IMPLEMENT A NOVEL SYMMETRIC BLOCK CIPHER ALGORITHM

Ali M Alshahrani1 and Prof. Stuart Walker

Computer Science and Electronic Engineering,
University of Essex,
Wivenhoe Park, Colchester, Essex, UK, C04 3SQ

ABSTRACT

Cryptography technology is a security technique used to change plain text to another shape of data or to symbols, which is known as the cipher text. Cryptography aims to keep the data secure during its journey through public networks. Currently, there are many proposed algorithms that provide this service especially for sensitive data or very important conversations either through mobile or video conferences. In this paper, an inventive security symmetric algorithm is implemented and evaluated, and its performance is compared to the AES. The algorithm has four different rounds for each quarter of the key container table, and each of them serves to shift the table. The algorithm uses the XOR operation, which, being lightweight and cheap, is very appropriate for use with Real Time Applications. The result shows that the suggested algorithm spends less time than AES although it has 16 rounds and the numbers used to mix up the table are big.

KEYWORDS

Encryption, Decryption, Key size, Block size. AES, Shared secret key.

1. INTRODUCTION

Real Time Applications (RTAs) stand for all data types, such as images, videos, and voices, and their main feature is their huge size compared to text. This large size is a concern because it may cause a significant time delay that will affect the quality of the data. Transmitting an RTA through the Internet is very risky, and efficient security measures must be applied to protect the data [1][2]. In recent years, RTAs' Internet Protocols (IP) have been developed and their use has become common around the world. Most companies have developed many intelligent applications that can be used by computers, laptops, and smartphones to exchange all the multimedia data [3].

A cryptography system is one of the most important security techniques as it is guaranteed to exchange sensitive data in a secure way. It aims to change the original shape of the data before sending it to the receiver through the Internet. Both communication participants must be aware of the key that will be used to encrypt and decrypt the data [4][5][6]. As a result, many cryptography systems have been proposed and subsequently implemented to protect the data. However, some

DOI:10.5121/ijcis.2014.4401

of these are very good with text but not so good with multimedia. Moreover, some of these techniques contain a very small key that is easy to break or that can be attacked using very simple techniques.

Actually, delay is the key to the quality of any proposed solution so applying quality of service (QoS) to the security system is very important. RTAs use a protocol called the User Datagram Protocol (UDP); this is considered as more functional than the Transmission Control Protocol (TCP) since the important feature of RTAs is not to transmit every single packet but to continue to transmit the packets even if any loss occurs during the process. The packet-loss dilemma could be happen in any part of the network or at the end of the system and can be due to many reasons, such as network failure and congestion [7][8].

The end-to-end delay is affected by the huge size of multimedia, such as video and voice, which are very sensitive during transmission. Therefore, reducing the time to the lowest possible value that the system needs to execute the algorithm, apply the algorithm, and code and decode, is very important [2][9].

A reasonable rate of end-to-end one-way voice delay is 150 ms but a maximum delay of 400 ms is still acceptable but not suitable for a large multimedia size as stated by the International Telecommunication Union (ITU-T) in its G114 recommendation. Thus, the proposed system will overcome the drawbacks of some of the current algorithms by using a new approach.

2. BACKGROUND

2.1 Cryptography:

Some of the encryption methods have existed for centuries or even millennia; for example, the Egyptians developed hieroglyphic writing. However, in the past few decades, the changes in encryption techniques have taken place because the current generation of computers can carry out the difficult task of seeking methods to decipher a code, and they can certainly achieve this far faster in comparison to a human being. Therefore, the applied encryption techniques have to be far more sophisticated and complicated. An encryption and decryption system is defined as a set of algorithms that convert plain text data to the cipher text on the sender side using an agreed key (encryption). The decryption process is done on the receiver side by using the agreed key to obtain the plain text again. The cryptosystem has 5-tuble grouped as E, D, M, K, and C. E stands for the encryption algorithm whereas D stands for decryption algorithm. The encryption and decryption is very important to evaluate the level of system quality. M or P is the plain text, that is, the original text before its transmission, and this is always located on the sender side. On the other hand, C is the cipher text which is the plain text after decryption. The key takes K as shortcut letter. The key is an extremely important factor in the cryptography process, and its length and its creation technique are controlled in the strongest of the algorithms [10][11].

2.2 Types of Cryptographic algorithms:

2.2.1 Symmetric Key:

Symmetric cryptography, commonly called secret or conventional encryption, refers to the type of encryption where the keys of encryption and decryption have equivalent values. Another definition of symmetric encryption describes it as a shared key cryptography or shared secret cryptography due to the fact that it applies only one “shared” key, which is employed in encrypting and decrypting the message.

The application of symmetric cryptography has both benefits and disadvantages. The advantages of employing symmetric encryption include authentication that the key remains secret, the encryption of data is performed instantly, and key symmetry permits encryption and decryption using the same key. Moreover, it is considered as a fast technique because there is no need for additional processes.

However, in the case that the key is disclosed (guessed, lost, or stolen, etc.), the scan or intercept instantaneously would decrypt anything encrypted by applying the key. The suggested solution here would be to change the keys regularly with each set of packets [12].

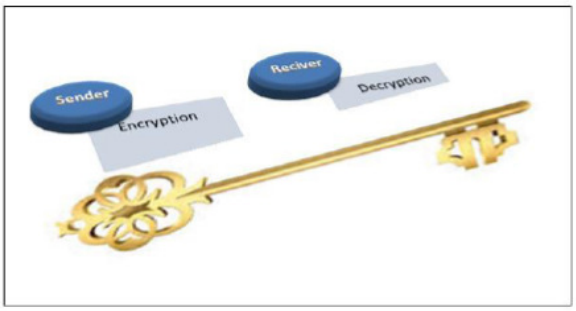

Figure 1: Symmetric key.

2.2.2 Asymmetric Key:

The term "asymmetric encryption", which is commonly referred to as public key encryption,employs two different keys for the purpose of encryption and decryption. One of the two keys in cryptography is a public key, which can be made available to anyone. However, the second key,known as a secret or a private key, is a mathematically-related one. This cryptography key is the one which has to be kept confidential from others. In other words, only the owner can gain access to the secret key or its back-up duplicates. Thus, every user owns two keys, a public key and a private key.

The main advantages of having a public key are that it provides a very strong key that is not easily broken, and the key exchange is very secure. On the other hand, the drawbacks of asymmetric encryption are that its keys are very long in order to provide a good resistance to attacks, which means more processes are required, and thus the time required will be increased.

Figure 2: Asymmetric key.

3. THESUGGESTEDALGORITHM

In this paper, a symmetric block cipher algorithm is designed to achieve a high level of security in less time than is required for some other systems. It has 4 complicated rounds that will shift a smart table that consists of 4 separate quarters, and each single quarter has 64 bytes. Each quarter in this table will be used to generate 16 bytes as a key with a total of 64 bytes in each quarter. Moreover, this table has a variable key length, and the maximum generated key could be 2048-bits.

The algorithm has a table called a key container table that contains of 256 bytes. This table will be shifted by the agreed shared secret key. The key length here is extremely long compared to the other existing algorithms, such as AES. The length of the key and the complicated rounds here will make the algorithm fast as well as very difficult to break.

1) The main table (Keys Container):

The key container table is used to generate a very strong key with 256 bytes, and this table must be announced. The feature here is that the system deals with the table as a four different tables. This table contains 256 bytes, but the used mechanism generates only 64 bytes. The table will be generated automatically or by using a published secret algorithm, such as SHA-256. Matrix R comprises random numbers and is defined below:

$$R=\begin{bmatrix} r1,1 & \cdots & r1,16 \\ \vdots & \ddots & \vdots \end{bmatrix} \quad (1)$$

$$ri,j=\{n\in Z^{+}|0\leq n\leq 255\} \quad (2)$$

As explained above, this matrix has four parts, each of which is 8 × 8 and thus contains 64 entries (or bytes).

The parts (table's quarters) are defined $\begin{bmatrix} Q1 & Q2 \\ Q3 & Q4 \end{bmatrix}$, aswhere Q1-4 are quarter 1 to 4.

2) The shared secret key:

A shared secret key must be exchanged by an efficient key management algorithm such as Diffie-Hellman. It aims to mix up the key container table in all possible directions (up, down, right, and left) in order to generate the key. The main advantage here is in the mechanism used to mix up the quarters of the table. The system shifts the quarters among themselves and each quarter is exchanged with the other quarters. Each quarter of the table will be the main quarter in the case of regeneration using another key. For example, the rounds will start from quarter 1 to generate the first 64 bytes and from quarter 2 to generate another 64-bytes key and so on. Matrix A uses the secret key to generate the key, which is defined below:

$$A = \begin{bmatrix} a1,1 & \cdots & a1,4 \\ \vdots & \ddots & \vdots \\ a16,1 & \cdots & a16,4 \end{bmatrix} \quad (3)$$

$$a_{i,j} = \{n \in Z^+ | 0 \leq n \leq 255\} \quad (4)$$

There are four rounds for each quarter, and these rounds will be applied in two different techniques. The first one applies the four rounds together on the key container table once. Secondly, each quarter in table 1 will be re-arranged independently depending on the values in each round in the table. In matrix A, a1,j and a2,j contain values that are used for shifting rows up and down respectively, and a3,j and a4,j contain entries that are responsible for shifting columns left and right respectively.

The shifting in a1,j and a3,j occurs in x units where x is defined as follows:

$$x = \{n \in Z^+ | n = 2k - 1, 1 \leq n \leq 8\} \quad (5)$$

and the shifting in a2;j and a4;j occurs in y units where y is:

$$y = \{n \in Z^+ | n = 2k, 1 \leq n \leq 8\} \quad (6)$$

The shifting operations are applied on any paired quarters. In other words, two quarters from matrix R are placed together in order to perform the shifting. The first four rows in matrix A contain the data to be used for shifting the paired quarters of Q1-Q1, Q1-Q2, Q1-Q3 and Q1-Q4. The second four rows are used for shifting Q2-Q1, Q2-Q2, Q2-Q3 and Q2-Q4, and by the same token, the third and fourth rows are also used for shifting the rows and columns of Q3-Q1, Q3-Q2, Q3-Q3 and Q3-Q4, and Q4-Q1, Q4-Q2, Q4-Q3 and Q4-Q4 respectively.

3) Generating Matrix N:

In this section, matrix N is introduced, which is the result of applying the movement rules in matrix A to matrix R, which contains some randomly generated numbers within a specified range.

$$N=\begin{bmatrix} n1,1 & \cdots & n1,16 \\ \vdots & \ddots & \vdots \\ n16,1 & \cdots & n16,16 \end{bmatrix} \qquad (7)$$

As shown below, matrix N, which is the rearranged version of matrix R, has the same dimensionality as matrix R.

The steps taken to generate matrix N are explained next.

Four main shifting operations are used in this encryption algorithm: shifting rows up (U) and down (D), and shifting columns left (L) and right (R).

The order in which these operations are executed is U, L, D, and R.

Assuming we are to apply the values of a1,1, a1,2, a1,3, a1,4 in matrix R, we start with a1,1 and the first operation (U). Given it is the first round (n = 1), eq. 5 (i.e. 2n - 1) is used to determine which row to shift up . Therefore, in the first operation of the first round, the first row of the relevant quarters in matrix R is shifted up a1,1 times.

The second operation of the first round is L. Given a1,3 uses eq. 5 too, the first column is shifted left a1,3 times.

The third and fourth operations (D and R) use eq. 6 to determine which row and column to shift (since n = 1, therefore, 2n = 2). Thus, the second row is shifted down a1,2 units, and the second column is shifted right a1,4 units.

In the second round, eq. 5 shows that the third row and the third column should be shifted up by a1,1 and left by a1,3 units respectively.

As for the down and right shift operations, the fourth (since n = 1, therefore, 2n = 4) row and column are shifted a1,2 and a1,4 units respectively.

This process is repeated and once n > 8, the second row in matrix A is considered in the updated version of matrix R.

Once all the rows of matrix A have been considered, matrices A and N are used to generate the key.

4) Generation The Key:

In order to generate the key, the entries of matrix A are used as pointers in matrix N. In other words, taking the value of the entry a1,1, which refers to p1 as an example, the a1,1 value in matrix N is retrieved and kept as the first byte of the key, k. Other entries of matrix A are considered in turn and each fetch a value from matrix N that is then added to k. This process, which leads to having a 64 byte key, is repeated until all the pointers in matrix A have been considered.

Algorithm 1 gives a high-level description of the process:

Algorithm: High Level Description

1: Generate 16 X 16 random matrix, R
2: Generate 16 X 4 random matrix, A
3: Use matrices R and A to generate matrix N
4: Use matrices A and N to generate a 64 byte key, k

4. EXAMPLE :

1) ***If the numbers that are used*** to shift are as in the table below, they will be converted to binary as in the example below:

Table 1: The process of converting key decimal digits to binary digits.

Cell number	8	145	22	200	119	90	4	233
Value holder	112	42	22	191	100	124	186	107
DEC2BIN	1110000	101010	10110	10111111	1100100	1111100	10111010	1101011
Cell number	130	170	3	20	49	209	88	51
Value holder	160	184	177	128	152	78	94	206
DEC2BIN	10100000	10111000	10110001	10000000	10011000	1001110	1011110	11001110

2) Now the binary digits below present the first 16 bytes of the key in the first round, and as mentioned above, the rest of the keys can be identified from the rest of rounds. As suggested, the first quarter of the key is shown as follows

```
11100001010100010110000101111111100100011
11100010111010110101101010000010111000101
1000110000000  10011000  10011100  1011110
011001110
```

3) Then, the generated key above will be XOR-ed with the plain text (original message) : the below snapshot is a suggested plain text that worth 16 bytes size.

```
10101000101100001010001011100110100101111
00010111000000010111010100001001101000011
```

```
00011011100100100100111010000010011001111
00000
```

4) The encrypted message will be the result of the XOR-ed plain text and the generated key: the snapshot below is a suggested plain text that has a size of 16 bytes.

```
11100001010100010110000101111111100100011
11100010111010110101101010000010111000 1
01100011000000010011000  10011100  1011110
011001110
```

5) The diagram of the sugested algorithm:

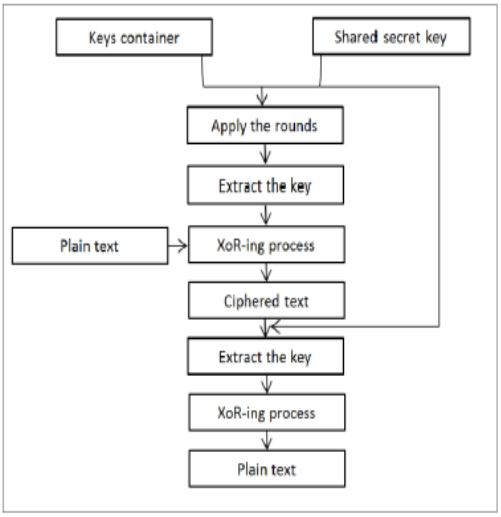

Figure 3: algorithm process.

5. IMPLEMENTATIONAND ANALYSIS:

As mentioned earlier in this paper, the aim is to design a symmetric block cipher cryptography that requires less time compared to others. The key size is 64-bytes, and the system is implemented by NetBeans IDE 8. The system provides the information about the number of blocks that are encrypted by the system. Always, the data block size is equal to the key length so the data block size is 512-bits. The time required is compared to the common algorithm, that is, AES, and the same files are tested in both systems. The important thing that must be considered to reduce the time is to use small numbers in the shifting process. A 1588 block size is tested and the result was as follows:

Table 2: Compression in ms between AES and the suggested algorithm.

Algorithm	Encryption time in ms	Decryption time in ms	Total
AES	718	212	930
The suggested algorithm	306	16	321

From the above result, it is clear that the suggested algorithm is around twice as fast compared to AES and that round of techniques in AES difficult and complicated compared to the suggested algorithm.

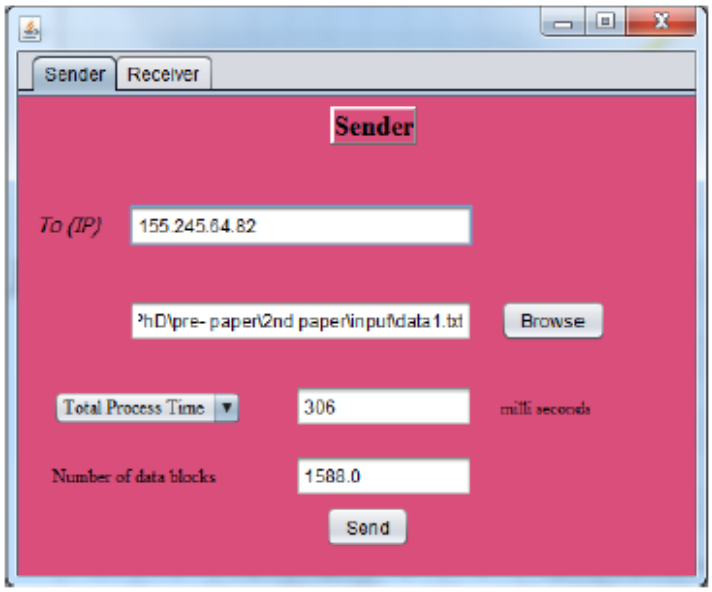

Figure 4: Encryption interface in sender side.

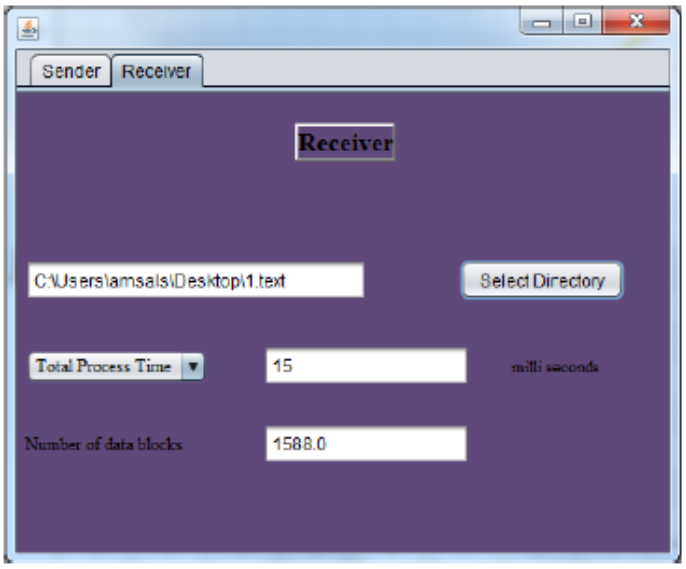

Figure 5: Decryption interface in receiver side.

CONCLUSION

This paper implemented a novel and complicated algorithm that can be used for security purposes. The suggested system is compared to AES. Firstly, the key size in the suggested algorithm is longer than the AES key. There are 16 rounds in the suggested system, but they are working in a complicated mechanism whereas the 14 rounds in AES have 256 bits. Referring to the suggested algorithm features, the algorithm is faster than the AES algorithm.

FUTUREWORK:

Implement a new algorithm with different techniques by using some of concept that used in this paper.

ACKNOWLEDGEMENTS:

I would like to express my very great appreciation to Prof. Walker for his advice and completely supporting during this paper.

REFERENCES:

[1] Stinson," Cryptography Theory and Practice", CRC Press Inc., NY, USA, 1995.
[2] E. Cole, R. Krutz and J. W. Conley," Network Security Bible", Wiley Publishing Inc, 2005.
[3] Elbayoumy, A.D. ; Sch. of Eng. Design & Technol., Bradford Univ, "QoS control using an end-point CPU capability detector in a secure VoIP system", 10th IEEE Symposium on Computers and Communications (ISCC 2005).
[4] Alexander, A.L. ;Wijesinha, A.L. ; Karne, R., "An Evaluation of Secure Real-time Transport Protocol (SRTP) Performance for VoIP" Third International Conference on Network and System Security, 978-0-7695-3838-9/09 $26.00 © 2009 IEEE.
[5] P. Zimmerman, " An Introduction to Cryptography", Doubleday & Company, Inc., United State of America, USA, 1999 .
[6] Computational Aspects of Social Networks (CASoN), 2012 Fourth International Conference, PP. 175-180, 978-1-4673-4794-5/12/$31.00_c 2012 IEEE.
[7] J. Evans, and C. Filsfils, Deploying IP and MPLS QoS for Multiservice Networks: Theory and Practice. Francisco: Morgan Kaufmann, 2007.
[8] S. P. Mehta, "Comparative Study of Techniques to minimize packet loss in VoIP," 2005.
[9] R. Dimova, G. Georgiev, and Z. Stanchev, "Performance Analysis of QoS Parameters for Voice over IP Applications in a LAN Segment," International Scientific Conference Computer Science, 2008.
[10] Katz, Jonathan and Yehuda Lindell (2007).'Introduction to Modern Cryptography'.
[11] Stallings, William; "Cryptography and Network Security Principles and Practices"; Fourth Edition; Pearson Education; Prentice Hall; 2009.
[12] Stallings, W;"Cryptography and Network Security", Prentice Hall, 4th Edition, 2005.
[13] HristofPaar, Jan Pelzl, "Stream Ciphers", Chapter 2 of "Understanding Cryptography, A Textbook for Students and Practitioners", 2009.
[14] Knudsen, Lars R., The Block Cipher Companion. Springer.ISBN 9783642173417, (2011).

Authors:

Ali Alshahrani was born in Saudi Arabia in 1982. He received his M.Sc. from University of Essex in 2011. He is currently PhD student at Essex University, UK, Colchester. His research interests include Network Security, Image Processing, Mobile Payment and e-learning.

Prof. Stuart D.Walker was born in Dover, U.K., in 1952.He received the B.Sc. (Hons) degree in physics from Manchester University, Manchester, U.K., in 1973, and the M.Sc. degree in telecommunications systems and the Ph.D. degree in electronics from Essex University, Essex, U.K., in 1975 and 1981, respectively. After a period of postdoctoral work at Essex University, he joined the then British Telecom (BTPlc) Research Laboratories, Martlesham Heath, Ipswich,

U.K., in 1982. Initially, he was concerned with regenerator design issues in submarine optical transmission systems. While at BT Plc, he was jointly responsible (with Prof. P. Cochrane) for pioneering the unrepeatered-transmission-system concept. In 1987, he was promoted to head the transatlantic link-repeater group, where he supervised the design and fabrication of high-reliability integrated circuits. In 1988, he became a Senior Lecturer at Essex University. There, his research interests included fiber-polarization studies and novel optoelectronic-device configurations. He then developed an interest in access-network design and construction, where he formed a specialist research group. In 2003, he was promoted to Reader and to Full Professor in 2004. He has published over 150 journal and conference papers and has 6 patents granted.