

INFORMATION SECURITY MODEL USING TWOFISH ENCRYPTION AND DECRYPTION ALGORITHM

Abikoye, Oluwakemi C. and Ademarati, Oluwatoyin A.
Department of Computer Science, University of Ilorin, Ilorin, Nigeria
Kemi_adeoye@yahoo.com

Abstract

Cryptography has gained more attention from researchers due to the need to enable the security of messages sent over an unsecure network. Message sender want to ensure that only authorized receiver is able to interpret the message sent. So, even if a message falls in the hands of another person other than the authorized recipient, the message is still secured. This proposed system shows how a symmetric key algorithm (Twofish) is used to encrypt messages to make it secure when sent over the network. In this paper, the Twofish algorithm with a 16 bits character key length is implemented using JAVA programming language. The result is efficient because it gives a different ciphertext each time encryption is performed.

Keywords: Algorithm, encryption, ciphertext, Twofish Algorithm, Symmetric Key.

Introduction

Information security plays a pivotal role during internet communication in today's era of technology. It is tremendously important for people doing e-transactions (Shivangi, 2012). A lot of information ranging from texts, video streams, audios and others are usually communicated through the internet. Some of this information are important and private to individuals and organizations and should be kept away from outsiders, hence the need for information security. According to Sangapu and Gomatam (2014) the internet is a channel of communication between tens of millions of people and there is a great increase in its use even for commercial purposes. Due to these, security becomes a tremendously important issue to deal with.

Information Security is simply the process of keeping information secure: protecting its availability, integrity, and privacy. Mark (2013) in his book on information security thought of information security in the context of the three Ds: defense, detection, and deterrence - each of which is equally important. Defense reduces misuse and accidents, detection provides visibility into good and bad activities, and deterrence discourages unwanted behavior.

Information security uses cryptography to transform usable information into a form that renders it unusable by anyone other than an authorized user; this process is called encryption. Cryptography provides information security with other useful applications as well including improved authentication methods, message digests, digital signatures, non-repudiation, and encrypted network communications.

According to Shivangi (2012), cryptography is the practice and study of techniques used to secure communication in the presence of adversaries. It entails constructing and

analyzing protocols that disallow adversaries to influence information communication. Ayushi (2010) also refers to cryptography as the art of securing information by encoding messages so that they cannot be readable. The message to be sent is called a plaintext. The method of converting plaintext into unclear or unreadable text is called encryption. The encrypted (unclear or unreadable) text is called cipher text. The process of converting ciphertext back to plaintext is decryption. Encryption and decryption would not take place unless there is an algorithm that does the conversion of messages. According to Bruce (1996) a cryptographic algorithm (which is also referred to as a cipher) is a mathematical function used for encryption and decryption. Bruce further explained that the algorithm can be kept secret as in restricted algorithm. Restricted algorithms have drawbacks such as – the need to constantly change algorithm in order to block an unwanted user, unavailability of room for quality control and standardization, eavesdroppers' ease of purchasing product and learning algorithm and insecurity of algorithm if users are not good cryptographers.

However, generally known algorithms can be used with a key (which can be any one of the large number of values). Cryptographic algorithms can be categorized into two depending on how key is managed – public key cryptography and private key cryptography. Public key cryptography is also known as asymmetric key cryptography while private key is also known as secret key or symmetric key cryptography (Sangapu & Gomatam, 2014). Symmetric key algorithms allow one key to be used for encryption and decryption while asymmetric key algorithms use different keys for encryption and decryption (Nivedita & Sapna, 2015). The RSA and Diffie-Hellman are public key algorithms. Symmetric key cryptographic ciphers come in two varieties, stream and block ciphers. Stream ciphers work on a stream of bits or bytes. Stream ciphers are used for securing data of terminal and wireless applications. Block ciphers perform encryption or decryption on fixed size block of data (Ranjeet, Vivek, Jibi & Rajni, 2014). Commonly used block ciphers are Data Encryption Standard (DES), Advanced Encryption Standard (AES), Blowfish, Twofish, Serpent, IDEA, RC4, CAST5 and so on.

In this paper, Twofish cipher is implemented to secure information. A messaging system is modeled using Twofish cipher to secure the message before they can be sent to their destination. The rest of the paper talks about review of related works on Twofish algorithm, methodology, results & discussion and conclusion.

Literature Review

A General Review of Information Security

Information security has been in existence a long time. This claim is illustrated by an event in the Dutch history. In January 1684, when a war commenced between the Dutch Republic and France; it seemed like the French were on the winning side so Stadholder Williams III, a semi-hereditary commander of the army and navy as well as chief executive of the foreign policy of the Republic was willing to fight the French in the Southern Netherlands. The French ambassador Count D'Avaux knowing this entered direct negotiations with the city council of Amsterdam in order to prevent that city from raising money for troops as the Stadholder had requested. The act of D'Avaux was a direct interference in the internal affairs of the Dutch State and it was an uncommon thing for a French ambassador to do.

However, the Stadholder decided to shadow the ambassador's messenger at a time he was most likely carrying a letter on the negotiation to the King. He successfully attacked and robbed the messenger with the help of some Maastricht garrison horsemen leaving him with his boots and jacket. This affair caused much distress to the Amsterdam city council but D'Avaux reassured them that the letter was fully coded and that no one could read it without a key.

On 16th February 1684, Stadholder entered a meeting with the Amsterdam city council with the decoded copy of the letter, accusing her of treason. D'Avaux could only help the Amsterdam by pretending that William's cryptanalyst had interpreted the letter wrongly by producing a different copy (which he claimed was the genuine letter) of the letter for circulation. To counter this, William III released a copy leaving out many unsolved code groups at first, and later released a full version plain text accompanied by the solutions from other letters which were intercepted at the same time and which were compromising. With this, William was able to counter D'Avaux lies (Story by Kurtz G.E in Willem III en Amsterdam). The incident made William III who was to ascend the British throne in 1689 well aware of the benefits of intercepting mail. Mail interception became a trending weapon against opponents. It is information warfare at its best (Karl & Jan, "n.d."). According to Singh, Vaish and Kumar (2014), at the close to the 20th century, increase in computer networks gave rise to the Internet, the first manifestation of a global network of networks. Due to the dominant increase in networked computers in computing, there came a need to secure computers physically and the information stored on it, as it is more exposed to threats on the internet. Internet security of this day was discussed by some researchers.

Today, the Internet has brought millions of unsecured computer networks into communication with each other. Our ability to secure each computer's stored information is now influenced by the security on each computer to which it is connected.

The rapid growth and widespread use of electronic data processing and electronic business conducted through the Internet, along with numerous occurrences of international terrorism, fueled the need for better methods of protecting the computers and the information they store, process and transmit. Governments, military, corporations, financial institutions, hospitals, and private Businesses collect and store huge volumes of confidential information. The information may be about employees, customers, research, products or financial operations. Most of this information is collected, processed and stored on computers and transmitted across networks to other computers. If this information fell into the wrong hands, it could lead to lost business, law suits, identity theft or even bankruptcy of the business. With cybercrime on the rise, protecting your corporate information and assets is vital. Protecting confidential information is a business requirement, and in many cases also an ethical and legal requirement (Singh *et al.*, 2014). Cryptography is a major technique in information security.

Cryptography and its Classification

Cryptography can be classified based on different criteria. Based on time, it can be classified into classical cryptography and medieval (modern) cryptography.

Classical Cryptography

Once upon a time, keeping data secret was not hard. Few people were literate, the use of written language alone often sufficed to keep information from becoming general knowledge. To keep secrets then, you simply had to write them down, keep them hidden from those few people who could read, and prevent others from learning how to read. Deciphering the meaning of a document is difficult if it is written in a language you do not know (Mark, 2013). Mark (2013) explains that a new method of hiding information had to be adopted when reading and writing became common amongst people. Traditional ciphers were later adopted. Traditional ciphers used two techniques for hiding information from an intruder: substitution and transposition.

Medieval Cryptography

Modern cryptography is majorly subdivided into symmetric and asymmetric key cryptography.

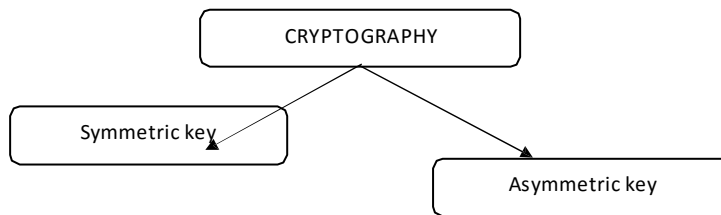


Figure 1: Modern cryptography techniques

Symmetric key cryptography: Cryptography involves two opposite actions-encryption and decryption. A key is combined with a plaintext to make it a ciphertext. Bruce (1996) claimed that the security of an algorithm is based on the key. In symmetric (which is also called secret key cryptography or private key cryptography), a single key is used for both encryption and decryption. As shown in Figure 2.2, the sender uses the key (or some set of rules) to encrypt the plaintext and sends the ciphertext to the receiver. The receiver applies the same key to decrypt the message and recover the plaintext. With this form of cryptography, it is obvious that the key must be known to both the sender and the receiver; that, in fact, is the secret. The biggest difficulty with this approach, of course, is the distribution of the key.

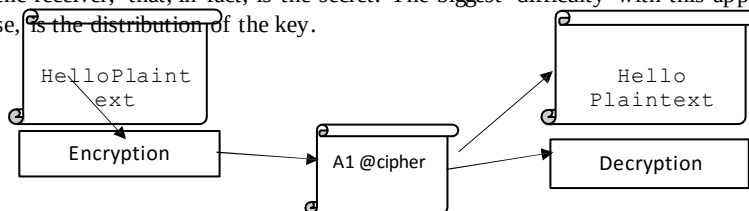


Figure 2: Symmetric key cryptography.

Examples of algorithms that use the symmetric key scheme are Data Encryption Standard (DES), Advanced Encryption Standard (AES), Blowfish, Serpent, Twofish etc.

Asymmetric key cryptography: This kind of scheme uses two keys. One for encryption and the other for decryption. The encryption key need not be kept private. It is known by everyone and used by everyone to encrypt their message hence making the scheme a public key. However a private key known only to the receiver is used to decrypt the message.

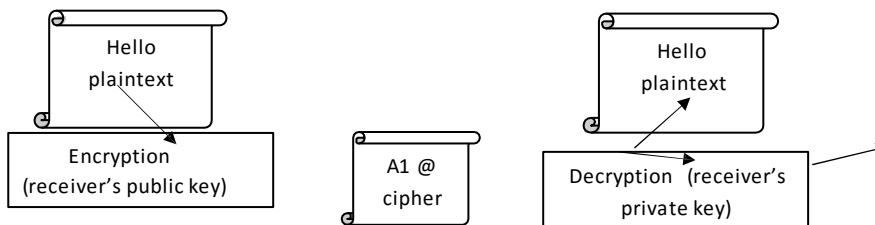


Figure 3: Asymmetric key cryptography.

Twofish Algorithm

The proposed system is designed using the Twofish algorithm. The Twofish algorithm is a 128 bits symmetric block cipher. It accepts a key length of 128-192 and 256 bits. Its structure is a Feistel network and it operates a 16 round encryption process (Bruce et al, 1998). Below are the steps involved in Twofish algorithm;

1. Plaintext (128-bit) $\xrightarrow{\text{Split using}}$ $P_0, \dots, P_3$ (32-bits each)

$P_0, \dots, P_{15}$ Split using little-endian conversion

$$P_i = \sum_{j=0}^3 p(4i+j) \cdot 2^{8j} \quad i = 0, \dots, 3$$

2. Pre-whitening or input whitening - Each 32 bits is XORed with a 32 bits key to produce a whitening. (The result of whitening gives R_0, R_1, R_2 and R_3).

$$R_{0,i} = P_i \oplus K_i \quad i = 0, \dots, 3$$

3. 16 Iterations of round functions – This is a major stage in the algorithm. It is the body of the entire encryption process. The result of the input whitening – R_0, R_1, R_2 and R_3 are manipulated to produce new four 32 bits output. The following steps are carried out;

- i. The first two 32 bits (R_0 & R_1) are passed into an F-function to produce F_0 and F_1 .
- ii. F_0 is XORed with R_2 and the result is rotated to the right by one bit to give C_2 .
- iii. R_3 is first rotated to the left by one bit and the result is XORed with F_1 to produce C_3 .
- iv. The new result is R_0, R_1, C_2 and C_3 . The result is swapped (to give C_2, C_3, R_0 & R_1) before it passed into the next round.

$$\begin{aligned} (F_{r,0}, F_{r,1}) &= F(R_{r,0}, R_{r,1}, r) \\ R_{r+1,0} &\equiv \text{ROTR}(R_{r,2} \oplus F_{r,0}, 1) \\ R_{r+1,2} &= R_{r,0} \end{aligned}$$

$$R_{r+1,3} = R_{r,1}$$

for $r = 0, \dots, 15$ and where ROR and ROL are functions that rotate their first argument (a 32-bit word) left or right by the number of bits indicated by their second argument. This process is repeated 16 times, this is why it is called the Twofish rounds.

4. Output whitening – XORing with sub-key.

$$C_i = R_{16, (i+2) \bmod 4} \oplus K_{i+4} \quad i = 0, \dots, 3$$

5. $C_0, \dots, C_3$ of ciphertext $\xrightarrow{\text{little-endian conversion}}$ 128-bit ciphertext, c

Elements of Twofish

F-Function - The function F is a key-dependent permutation on 64-bit values. It takes three arguments, two input words R_0 and R_1 , and the round number 'r' used to select the appropriate subkeys. The results are achieved by doing the following:

- R_0 is passed through a g function, which yields T_0 .
- R_1 is rotated left by 8 bits and then passed through the g function to yield T_1 .
- The results T_0 and T_1 are then combined in a PHT (Pseudo Hadamard Transform) and two words of the expanded key are added.

$$T_0 = g(R_0)$$

$$T_1 = g(\text{ROL}(R_1, 8))$$

$$F_0 = (T_0 + T_1 + K_{2r+8}) \bmod 2^{32}$$

$$F_1 = (T_0 + 2T_1 + K_{2r+9}) \bmod 2^{32}$$

where (F_0, F_1) is the result of F .

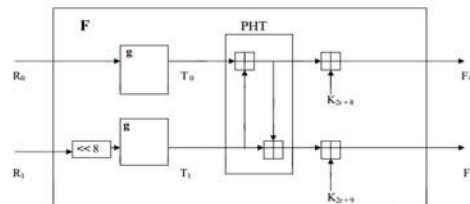


Figure 4: F-function

Function-G - The function g is the most important part of Twofish and forms the heart of the algorithm. The following are done in the function g :

- The input word X is split into four bytes.
- Each byte is run through its own key-dependent S-box. Each Sbox is bijective, takes 8 bits of input, and produces 8 bits of output.
- The four results are interpreted as a vector of length 4 over $GF(2^8)$, and multiplied by the 4×4 MDS matrix (using the field $GF(2^8)$ for the computations).

- The resulting vector is interpreted as a 32-bit word which is the result of g.

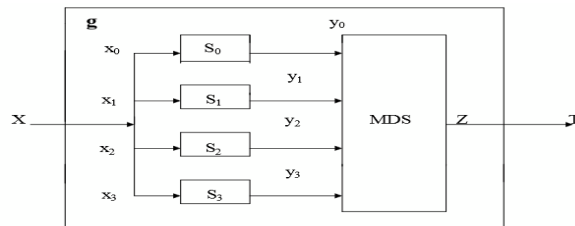


Figure 5: Function-G

S-BOXES - The s-box (substitution box) is a basic component of a symmetric algorithm used for substitution. In block ciphers, they are typically used to obscure the relationship between the key and the ciphertext. An S-box is a table-driven non-linear substitution operation. They vary in both input size and output size, and can be created either randomly or algorithmically. S-boxes were first used in Lucifer, then DES, and afterwards in most encryption algorithms. Twofish uses four different, bijective, key-dependent, 8-by-8-bit S-boxes (Bruce et al, 1998). Singh ('n.d') explains that each s-box consists of three 8-by-8-bit fixed permutations chosen from a set of two possible permutations q_0 and q_1 . Between these three permutations, XORed operations are performed with subkeys S_0 and S_1 . These subkeys are computed only once for a particular global key and stay fixed during the entire encryption and decryption process.

MDS Matrix - According to Wikipedia, an MDS (Maximum Distance Separable) matrix is matrix representing a function with certain diffusion properties that have useful applications in cryptography. An MDS code over a field is a linear mapping from a field elements to b field elements, producing a composite vector of a + b elements, with the property that the minimum number of non-zero elements in any non-zero vector is at least b + 1. Put another way, the "distance" (i.e., the number of elements that differ) between any two distinct vectors produced by the MDS mapping is at least b + 1.

PHT - Wikipedia describes a pseudo-Hadamard transform as a reversible transformation of a bit string that provides cryptographic diffusion. The bit string must be of even length, so it can be split into two bit strings a and b of equal lengths, each of n bits. The pseudo-Hadamard transform (PHT) is a simple mixing operation that runs quickly in software.

Given two inputs, a and b, the 32-bit PHT is defined as:

$$\begin{aligned} a' &= a + b \bmod 2^{32} \\ b' &= a + 2b \bmod 2^{32} \end{aligned}$$

Bruce et al (1998) however discussed that Twofish uses a 32-bit PHT to mix the outputs from its two parallel 32-bit g functions. This PHT can be executed in two opcodes on most modern microprocessors, including the Pentium family.

Key Schedule - The key schedule is the means by which the key bits are turned into round keys that the cipher can use. Twofish needs a lot of key material, and has a complicated key schedule. To facilitate analysis, the key schedule uses the same primitives as the round function.

Review of Related Literature

In 2016, Aparna *et al.*, did a study on the Twofish algorithm. It was concluded that encryption algorithm and the key schedule must be designed in tandem. Key should be as short as possible. It is much harder to design an algorithm with a long key than an algorithm with a secret key. Future work can be done to minimize the key and security transmits it to the receiver. In future Twofish can be used for other digital media files like image, audio, and video.

Gehlot, Biradar and Singh (2013), modified the Twofish algorithm using 128 and 192 bits and implemented it on VHDL (very high speed integrated circuit hardware description language). Their major aim was to efficiently implement a Twofish algorithm with the least delay and possessing high performance in terms of power and area used. The three used the software Xilinx 6.1 – xst and the language VHDL for their work. Xilinx software did the simulation of the modified process. Inputs were converted into binary form and given as input to the "Model-Sim Simulator" of Xilinx 6.1 xst, and in the output produced the RTL diagram, the waveform and the synthesis report, from which the values of delay and area were gotten.

All the modules and functions are interrelated hence, after modifying MDS and PHT, function g and function f also got modified. The results showed the delay of Twofish algorithm of 128-bit key and modified twofish of 128-bit key, delay results were compared. The analysis showed that modified algorithm has less delay than the conventional one. After that the delay results of Twofish algorithm with 192-bit key and modified Twofish with 192-bit key were compared. According to the results it was clear that modified 192-bit key Twofish algorithm has less delay than 192-bit Twofish. Gehlot and his colleagues also proposed that the algorithm can be implemented on sensor networks and ad-hoc networks on cross-layers in future. Also, the other modules of algorithm can be modified to reduce further delay.

Durgadevi, Selvanathiya and Sivasubramanian ("n.d.") in their work used the ALTERA FPGA device to implement a two fish algorithm considering only the 128 bits key length to make their work less complex. They improved the process speed of the Twofish cryptographic algorithm and designed it to be suitable for use in a wireless communication environment. Durgadevi and his colleagues further explained that MDS

block implemented in Twofish takes a lot of process time thereby making Twofish a slow algorithm.

Due to this, Durgadevi and others used the MDS-M2 (Maximum distance separable modulo-2) to control an increase of process time and reduce data process time. In conclusion, even though Twofish is slower than Rijndael, with the new MDS-M2, they claimed that the new Twofish cryptosystem algorithm by the simulation results confirmed a performance improvement of 11% than the existing Twofish algorithm. They concluded that the security system whose Twofish cryptographic algorithm used an improved MDS-M2 block is very suitable for wireless communication environment.

Mirza and Murphy (1999) made an observation on the key schedule of Twofish. They stated that key scheduling of Twofish has two properties that are contrary to claims implicit in the original submission of Twofish and could potentially be exploited. Firstly, both the pre- and post-whitening subkeys of Twofish occur with a non-uniform distribution, which gives information about the key. Secondly, the round subkeys of every reduced version of Twofish (that is, a version of Twofish with S0, S1) fixed occurs with a non-uniform distribution, which gives information about the key. An attack on any reduced version of Twofish would have cryptographic consequences for the full version of Twofish. For example, the unbalanced key schedule described in reduced Twofish may aid an attacker in deriving collisions if Twofish is used in a Davies-Meyer hash.

Singh ('n.d') claimed that Twofish is named due to the use of two main diffusion elements – MDS and PHT (Pseudo Hadamard Transform). (Moreover it is customary to name ciphers after sea-creatures and Twofish is the successor of Blowfish). Singh did a deeper analysis of its most significant diffusion element, the MDS matrix and proposed a VHDL model for the hardware implementation of the matrix. This he stated could be used to observe outputs that conformed the expected results from theory. Bruce *et al.* (1998) in their article on two fish claimed that Twofish was their submission to the AES selection process. They said that it met all the required National Institute of Standards and Technology (NIST) criteria—128-bit block; 128-, 192-, and 256-bit key; efficient on various platforms; etc.—and some strenuous design requirements, performance as well as cryptographic, of our own.

Methodology

Twofish algorithm is implemented using JAVA programming language. The system algorithm describes the step by step way of carrying out the precise problem. The proposed system uses two major algorithm which are reverse of each other. They are;

1. Encryption algorithm.
2. Decryption algorithm.

Encryption algorithm

The encryption algorithm is carried out as follows;

1. Examine the 128 bits block of input text and divide it into four 32 bits.
2. Whiten the input text by XORing each 32 bits with a 32 bits subkey.
3. Pass the first two 32 bits (R_0 & R_1) of the whitening into an F-function to produce F_0 and F_1 .
4. F_0 is XORed with R_2 and the result is rotated to the right by one bit to give C_2 .
5. R_3 is first rotated to the left by one bit and the result is XORed with F_1 to produce C_3 .
6. The new result is R_0, R_1, C_2 and C_3 . The result is swapped (to give C_2, C_3, R_0 & R_1) before it passed into the next round.
7. Step 3 to 6 repeated 15 more times using the swapped output of the preceding round.
8. The result of the final round is XORed with sub-key to produce an output whitening.
9. The final four 32 bits ciphertext is converted to a 128 bits ciphertext using the little-endian conversion.

F-Function Algorithm

The following are the steps carried out in the f-function:

1. Pass R_0 into a function-g to yield T_0 .
2. Rotate R_1 left by 8 bits and pass the result through a function-g to produce T_1 .
3. T_0 and T_1 are combined in a PHT.
4. The results from step 3 above are combined with two words of expanded key from the key schedule to give F_0 and F_1 which are the results of the f-function.

Function-G Algorithm

The following are the steps involved in the function-g:

1. The input word X is split into four bytes.
2. Each byte is run into its own key-dependent s-box.
3. Each s-box produces an 8 bits output which are passed through an MDS Matrix to produce a 32 bits output for the function-g.

Algorithm for S-boxes

The steps in s-boxes include;

1. Each s-box consists of a set of three 8 by 8 permutation chosen from a set of two possible permutation q_0 and q_1 .
2. XORs are performed between these three-permutation using the subkeys S_0 and S_1 to produce the result of the s-boxes and sent to the MDS matrix in the function-g.

MDS Matrix Algorithm

The following are the steps involved in MDS matrix;

1. Multiply a vector of four byte using the Galois Field (2^8) with the primitive polynomial, $x^8+x^6+x^5+x^3+1$.
2. After multiplication a 32 bits result is produced.

PHT

In the PHT, a simple transformation is done on a 32bits output using the equation below;
 $a' = a + b \bmod 2^{32}$ $b' = a + 2b \bmod 2^{32}$

Decryption algorithm

The decryption algorithm is a reverse of the encryption algorithm above so that encrypted messages when decrypted produces the same text as the ones encrypted.

Results and Discussion

This section discusses how the proposed system works. The proposed system does not share files between the networks. It also enables messages to be sent over the network.



Figure 6: Plaintext with 16 characters key length

The encryption interface allows users to enter their text in plain form and enter an encryption key alongside. On clicking the encrypt button, the plaintext clears and is replaced with the ciphertext as shown in figure 7. The clear button allows users to clear the interface so that another data can be inputted. Once the send button is clicked, the message is sent to destination over the network as shown in figure 8.

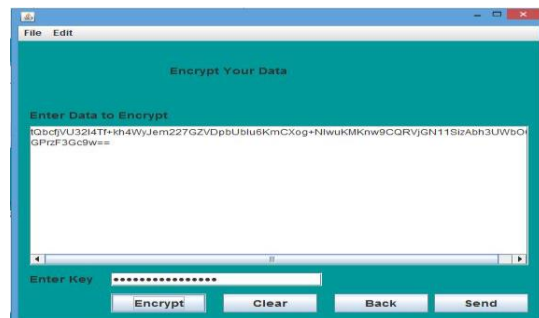


Figure 7: Corresponding ciphertext after encryption.

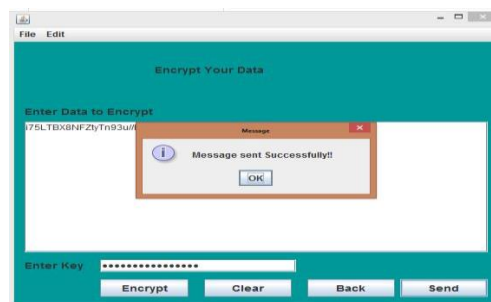


Figure 9: Sending of text

The Decryption Interface allows the user to decrypt ciphertext by clicking on the decrypt button after entering the correct key. If a wrong key is entered the user gets an incorrect text and is not able to get the real plaintext. New ciphertext can be decrypted by clearing old text and inputting new ones. On clicking back, the main menu appears. Figure 10 shows the corresponding plaintext after decryption using the correct key at the receiver side.

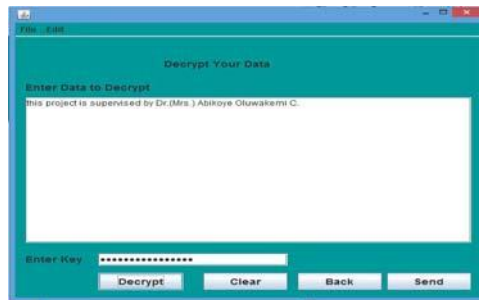


Figure 10: Corresponding plaintext after decryption

Conclusion

There are many messaging systems available for sending message from one end to another over the internet. Many of these systems lack message security. Unwanted people are able to read the messages without the permission of the sender or receiver. This is why this study is done to ensure that a medium which is enhanced with information security using Twofish algorithm is carried out. Twofish system is a private key cryptosystem that is based on confusion elements like MDS matrix, s-boxes, PHT, functions. In this work, a message security model was developed using Twofish algorithm with a single private key for both encryption and decryption, hence, it is symmetric encryption algorithm. The algorithm gives a different ciphertext each time encryption is performed using a different key. However, the disadvantages of Twofish algorithm includes its slow speed, and also it can send a limited file size and encrypts only text, many keys have to be generated for every message. Hybridization that is combination of two or more algorithms can be done to improve the efficiency and application of the system for securing data and information.

Recommendation

The proposed system is recommended for exchange of messages over the internet. The elements of Twofish are effective for diffusion and toggling of plaintext. Twofish elements can be improved by making adjustment in order to create a stronger encryption. Also, the elements can be improved so that the algorithm works faster. Further research could be done by hybridizing both symmetric and asymmetric algorithms in order to improve the efficiency and application of the system for securing data and information.

References

- Aparna, K., Jyothy, S., Harini, M., & Indhumathi, V. (2016). A Study of Twofish Algorithm. *International Journal for Engineering Research and Application (IJERA)*, 4(2), 148-150.
- Atbash. (n.d). In *Wikipedia*. Retrieved May 12, 2016, from <https://en.wikipedia.org/wiki/Atbash>

- Ayushi. (2010). A Symmetric Key Cryptographic Algorithm. *International Journal of Computer Applications*, 1(15), 1-4.
- Bruce, S. (1996). *Applied Cryptography* (2nd edition). New Jersey Place of publication: John Wiley & Sons.
- Bruce, S., John, K., Doug, W., David, W., Chris, H., & Niels, F. (1998). Twofish: A 128-Bit Block Cipher. AES Submission.
<http://www.counterpane.com/twofish.html>
- Caesar Cipher. (n.d.). In *Wikipedia*. Retrieved May 12, 2016, from https://en.wikipedia.org/wiki/Caesar_cipher
- Durgadevi, K., Selvanathiya, & Sivasubramanian, M. (n.d). Implementation of Secure Master Using Modified Twofish Algorithm in FPGA Devices. *International Journal for Engineering Research and Application (IJERA)*, 1(3), 507-512.
- Gehlo, P., Biradar, S., & Singh, B. (2013). Implementation of Modified Twofish Algorithm using 128 and 192-bit keys on VHDL. *International journal of computer applications*, 70(13), 37-42.
- Information security (n.d.). In *Wikipedia*. Retrieved May 16, 2016, from https://en.wikipedia.org/wiki/Information_security
- Karl, L., & Jan, B. (n.d). The History of Information Security: A Comprehensive Handbook. Elsevier B.V.
- Landge, I., Bharmal, T., & Narwankar, P. (2012). Encryption and Decryption of Data Using Twofish Algorithm. *World Journal of Science and Technology*, 2(3), 157-161.
- Mansoor, E., Shujaat, K., & Umer, B. (2013). Symmetric Algorithm Survey: A Comparative Analysis. *International journal of computer applications*, 61(20), 12-19.
- Mark, R. (2013). *The Complete Reference: Information Security* (2nd edition). New York. Mc Graw-Hill companies.
- MDS matrix. (n.d.). In *Wikipedia*. Retrieved June 7, 2016, from https://en.wikipedia.org/wiki/MDS_matrix.
- Mirza, F., & Murphy, S. (1999, March). An Observation on the Key Schedule of Twofish. In *The Second AES Candidate Conference, Printed by the National Institute of Standards and Technology Gaithersburg, MD* (pp. 151-154)
- Mohammadreza, N., Behnam, S., Alireza, M., & Kambiz, B. (2015). Comparison of Serpent, Twofish and Rijndael Encryption Algorithms in Teleophthalmology System. *Advances in Natural and Applied*, 9(4), 137-149.
- Murphy, S. (2000, April). The Key Separation of Twofish. In *Proceedings of the 3rd AES Conference (AES3)*.
- Nivedita, B., & Sapna, S. (2015). A comparative study of some symmetric and asymmetric key cryptography algorithms. *International Journal of Innovative Research in Science Engineering and Technology*, 4(3), 1028-1031.
- Practical cryptography: Atbash ciphers. (n.d.) In *Wikipedia* Retrieved May 12, 2016, From <http://practicalcryptography.com/ciphers/atbash-cipher-cipher/>

- Ranjeet, M., Vivek, S., Jibi, A., & Rajni, M. (2014). Analysis and Comparison of Symmetric Key Cryptographic Algorithms Based on Various File Features. *International Journal of Network Security & its Applications (IJNSA)*, 6(4), 43-52.
- Sangapu, V.A., & Gomatam, V.A. (2014). Recent Advancements on Symmetric Cryptography Techniques -A Comprehensive Case Study. *Global Journal of Computer Science and Technology: Graphics & Vision* 14(2), 19-30.
- Shivangi, G. (2012). A Survey on the Applications of Cryptography. *International journal of science and technology* 1(3), 137-140.
- Singh, A. ('n.d'). Study of MDS Matrix used in Twofish AES (Advanced Encryption Standard) Algorithm and its VHDL Implementation.
- Singh, A., Vaish, A., & Kumar, K. (2014). Information Security: Components and Techniques. *International Journal of Advanced Research in Computer Science and Software Engineering* 4(1).1072- 1077.
- Shon, H. (2012). CISSP All-In-One Exam Guide book (6th Edition). New York. McGraw-Hill/Osborne Media.
- Substitution ciphers. (n.d.). In *Wikipedia* Retrieved May 12, 2016, from https://en.wikipedia.org/wiki/Substitution_cipher The English Dictionary, Retrieved May 16, 2016, from <https://wiktionary.org>
- Transposition ciphers (n.d.). In *Wikipedia* Retrieved May 12, 2016, from https://en.wikipedia.org/wiki/Transposition_cipher
- William, S. (2011). Cryptography and Network Security Principles and Practice. (5th edition) Boston. Prentice Hall.