to as the Plain Text and the data after the encryption is known as the Cipher Text [1]. The major basis of different Encryption Techniques is divided into two generic types: symmetric- key and public-key [14], [15]. Both of these types have their own advantages and are used by the cryptographic community to exploit the strengths of each. However, each of these techniques has a constraint that being that the encrypted key can be breached easily by using an exhaustive key search. To overcome this constraint increases the uncertainty factor of the generated key, such that it rivals that of the plaintext. Although traditional one-time pad method provides infinite key space to increase the uncertainty factor this method has a drawback that the length of the key should be as long as the plaintext. This problem has also been overcome by using this novel method of cipher generation. Our plan is to introduce an efficient approach to the Book Cipher encryption method in this paper.

In earlier encryption project was too complex than the entire project. In the existing system, the encrypted key is sent with the document.If the key is sent with a document, any user can view the encrypted document with that key. It means the security provided for the encryption is not handled properly. And also the Key byte (the encrypted key) generate with a random byte. Without user interaction, the Key byte is generated. A security system was the most important drawbacks of the system. Various research works have been done on network issues [5], [6].

The previous study [2] shows that the development of a secure messaging system can only give security to text message during communication. There is no such cryptographic system which can convert text, audio, video, files, etc. at a time. Our system is developed after a thorough review of the existing Encryption systems [12], [13]. Our proposed system can encrypt any length of a video message, audio, text, etc. using a key and then decrypts the ciphertext with the same key to see the plaintext on the receiving end. The lucrative part of our system is whatever the data is encrypted, the ciphertext will be in text type which will give more security to the data because a hacker cannot guess the data type to hack.

Copyright © 2018 Nahida Nigar. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

2. Methodology

Software is a complex artifact created by a human being. The entire complex being is produced in a step-by-step procedure, which is called methodology for that artifact. Effective management of a software project depends on thoroughly planning the progress of the project. The project developer must anticipate problems which might arise and prepare tentative solutions to those problems. A plan, draw up at the start of the project, should be used as the driver for the project. This initial plan should be the best possible plan given the available information [10]. Our project is divided into several segments. They are feasibility study, requirement engineering, system specification design, implementation, application of the system and maintenance. Through this feasibility study, we find feasible solutions for the present problems which will work efficiently to implement our secure communication system. The system specification and design techniques are revolted according to requirement analysis, specification, and validation. A most important part of the project is an implementation which contains coding, testing, object models of the software. We used the AES [14] and 3DES [15] algorithm to implement the software. The last part contains the application and maintenance of the system that implies the effectiveness and reliability of the software. We have used Visual Basic .NET [11] Language to designing interface of the software.

2.1. Algorithm of the proposed system

Step 1: Enter the correct username and password.
Step 2: Select any file to be encrypted.
Step 3: Select one symmetric key algorithm.
Step 4: Setup the AES Algorithm Value.
Step 5: Select Ciphertext and anyone algorithm to decrypt.
Step 6: Select the save file and decrypt it.
Step 7: Successfully Close the Application.

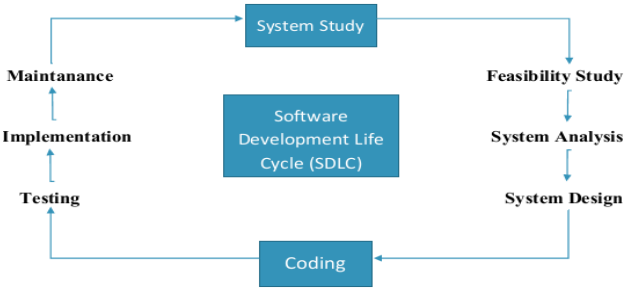


Fig. 1: A System Development Life Cycle for Secure Communication System.

3. System specification

Software requirements specification (SRS) [10] is a description of a software system to be developed, laying out functional and non-functional requirements, and may include a set of use cases that describe interactions the users will have with the software.

3.1. Use case diagram

Use case [10] is referred to as the key functions of the system fulfilled by the user. The Use case model focuses on the use case (key functions), the users and interaction between them. The model can be shown graphically through the use case diagram. Use case diagram is the graphical modeling that shows the communication between actor and use case [10].

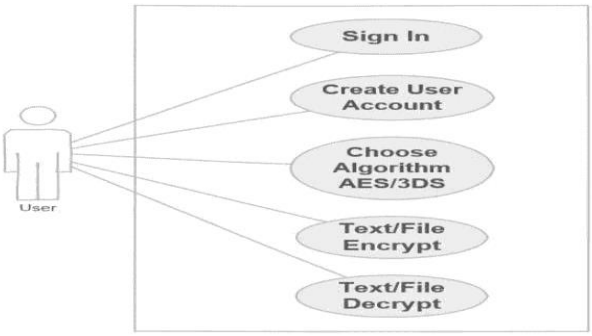


Fig. 2: Use Case Diagram for Secure Communication System.

3.2. Entity-relationship model

A graphical representation of entities and their relationships to each other, typically used in computing in regard to the organization of data within databases or information systems. An entity is a piece of data-an object or concept about which data is stored [10]. The Entity-Relationship model for encryption secure communication system is given below:

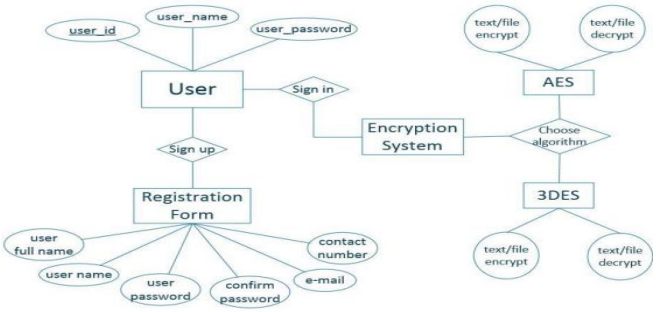


Fig. 3: ER Model for Secure Communication System.

3.3. Activity diagram

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration, and concurrency. The activity diagram of encryption secure communication system is given below:

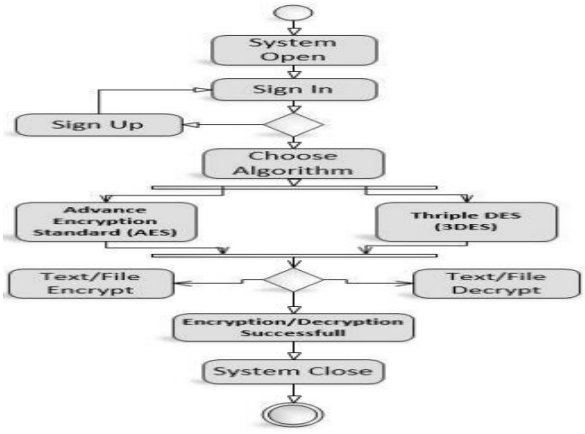


Fig. 4: Activity Diagram for Secure Communication System.

3.4. Data flow diagram

Data flow model shows the passage of data in the system by representing lines joining system components. An arrow indicates the direction of the flow and the line labeled by the name of the data flow.

3.4.1. Context diagram for secure communication system

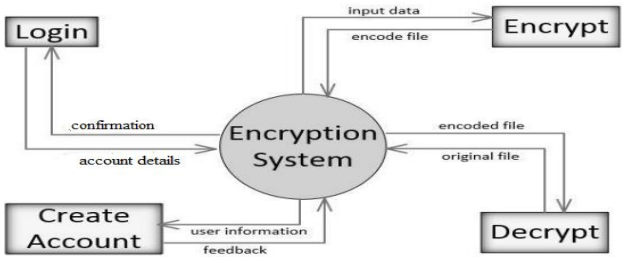


Fig. 5: DFD Level 0 for Secure Communication System.

3.4.2. DFD level 1 for secure communication system

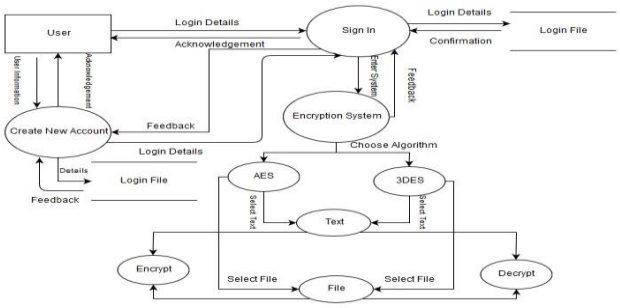


Fig. 6: DFD Level 1 for Secure Communication System.

4. System design

The user interface is designed for both sender and receiver, as shown in Figures 7, 8, 9 and 10 respectively. This includes login, profile, registration, Form to choose encryption/decryption algorithm, key list.

In this project work, the proposed secure communication system has been developed using VB.net [11]. User registration is needed to log into the system and a profile created for registered user. After login, the system provides a framework with menus where a user can choose encryption/ Decryption algorithm to encrypt a file. The file can be of any type. The user can select key for AES or 3DES to encrypt the selected file. At the receiver end, the receiver uses the same GUI and request for the value of "key" from the database. After the correct input of the key values will return the plaintext as sent by the sender. Using this key the receiver can decrypt the ciphertext and then read the original message. The following figure shows the encryption system and user database:



Fig. 7: Front Form of Encryption System.



Fig. 8: Login Form.

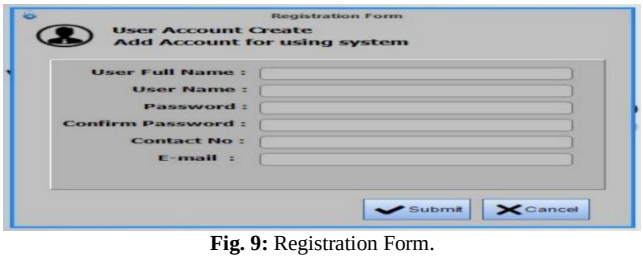


Fig. 9: Registration Form.

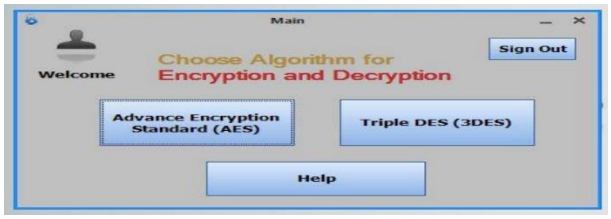
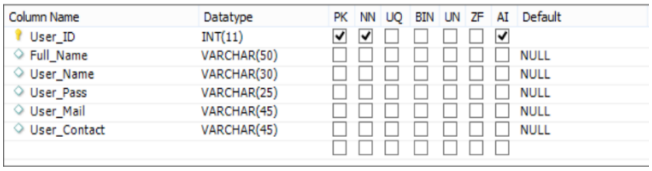
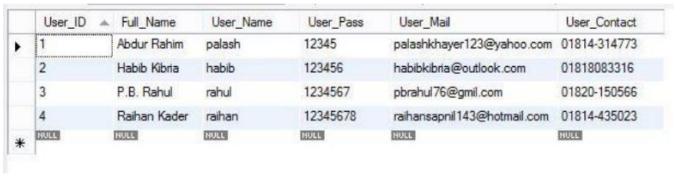


Fig. 10: Main Form.



Column Name	Datatype	PK	NN	UQ	BIN	UN	ZF	AI	Default
User_ID	INT(11)	☑	☑	☐	☐	☐	☐	☑	
Full_Name	VARCHAR(50)	☐	☐	☐	☐	☐	☐	☐	NULL
User_Name	VARCHAR(30)	☐	☐	☐	☐	☐	☐	☐	NULL
User_Pass	VARCHAR(25)	☐	☐	☐	☐	☐	☐	☐	NULL
User_Mail	VARCHAR(45)	☐	☐	☐	☐	☐	☐	☐	NULL
User_Contact	VARCHAR(45)	☐	☐	☐	☐	☐	☐	☐	NULL
		☐	☐	☐	☐	☐	☐	☐	

Fig. 11: User Database Screenshot of Encryption System.



User_ID	Full_Name	User_Name	User_Pass	User_Mail	User_Contact
1	Abdur Rahim	palash	12345	palashkhayer123@yahoo.com	01814-314773
2	Habib Kibria	habib	123456	habibkibria@outlook.com	01818083316
3	P.B. Rahul	rahul	1234567	pbrahul76@gmil.com	01820-150566
4	Raihan Kader	raihan	12345678	raihansapnil143@hotmail.com	01814-435023
NULL	NULL	NULL	NULL	NULL	NULL

Fig. 12: User Database Table of Encryption System.

5. System testing

System testing [10] is the testing to ensure that by putting the software in different environments (e.g., Operating Systems) it still works. System testing is done with full system implementation and environment. It falls under the class of black box testing. Implementation and Testing are the most important parts of the Software development life cycle [10]. In this two-stage, the software design is realized as a set of programs or program units. Moreover, unit testing involves verifying that each unit meets its specification depending on implementation technique. System testing is the stage of implementation that is aimed at ensuring that the system works accurately and efficiently before live operation commences. Testing is vital to the success of the system. System testing makes a logical assumption that if all the parts of the system are correct, then the goal will be successfully achieved. A series of testing is done for the proposed system before the system is ready for user acceptance testing.

5.1. The testing process

To evaluate the performance of the proposed system in this paper several testing procedures have been done. All the testing strategy results are summarized in table 1. The testing process of a secure communication system is given below:

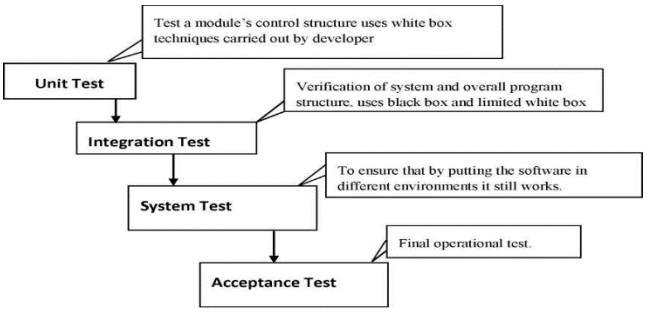


Fig. 13: Testing Process of Secure Communication System.

5.2. Testing strategy

The Test Strategy results of Secure Communication System are shown in Table 1.

Table 1: Test Strategy of Secure Communication System

Test Number	Test Name	Test Data	Expected Result	Action	Comments
1.	Login Check	Correct ID, Pass	Should be signed in	Sign in	Test-ok
2.	Login Check	Incorrect ID, Pass	Should not be signed in	ID, Pass does not exist	Test-ok
3.	AES Text Encryption	Plain Text	Ciphertext	Encode	Test-ok
4.	AES Text Decryption	Cipher text	Plain Text	Decode	Test-ok
5.	AES File Encryption	Input File/Documents	Encrypted File/Documents include password	Encryption Complete	Test-ok
6.	AES File Decryption	Encrypted File/Documents Include correct password	Original File/Documents	Decryption Complete	Test-ok
7.	AES File Decryption	Encrypted File/Documents Include incorrect password	Password does not match	Decryption incomplete	Test-ok
8.	3DES Text Encryption	Plain Text	Cipher text	Encode	Test ok
9.	3DES Text Decryption	Ciphertext	Plain Text	Decode	Test-ok
10.	3DES File Encryption	Input File/Documents	Encrypted File/Documents include key	File successfully Encrypted	Test-ok
11.	3DES File Decryption	Encrypted File/Documents with the correct key	Original File/Documents	File successfully Decrypted	Test-ok
12.	3DES File Decryption	Encrypted File/Documents with the incorrect key	Key does not match	Decryption incomplete	Test-ok

All of the testing results screenshots are given below:

i) Test No: 01



Fig. 14: Login Test with Correct Id and Password.

ii) Test No: 02



Fig. 15: Login Test with Incorrect Id and Password.

iii) Test No: 03



Fig. 16: AES Text Encryption Test.

iv) Test No: 04

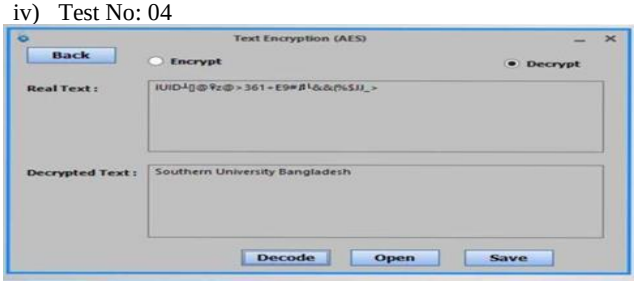


Fig. 17: AES Text Decryption test.

v) Test No: 05



Fig. 18: AES File Encryption Test.

vi) Test No: 06



Fig. 19: AES File Decryption Test.

vii) Test No: 07



Fig. 20: AES File Decryption Test with the Wrong Password.

viii) Test No: 08



Fig. 21: 3DES Text Encryption Test.

ix) Test No: 09

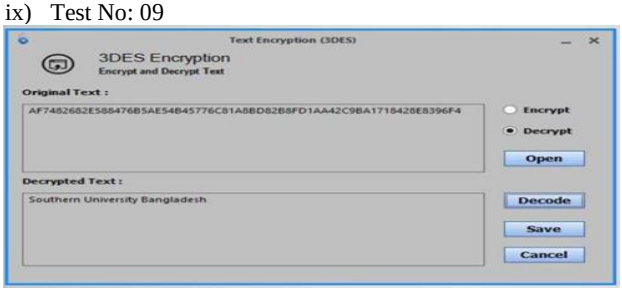


Fig. 22: 3DES Text Decryption Test.

x) Test No: 10



Fig. 23: 3DES File Encryption Test.

xi) Test No: 11



Fig. 24: 3DES File Decryption Test.

xii) Test No: 12



Fig. 25: 3DES File Decryption Test with the Wrong Password.

6. Conclusion

The previous study [2] shows that developing a secure message system can only provide text messages with security during communication. This paper is concerned with the development of a secure communication system which will satisfy some aspects such as reliability, maintainability, security, and user-friendliness. No such cryptographic system which can convert text, audio, video, files, etc. at a time. In this paper, we proposed a system which can efficiently encrypt any length of a video message, audio, text, etc. using a key and then decrypt the ciphertext with the same key to see the plaintext on the receiving end. The lucrative part of our system is whatever the data is encrypted, the ciphertext will be in text type which will give more security to the data because a hacker cannot guess the data type to hack. Our proposed system is based on symmetric key encryption technique namely AES and Triple DES. The system is developed after a thorough review of the existing Encryption systems [12], [13]. Unlike other secure communication systems, our proposed system can be used in both online and offline.

References

[1] Rivest RL (1990) Cryptology. Handbook of Theoretical Computer Science.

[2] Rahman, M. M., T. Akter, and A. Rahman. "Development of Cryptography-Based Secure Messaging System." *J Telecommun Syst Manage* 5.142 (2016): 2167-0919.

[3] Alanazi, Hamdan, et al. "New comparative study between DES, 3DES, and AES within nine factors." *arXiv preprint arXiv:1003.4085* (2010)

[4] Meyer, Carl H., and Stephen M. Matyas. *CRYPTOGRAPHY: A new dimension in computer data security: A guide for the design and implementation of secure systems*. Wiley, 1982.

[5] Nigar, Nahida, and Muhammad Anwarul Azim. "Fairness Comparison of TCP Variants over Proactive and Reactive Routing Protocol in MANET." *International Journal of Electrical and Computer Engineering (IJECE)* 8.4 (2018). https://doi.org/10.11591/ijece.v8i4.pp2199-2206.

[6] Nigar, Nahida. "Comparative Performance Evaluation of TCP with Identical and Cross-Variant Congestion Control."

[7] Van Tilborg, Henk CA. *An introduction to cryptology*. Vol. 52. Springer Science & Business Media, 2012.

[8] William, Stallings. "Cryptography and network security: principles and practice." *Prentice-Hall, Inc* (1999): 23-50.

[9] Sommerville, Ian. *Software engineering*. Boston: Pearson, 2011.

[10] Wakefield, Cameron, Henk-Evert Sonder, and Wei Meng Lee. *VB. Net Developer's Guide with Cdrom*. Syngress Publishing, 2001.
[11] Rohilla, Charu, et al. "Encryption and Decryption for Secure Communication."
[12] Saraireh, Saleh. "A Secure Data Communication system using cryptography and steganography." *International Journal of Computer Networks & Communications* 5.3 (2013): 125. https://doi.org/10.5121/ijcnc.2013.5310.
[13] Daemen, Joan, and Vincent Rijmen. *The design of Rijndael: AES-the advanced encryption standard*. Springer Science & Business Media, 2013.
[14] Barker, William C. *Recommendation for the triple data encryption algorithm (TDEA) block cipher*. National Institute of Standards and Technology, 2004. https://doi.org/10.6028/NIST.SP.800-67ver1.