Journal of Telecommunications System & Management

Research Article OMICS International

Development of Cryptography-Based Secure Messaging System

Rahman MM*, Akter T and Rahman A

Department of Computer Science and Engineering, Jatiya Kabi Kazi Nazrul Islam University, Bangladesh

Abstract

Today data communication is a modern technology that contains a powerful computer processor to exchange information. But brute force attacks are made to break the encryption techniques and these attacks are the main drawbacks of older algorithms. This paper is concerned with the development of a secure messaging system based on cryptographic algorithms that is which is more faster, better immune to attacks, more complex, easy to encrypt and many more advanced security feature included. This project work is designed and developed for a secure messaging both in web and android platforms. The application is well featured and provides encryption/decryption that can protect message from unauthorized access and disclosure over networks. To send message, a recipient or registered user types and encrypts a text message using keyword mono-alphabetic substitution algorithm with a key, selected from key list. The encrypted message is stored in the database and receiver's inbox with serial number of key (not the value). The receiver, after log into his/her own account, selects the key value and then decrypts the encrypted message with the key to see the original message. With compared to other messaging systems, the proposed secure messaging system can be used for chat, messaging, video conferencing and real time file sharing in both web and android platforms.

Keywords: Secure messaging; Cryptography; Encryption; Decryption; Web application; Android apps

Introduction

Technology is used in every sphere of life and people are more dependent on Smartphone technology that contains a powerful computer processor to exchange data information. This is because of necessity of our multimedia documents to be protected from unauthorized person. So a day-to-day use of cryptography [1] in our life is increasing tremendously. Messaging system is a text or instant messaging service component of phone, web, or mobile communication systems over the world. But is it really safe to use? Recently the Electronic Frontier Foundation (EFF) [2] has submitted a report that is not comfortable for all users. Because we have to rely as much of our personal information while chatting in fact it is not safe to write there. The public instant messaging systems, the messages are travel from the client to the server and back to the second client. This data is potentially visible to eavesdroppers anywhere along its Internet path or within the network. So the information at any moment it could have gone to someone else. For this reason, this project work is concern with the development of secure messaging system using cryptographic technique.

Secure messaging is a server-based approach to protect sensitive data from unauthorized access over Internet. It is confidential and authenticated exchange by any internet user worldwide. Secure messages provide non-repudiation as the recipients are personally identified and transactions are logged by the secure email platform. Brute force attacks [3] are made to break the encryption and they are growing so faster. These attacks are the main drawbacks of older algorithm. But with feature this algorithms will be replaced by other techniques that will provide better protection. In this paper we are going to proposed a secure messaging system that is implemented by an encryption technique which is more faster, better immune to attacks, more complex, easy to encrypt and many more advanced security feature included.

Cryptography Algorithms

Cryptography is the study of Secret (crypto-) and Writing (-graphy), respectively [4]. It is a technique for storing and transmitting data or message in a particular form so that only those for whom it is intended can read and process it. In today's computer technology, cryptography is most often associated with scrambling ordinary text (also referred to as plaintext) into cipher text, the process called encryption then back again plaintext, the process known as decryption. Individuals who practice this field are known as cryptographers. Modern cryptography concerns itself with four major objectives; such as Confidentiality (the information cannot be understood by anyone for whom it was unintended), Integrity (the information cannot be altered or detected), Non-repudiation (the sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information), and Authentication (the sender and receiver can confirm each other's identity and the origin/destination of the information).

There are a number of algorithms for performing encryption and decryption. The most successful algorithms use a key. A key is simply a parameter to the algorithm that allows the encryption and decryption process to occur. The modern field of key-based cryptographic algorithms can be divided into two classes, such as symmetric-key cryptography and asymmetric cryptography or public-key cryptography. Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key. This was the only kind of encryption publicly known until June 1976 [5]. The public-key cryptography is cryptography in which a pair of keys is used to encrypt and decrypt a message so that it arrives securely. Another cryptographic algorithm is cryptographic hash function that uses a mathematical transformation to irreversibly "encrypt" information.

***Corresponding author:** Rahman MM, Associate Professor, Department of Computer Science and Engineering, Jatiya Kabi Kazi Nazrul Islam University, Bangladesh, Tel: 8801712594569; E-mail: mijanjkkniu@gmail.com

Received October 12, 2016; **Accepted** October 21, 2016; **Published** November 02, 2016

Citation: Rahman MM, Akter T, Rahman A (2016) Development of Cryptography-Based Secure Messaging System. J Telecommun Syst Manage 5: 142. doi: 10.4172/2167-0919.1000142

These one-way hash functions have been called “the workhorses of modern cryptography” [6]. The input data is often called the message, and the hash value is often called the message digest or simply the digest. Although, it is difficult to determine the quality of an encryption algorithm, it is a good idea to choose an encryption algorithm that has been in use for several years and has successfully resisted all attacks (Figure 1).

Public-key cryptography

Symmetric-key cryptosystems use the same key for encrypting and decrypting message in network security. A significant disadvantage of symmetric encryption is the key management necessary to use them securely. In a groundbreaking 1976 paper, Whitfield Diffie and Martin Hellman proposed the notion of public-key cryptography in which two different but mathematically related keys are used; a public key and a private key [7]. A public-key system is so constructed that calculation of one key (the ‘private key’) is computationally infeasible from the other (the ‘public key’). Instead, both keys are generated secretly, as an interrelated pair. The historian David Kahn described public-key cryptography as “the most revolutionary new concept in the field since polyalphabetic substitution emerged in the Renaissance” [8]. An important element to the public key system is that the public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them. Moreover, it is virtually impossible to deduce the private key if you know the public key [9].

Types of ciphers in cryptography

Encryption is the process of transforming plaintext data into something that appears to be random and meaningless, known as cipher text. Decryption is the process of converting cipher text back to plaintext. To encrypt more than a small amount of data, symmetric encryption is used. A symmetric key is used during both the encryption and decryption processes. To decrypt a particular piece of cipher text, the key that was used to encrypt the data must be used.

There several types of operations used for encryption and decryption [10]. Substitution and transposition ciphers are two categories of ciphers used in classical cryptography, as shown in Figure 2. All encryption algorithms are based on these two principles. In substitution, each element in the plain text is mapped into another element, and in transposition, the plaintext are rearranged. Most systems referred to as product systems, involved multiple stages of substitution and transposition. Substitution and transposition differ in how chunks of the message are handled by the encryption process.

There are different types of substitution cipher. If the cipher operates on single letter, it is termed a simple substitution cipher; a cipher that operates on a group of letters is termed polyalphabetic. A mono-alphabetic cipher uses fixed substitution over the entire message, whereas a polyalphabetic cipher uses a number of substitutions at different positions in the message, where a unit from the plaintext is mapped to one of several possibilities in the cipher text and vice versa. The cryptographic algorithm with keyword mono-alphabetic cipher has been used in this project work.

Keyword mono-alphabetic encryption

A mono-alphabetic substitution is a cipher in which each occurrence of a plaintext symbol is replaced by a corresponding cipher text symbol to generate cipher text. The key for such a cipher is a table of the correspondence or a function from which the correspondence is computed. An affine cipher E(x) = (ax+b) MOD 26 is an example of a mono-alphabetic substitution. In a keyword mono alphabetic cipher, substitution characters are a random permutation of the 26 letters of the alphabet. An example is given in Table 1.

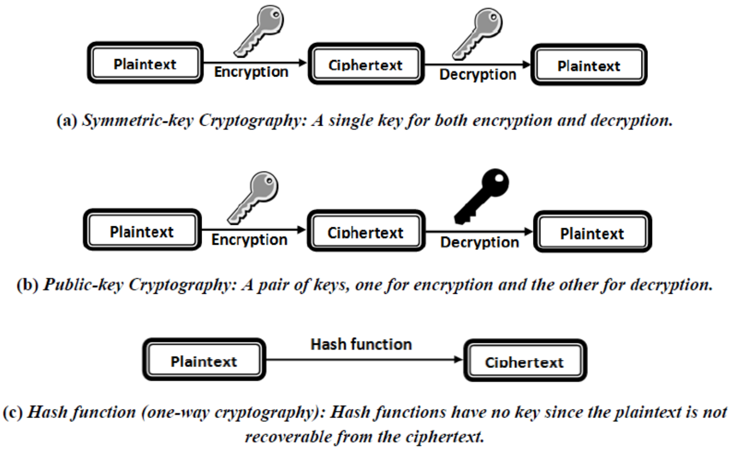

Plaintext
Encryption
Ciphertext
Decryption
Plaintext
(a) Symmetric-key Cryptography: A single key for both encryption and decryption.
Plaintext
Encryption
Ciphertext
Decryption
Plaintext
(b) Public-key Cryptography: A pair of keys, one for encryption and the other for decryption.
Plaintext
Hash function
Ciphertext
(c) Hash function (one-way cryptography): Hash functions have no key since the plaintext is not recoverable from the ciphertext.

Figure 1: Three types of cryptography: Symmetric-key, public-key, and hash function.

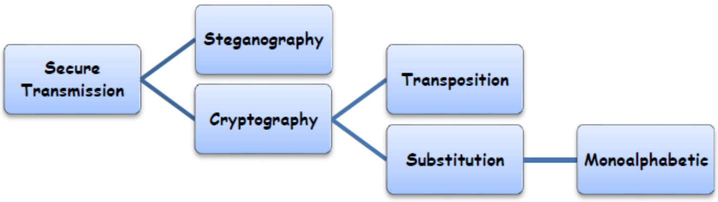


Figure 2: Categories of Secure Message Transmission.

The key now is the sequence of substation letters. There are 26! Permutations of the alphabet. Another ways to "generate" a mono-alphabetic substitution is Keyword mono-alphabetic substitution. A keyword or key phrase can be used to mix the letters to generate the cipher alphabet. Let us consider the KEYWORD is "how". In encryption 'a' will replace with 'H', 'b' with 'O' and so on. Then the transformation is given in Table 2. The cryptographic algorithm with keyword mono-alphabetic cipher is used in this research.

Algorithm

To design the cryptographic algorithm, the keyword mono-alphabetic cipher is used. Two character arrays are used; KEYWORD is an array of character will used instead of KEY as used in experiment and LETTER is used to form NEWLETTER in which first characters will be inserted from the KEYWORD and then the remaining character from LETTER will come sequentially. The KEY is the sequence of substation letters. There are 26! Permutations of the alphabet; hence the KEY length would be 26!. Also an array, MESSAGE is used to store the characters of the original message. The encryption and decryption algorithms for the keyword mono-alphabetic substitution technique are shown in Figure 3 and 4, respectively.

Secure Messaging System

Messaging system is a text or instant messaging service component of phone, web, or mobile communication systems. It uses standardized communications protocols to allow fixed line or mobile phone devices to exchange short text messages [11]. Messaging makes the messaging system responsible for transferring data from one application to another, so the applications can focus on what data they need to share as opposed to how to share it. But this system is not secure; anyone can access or alter the message during the time of transferring from sender to receiver.

Secure messaging is a server-based messaging approach to protect sensitive data or message when it is sent to others. In this research, the secure messaging system is designed using cryptographic algorithms. It can be known as secure e-Mail where confidential and authenticated exchanges can be done by any Internet user worldwide. Secure messages provide non-repudiation as the recipients are personally identified and transactions are logged by the secure email platform. Secure Messages are stored on a network or internet server which is typically more physically secure, and are encrypted when data is inbound or outbound. The transmission of an electronic message over a computer network using software immediately displays the message in a window on the screen of the recipient in a secure fashion. It can facilitate real time access and sharing of information in real time.

Methodological Steps

The methodological steps for designing the proposed secure messaging system (the system block diagram is shown in Figure 5) are given below:

Text message creation

The text message is an original intelligible message or data that is fed to the encryption algorithm as input. It is the contents of an ordinary sequential file readable as textual material without much processing. It is also known as a plaintext, what we want to encrypt. The plaintext can contain strings, characters etc.

Key selection

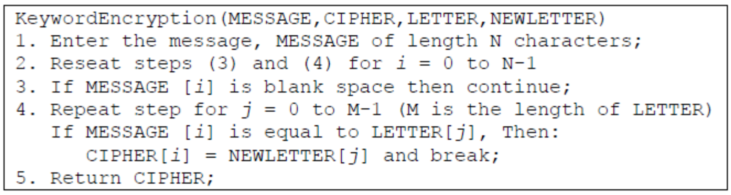
In cryptography, a key is a variable value that is used by a cryptographic algorithm to transform plaintext to cipher text and vice versa. This key remains private and ensures secure communication. Without a key, the cryptographic algorithm would produce no useful

Plain	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher	D	K	V	Q	F	I	B	J	W	P	E	S	C	X	H	T	M	Y	A	U	O	L	R	G	Z	N

Table 1: Example - mono-alphabetic substitution.

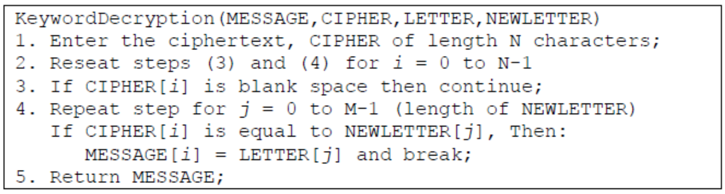
Plain	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher	H	O	W	A	B	C	D	E	F	G	I	J	K	L	M	N	P	Q	R	S	T	U	V	X	Y	Z

Table 2: Example- keyword mono- alphabetic substitution.



```
KeywordEncryption(MESSAGE,CIPHER,LETTER,NEWLETTER)
1. Enter the message, MESSAGE of length N characters;
2. Reseat steps (3) and (4) for i = 0 to N-1
3. If MESSAGE [i] is blank space then continue;
4. Repeat step for j = 0 to M-1 (M is the length of LETTER)
   If MESSAGE [i] is equal to LETTER[j], Then:
      CIPHER[i] = NEWLETTER[j] and break;
5. Return CIPHER;
```

Figure 3: Encryption algorithm using keyword mono-alphabetic substitution.



```
KeywordDecryption(MESSAGE,CIPHER,LETTER,NEWLETTER)
1. Enter the ciphertext, CIPHER of length N characters;
2. Reseat steps (3) and (4) for i = 0 to N-1
3. If CIPHER[i] is blank space then continue;
4. Repeat step for j = 0 to M-1 (length of NEWLETTER)
   If CIPHER[i] is equal to NEWLETTER[j], Then:
      MESSAGE[i] = LETTER[j] and break;
5. Return MESSAGE;
```

Figure 4: Decryption algorithm using keyword mono-alphabetic substitution.

result. In the proposed work, the key is generated using a keyword as the first characters and inserting the remaining characters of the English alphabet. Repeated letters in the word are removed, and then the encrypted message is generated with the keyword matching to A, B, C etc. A large number of keywords are stored in the database. The key is the sequence of substation letters and there are 26! Permutations of the alphabet; hence the length of key would be 26!. To prevent a key from being guessed, keys are generated randomly and contain sufficient keywords. Users can choose a keyword to encrypted text message as their wish.

Encryption

Encryption is the process that converts the text message into encrypted message by using keyword mono-alphabetic substitution algorithm, described in section 2.4. In the proposed system, the sender selects a key from key list and writes a text message as input. The sender end produces the encrypted message from the input message. After encryption the message stored as encrypted form is the draft and sent to the receiver. The encrypted message is an apparently random stream of data, as it stands, is unintelligible. Only authorized receiver can decrypt the encrypted messages.

Decryption

Decryption is the reverse operation of encryption. It is also used keyword mono-alphabetic substitution algorithm, described in section 2.4. In this system, the receiver end must know both the key that was selected by sender during encryption and encrypted message for decryption. The decryption process is very simple with the correct key; without the correct key it is impossible.

Interface design

The user interface is designed both for sender and receiver ends both in web and android platforms, as shown in Figures 6 and 7, respectively. This includes login, profile, notification, dashboard, quick mail, chat, mailbox (inbox, sent, draft, etc.) and key list.

System Implementation

In this project work, the proposed secure messaging system has been developed both in android and web platform. In web application, the web server solution stack package, consisting mainly of the Apache HTTP Server, MySQL database, and interpreters for scripts written in the PHP programming languages are used for implementing the system. A user registration is needed for log into the system and a profile created for registered user. After log in, the system provides a framework with menus where a user can send or retrieve a message. The compose message option provides receiver, keyword and write text message area. By clicking the send button the message stored on server as an encrypted form. At the receiver end, the receiver uses the "Inbox" GUI to request for the value of "key" from the database. A correct entry of the key value will return the key that was sent by the sender. Using this key the receiver can decrypt the encrypted message and then read original message.

Android based secure messaging application performs client side processing. This Client sends a HTTP request to the web server. The

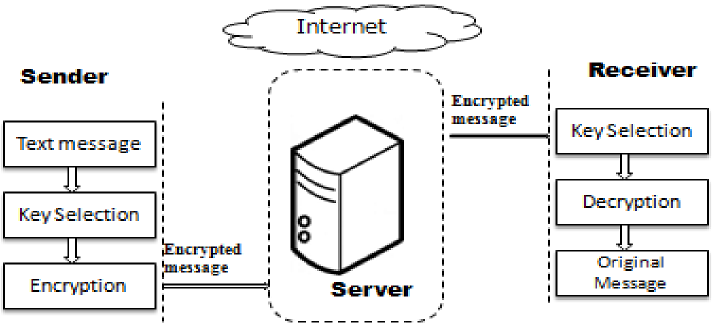


Figure 5: Block diagram of the proposed secure messaging system.

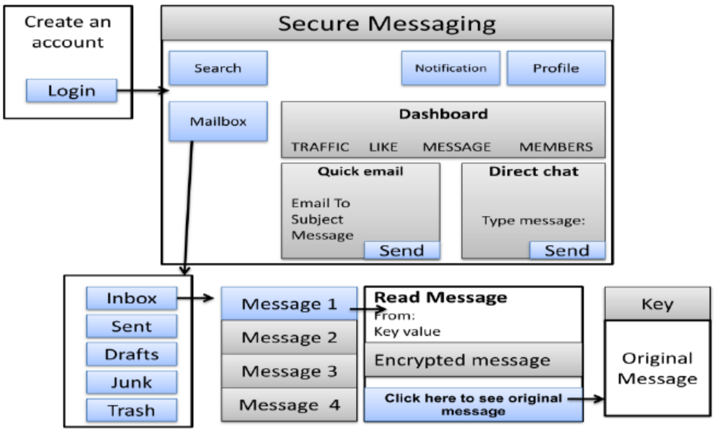


Figure 6: The user interface for secure messaging system in web platform.

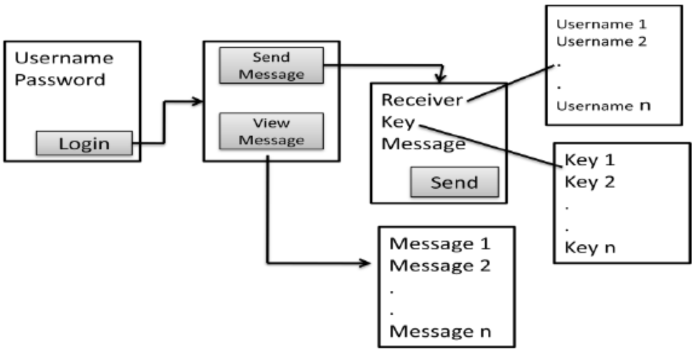
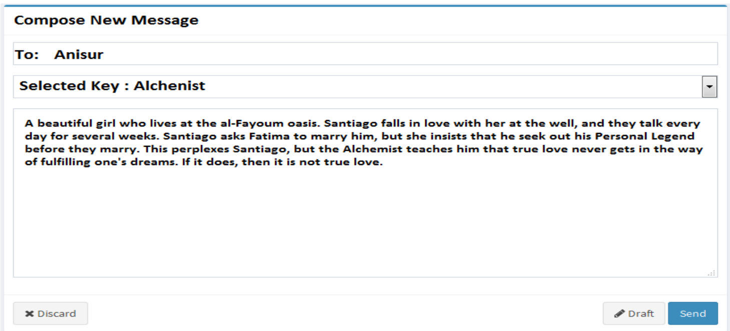


Figure 7: The user interface for secure messaging system in android platform.


Compose New Message

To: Anisur

Selected Key : Alchenist

A beautiful girl who lives at the al-Fayoum oasis. Santiago falls in love with her at the well, and they talk every day for several weeks. Santiago asks Fatima to marry him, but she insists that he seek out his Personal Legend before they marry. This perplexes Santiago, but the Alchemist teaches him that true love never gets in the way of fulfilling one's dreams. If it does, then it is not true love.

Figure 8: The GUI of the sender.

web server response to this request is sending result back in HTML document. The android application that is the client convert the HTML document into JSON format and process it as required. Sender sends message to receiver from a secure messaging application need to be able to get information about a receiver and keywords, ask questions, select keyword they wish to encrypt message, and submit message.

Experiments and Result Analysis

The Graphic User Interface (GUI) is designed for the proposed system that is more user-friendly. The system was run several times and tested online in both web and android platforms. The sender can write text message in the designed editor and encrypt with the selected key and then send the encrypted message with the key number (not the value of key) to the desired user. A sample of message sending is shown in Figure 8. At the receiver end, the encrypted message with key number is received, as shown in Figure 9. The receiver selects the numbering key from the key list and decrypts the encrypted message using this key, so that he/she can read the original message, as shown in Figure 10.

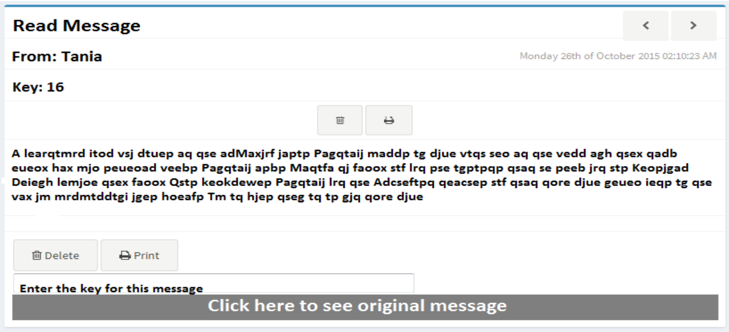
A Project of the Electronic Frontier Foundation presents a secure messaging scoreboard on the topics of secure and usable Cryptography [2]. According to this scoreboard, the proposed secure messaging system can be compared with other messaging systems, as given in Table 3.

Conclusion

The main objective of the proposed system is to transfer message in a communication system securely. Android-based and web-based applications for secure messaging have been developed using cryptographic algorithms for the users to send their message between registered users on any organization securely. The application is supported through user authentication before sending message. The proposed secure messaging system uses minimal processing with little overhead while maintaining security. The authentication of each user is made strong by storing sensitive credentials for each user by using Salt in the database. Encryption and decryption of message are done by using keyword mono-alphabetic substitution algorithm, which is based on Advanced Encryption Standard (AES) [12,13]. This is less secure than the public-key encryption scheme. This is main limitation of this work. An eavesdropper that breaks into the message will return a meaningless message. Obviously encryption and decryption is one of the best ways of hiding the meanings of a message from intruders in a network environment.

The proposed secure messaging can be used in many areas with personal and company-wide sensitive data exchanges. For example, financial institutions, insurance companies, public services, health organizations and service providers rely on the protection by Secure Messaging. This research work includes a background study and comparison analysis of existing systems and the analysis report is shown in Table 3. From the comparison table, given in Table 3, it is concluded that the developed application can be considered for chat, messaging, video conferencing and real time file sharing in these application areas.

The proposed system has been designed and developed with easy integration and modification to take full advantage of future technologies. There are some limitations in the current system to which solutions will be provided as a future development; such as, small number of keywords uses only keyword mono-alphabetic substitution algorithm and network bandwidth. In future, a public-key encryption scheme will be implanted in secure messaging system.



From: Tania

Monday 26th of October 2015 02:10:23 AM

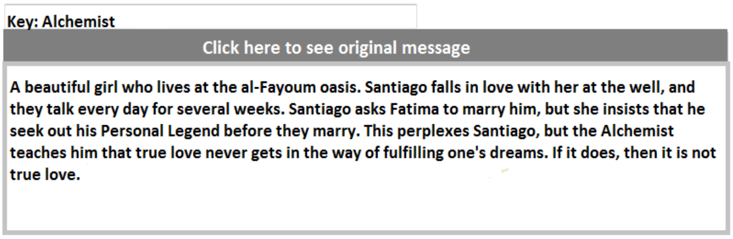
Key: 16

A learqtmrd itod vsj dtuep aq qse adMaxjrf japtp Pagqtaij maddp tg djue vtqs seo aq qse vedd agh qsex qadb eueox hax mjo peueoad veebp Pagqtaij apbp Maqtfa qj faoox stf lrq pse tgptpqp qsaq se peeb jrq stp Keopjgad Deiegh lemjoe qsex faoox Qstp keokdewep Pagqtaij lrq qse Adcseftpq qeacsep stf qsaq qore djue geueo ieqp tg qse vax jm mrdmtddtgi jgep hoeafp Tm tq hjep qseg tq tp gjq qore djue

Enter the key for this message

Click here to see original message

Figure 9: The GUI of the receiver without decryption.



Key: Alchemist

A beautiful girl who lives at the al-Fayoum oasis. Santiago falls in love with her at the well, and they talk every day for several weeks. Santiago asks Fatima to marry him, but she insists that he seek out his Personal Legend before they marry. This perplexes Santiago, but the Alchemist teaches him that true love never gets in the way of fulfilling one's dreams. If it does, then it is not true love.

Figure 10: The receiver end after decryption.

Name of the applications	Features						
	1. Is your communication encrypted in transit?	2. Is your communication encrypted with a key the provider doesn't have access to?	3. Can you independently verify your correspondent's identity?	4. Are past communications secured if your keys are stolen?	5. Is the code open to independent review?	6. Is the crypto design well-documented?	7. Has there been an independent security audit?
Proposed Secure Messaging System	**Yes**	**No**	**Yes**	**No**	**No**	**Yes**	**No**
Facebook Chat	Yes	No	No	No	No	No	Yes
Google Chat	Yes	No	No	No	No	No	Yes
Skype	Yes	No	No	No	No	No	No
SnapChat	Yes	No	No	No	No	No	No
Viber	Yes	No	No	No	No	No	No
Whats App	Yes	No	No	No	No	No	Yes
Yahoo Messenger	Yes	No	No	No	No	No	No

Table 3: Comparison features of the proposed system with others.

References

1. Rivest RL (1990) Cryptology. Handbook of Theoretical Computer Science.
2. https://www.eff.org/secure-messaging-scorecard.
3. Paar C, Pelzl J, Preneel B (2010) Understanding Cryptography: A Textbook for Students and Practitioners. Springer.
4. Liddell HG, Scott R, Jones H, McKenzie R (1984) A Greek-English Lexicon. Oxford University Press.
5. Diffie W, Hellma M (1976) New Directions in Cryptography. IEEE Transactions on Information Theory 22.
6. Schneier B (2014) Cryptanalysis of MD5 and SHA: Time for a New Standard. Computerworld.
7. Diffie W, Hellman M (1976) Multi-user cryptographic techniques. AFIPS Proceedings 45: 109-112.
8. Kahn D (1979) Cryptology Goes Public. Foreign Affairs.
9. Goshwe NY (2013) Data Encryption and Decryption Using RSA Algorithm in a Network Environment. IJCSNS International Journal of Computer Science and Network Security 13.
10. William Stallings (2006) Cryptography and Network Security Principles and Practices. Pearson Education Inc.
11. The Text Message Turns 20 (2012) CNN.
12. Federal Information Processing (2012) Announcing the ADVANCED ENCRYPTION STANDARD (AES).
13. James McCarey, Keeping Your Data Secure with the New Advanced Encryption Standard. MSDN Magazine.