FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645-2944
Vol. 2 No.3, September, 2018, pp. 41-45

AN ENHANCED SYMMETRIC KEY ALGORITHM FOR SECURED NETWORK COMMUNICATION

[1]Olanrewaju, O.M. [2]Adebayo, I.O. [*1]Adebiyi, F.O.

[1]Department of Computer Science and Information Technology, Federal university Dutsinma, Katsina State, Nigeria
[2]Centre for Mobile e-Services, Computer Science Department, University of Zululand, South Africa

*Corresponding author: fadebiyi@fudutsinma.edu.ng

ABSTRACT
Sending secured messages over the internet is a challenging task for today's network users as malicious users are increasing rapidly thereby making internet security a continuous research area. It also makes it necessary to develop a coding scheme that will enable users communicate in a more secured manner. This paper presents a review of four common symmetric key algorithms namely: Data Encryption Standard, Advanced Encryption Standard, Blowfish and RC4. The review was based on three different parameters which are key size, algorithm strengths and type of attacks related to each algorithm. The paper then proposed an enhanced symmetric key algorithm and implemented same using JAVA. The major feat of the proposed algorithm is that the generated key changes after every operation thereby providing a more secured key across the network.

Keywords: *Algorithm, Encryption key, Attack, Symmetric*

INTRODUCTION

Cryptography is the science of using algorithms to encrypt and decrypt data. It enables users on a network to both store and transmit sensitive information across the network in a secured manner (Ayushi, 2010). Cryptography as a branch of network control and security has its roots in information theory, computer security and engineering. Its applications are present but not limited to password generation, electronic commerce and security of smart cards. According to Ayushi, 2010, there are three basic goals cryptographic algorithms seek to achieve. These are explained as follows:

a) Confidentiality

Confidentiality is the process of ensuring that a transmitted message is received and accessed only by the intended recipient (Kaur & Kaur, 2017). One way confidentiality is achieved is through encryption. A message in its original form is known as plaintext while an encrypted text is known as cipher text. Plaintext is usually converted to cipher text using an encryption key.

b) Integrity

Integrity is the process of ensuring that a message sent remains intact without any modification (Ayushi, 2010). One way of achieving data integrity is by providing message authentication codes or hashes. This hashes are usually a fixed sized length of numeric values generated from a sequence of data transmitted via an unsecured medium.

c) Authentication

Authentication is the process of verifying that a message originates from a particular source (Kaur & Kaur, 2017). One way of achieving data authentication is through the use of digital signatures. These signatures are usually attached to hash values so the receiving party can verify the authenticity of its origin.

This paper presents a review of four commonly used symmetric key algorithms. Key criteria for selection of algorithms were highlighted, an enhanced symmetric key algorithm was proposed which was also implemented. The sample plaintext and resultant cipher text were presented. The rest of the article was organised as follows: Section 2 presents a review of symmetric key algorithms, Section 3 presents the proposed enhanced symmetric algorithm based on Cipher Block Chaining mode operation. Implementation of the proposed algorithm and result discussion is presented in Section 4 while the conclusion is drawn in Section 5.

CRYPTOGRAPHIC ALGORITHMS

Cryptographic systems can be classified into two broad groups, asymmetric and symmetric key algorithms. Asymmetric key algorithms consist of two keys, a public and private key for encryption and decryption. The public key as the name suggests is known to everyone on the network while the private key is only known by the receiver to decrypt the message on receipt. Some of the commonly used asymmetric algorithms are Diffie-Hellman, Digital Signature, ElGamal algorithms among others (Arya, Aswal, & Kumar, 2015).

Symmetric key algorithms use a single key to both encrypt and decrypt text in transmission. Being easy to understand and use, they are the most commonly used algorithms for encryption (Ayushi, 2010). Over the years, the number and application of symmetric key algorithms on the market has increased. In order to determine the best algorithm for a particular application, it then becomes necessary to evaluate all related algorithms in line with the design objectives of the said application.

Each symmetric key algorithm has its strengths and limitations when applied in varying conditions using different parameters. The parameters may include Architecture, Limitation, Flexibility, Security and Scalability (in terms of Encryption rate, Memory Usage, Software/hardware performances and

computational time).

Cryptographic algorithms are generally grouped as either stream or block ciphers. Stream ciphers are applied on a steady stream of bits or bytes and systematically encrypts each until the given text is completely encrypted. On the other hand, block ciphers operate on a predetermined block size of text. In an event where the text given does not always fit into that specified block size, it is padded with zeros to make up the block. It is because of this complexity that block ciphers are preferred over stream ciphers for most encryptions (Masram, Shahare, Abraham, & Moona, 2014).

Symmetric Key Algorithms and the Evaluation Metrics

Symmetric key ciphers are usually designed to accommodate high rates of data throughput depending on the implementation, either hardware or software. They can also be used as constructs for other cryptographic mechanisms like hash key functions, pseudorandom number generators, and digital signature keys among others (Yadav, 2010). The following criteria are key in analysing symmetric key algorithms for use:

a) Security: One of the most desirable characteristics of a cryptographic algorithm is its security. An affirmative measure of the system strength in resisting an attack is a desirable element of any encryption algorithm. It should possess the property of indistinguishability (built by combining substitution with transposition repeatedly). Security of an encryption algorithm depends on the key size (which is measured in bits) used to execute the encryption; generally, the greater the key's size, the stronger the encryption (Ayushi, 2010).

b) Architecture: Defines the structure and operations that an algorithm can perform, its characteristics and how they are implemented (Ebrahim, Khan, & Khalid, 2013). It also determines that the algorithm is symmetric or asymmetric, that is whether it makes use of secret key or public key for encryption and decryption.

c) Flexibility: Defines whether the algorithm is able to endure modifications or adoption according to the requirements. The more flexible an algorithm is, the more desirable it becomes for several applications.

d) Scalability: It is one of the major element on which encryption algorithms can be analysed. Scalability depends on certain parameters such as Memory usage, Encryption rate, Software/hardware performance and Computational efficiency (Ebrahim, Khan, & Khalid, 2013).

e) Limitations (Known Attacks): Defines how many of the known attack can the algorithm works for by making use of the computer resources available to it. Further how often it is vulnerable to different types of attacks (Ebrahim, Khan, & Khalid, 2013).

Categories of Symmetric Algorithms

Symmetric algorithms are popular because their speed enables them efficiently to encrypt large quantities of plaintext. There are two subcategories of symmetric cipher, stream and block flexibility both for software and hardware. It is a compact cipher, is time effective and provides enough resistance against cryptanalytic attacks.

AES can be well adapted to a wide range of modern processors such as Pentium, Reduced Instruction Set Computer (RISC) and parallel processors. In general, AES is also known as 16 rounds. In each of the rounds, starts with byte substitution where each 8-bit byte is reversibly mapped onto another byte after which the rows of bytes are shifted over four other offsets. After this, the bytes in the different columns are combined linearly then the sub-key is XORed. The same algorithm can be used in reverse for decryption. Though highly efficient and widely used, this process makes it possible to learn the corresponding plaintext value for every special character encrypted over time. This

ciphers.

a) Stream Ciphers

These algorithms operate upon one bit at a time. A stream of plaintext flows into the cipher and a stream of Ciphertext emerges as the output. Messages encrypted with a stream cipher are always the same size as the original plaintext. The encryption takes place by means of an operation in which each bit of the plaintext is XORed (i.e. manipulated by the Boolean operator exclusive OR – XOR) with a random bit to produce the Ciphertext (Saranya, Mohanapriya, & Udhayan, 2014). The essence of a stream cipher concerns the methods by which the shared key is used to generate the stream of random bits. Cracking attempts centre on analysing this random bit generator.

b) Block Ciphers

These ciphers encrypt data in blocks of bytes, rather than a single bit at a time. Block sizes vary according to the algorithm, 64 bits being the most common. Because the plaintext is unlikely to be a multiple of the algorithm's block size, it is often necessary to pad the input (Saranya, Mohanapriya, & Udhayan, 2014). For example, if the block length is 64 bits and the last block contains only 40 bits then 24 bits of padding must be added. The padding string can consist of all zeros, alternating zeros and ones, random bits, or some other sequence. Some encryption standards specify a particular padding scheme. DES (Data Encryption Standard), Blowfish and AES (Advanced Encryption Standard) are block ciphers.

Review of Specific Symmetric Algorithm

a) Data Encryption Standard (DES)

Data Encryption Standard is a 64-bit block cipher, designed by IBM based on the Fesitel Block Cipher. It was the first encryption standard to be published by NIST (National Institute of Standards and Technology). The DES uses a 56-bit key but is padded so that it becomes a 64-bit key. It was initially considered as a strong algorithm, but with the growth and advancement in Technology, the large size of data and short key length of DES limits its use (Ebrahim, Khan, & Khalid, 2013).

b) Blowfish

Blowfish is a public domain algorithm designed by Bruce Schneier, author of Applied Cryptography. It is highly rated as an encryption algorithm with a lot of focus on security. Blowfish is fast, compact, and a simple block encryption algorithm with variable length key allowing a trade-off between speed and security (Ebrahim, Khan, & Khalid, 2013). Blowfish has however been discovered to have weak keys and are vulnerable to second order differential attacks.

c) AES (Rijndael)

Rijndael was developed by Joan Daemen and Vincent Rijmen. It became U.S.'s new Advanced Encryption Standard in October 2000 declared by the National Institute of Standards and Technology as it stood out from other algorithms presented (Merrion, 2000). Rijndael makes use of variable key size and allows implementers enough

makes AES vulnerable to known plaintext and side channel attacks (Saranya, Mohanapriya, & Udhayan, 2014).

d) RC4

RC4 also known as ARCFOUR or ARC4 which means Alleged RC4 is most commonly used stream symmetric cipher which uses several security protocols. Based on random permutations, the key stream is entirely independent of the plaintext. It uses a variable length key from 1 to 256 bytes to create a 256-byte array. The array is used for generation of pseudo-random bytes and then a pseudorandom stream, which is XORed with the plaintext/ciphertext to give the ciphertext/plaintext (Pehlivanoğlu & Duru, 2015).

The algorithm involves two steps, key setup and ciphering which must be carried out for every new key being used. It has the ability to handle large amounts of data without compromising speed of encryption and decryption. Over time, a lot of attacks have been launched against RC4 successfully based on weak keys, weakness in initialization among others so much that RC4 is now generally considered an insecure algorithm (Dawson, Gustafson, Henrickson, & Millan, 2002). The summary of the symmetric algorithms are shown in Table 1.

Table 1: Summary of Symmetric Algorithms

S/No	Symmetric Key and Size	Designers	Year of Publication	Cipher Type	Strengths	Weaknesses
1	DES (56 bits)	IBM	1977	Block	First encryption standard published	Susceptible to Brute force attack
2	AES (128,192,256) bits	Vincent Rijmen, Joan Daemen	1998	Block	Fast, flexible and suitable for mobile devices	Susceptible to algebraic attack and key related attacks
3	Blowfish (32-448) bits	Bruce Schneider	1993	Block	Fastest block cipher, Unpatented and available for all users	Suffers from weak key problems
4	RC 4 (1-256) bytes	Zon Rivest	1987	Stream	Efficient, simply and widely used for secured web communications.	Vulnerable when individual key stream is repeated.

PROPOSED ENHANCED SYMMETRIC KEY ALGORITHM

The proposed enhanced symmetric key algorithm is based on Cipher Block Chaining mode operation. Instead of the encryption key with an 8-bit binary number in the top register as in Cipher Block Chaining, the proposed algorithm generates a 24-bit meaningless encryption key string once a message is received. The encryption key is uniquely generated each time a plain text is received. The procedure is depicted as follows in Figure 1.

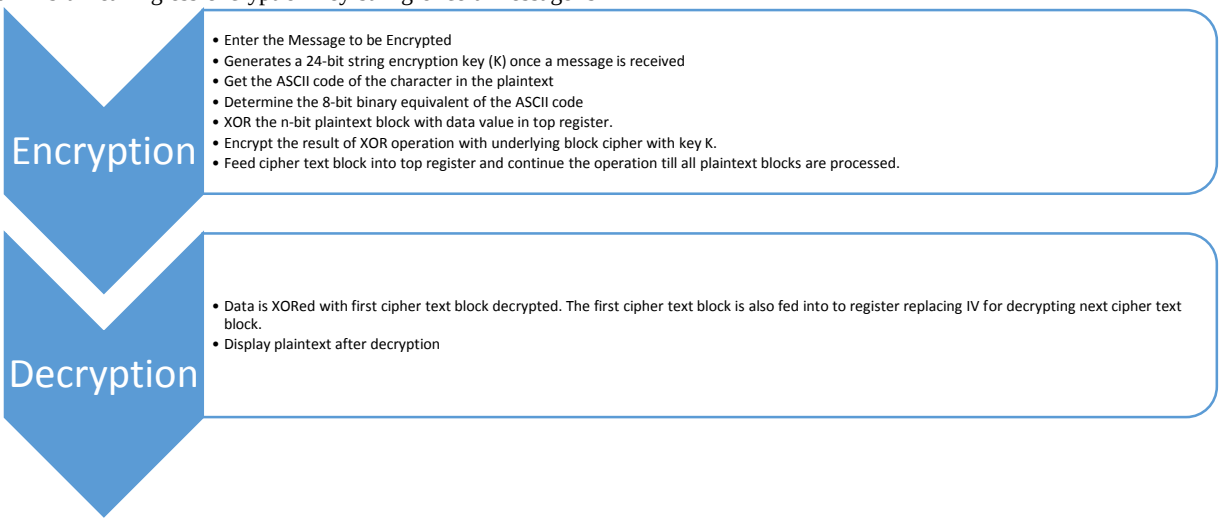

Figure 1: Procedural Flow Structure

EVALUATION AND RESULT DISCUSSION

The coding of the Algorithm was done using Java programming language. Sample text messages were used for encryption and decryption to test the effectiveness of the algorithm proposed.

Evaluation with Sample Texts

The code implementation of the algorithm was tested with the same sample text three times. Figure 2 to figure 4 reveals that the same text yielded different keys and different encrypted text First operation

```
Enter the message to be encrypted: Hello World!
Secret Key: Ju4Qywye7W8YhNN6QWI3fril
Encrypted message: ÝðùùúµÂúçùñ´
Enter the Secret Key to decrypt the message:
Ju4Qywye7W8YhNN6QWI3fril
Decrypted message: Hello World!
```

Figure 3: Second Sample plain text Encrypted and Decrypted

Second operation

```
Enter the message to be encrypted: Hello World!
Secret Key: ShYQXXSI2FDZv84abG0XePrh
Encrypted message: ïÂËËÈ?ðÈÕËÃ?
Enter the Secret Key to decrypt the message:
ShYQXXSI2FDZv84abG0XePrh
Decrypted message: Hello World
```

Figure 4: Third Sample plain text encrypted and decrypted

Third operation

```
Enter the message to be encrypted: Hello World!
Secret Key: eH7WdNjADe8BrIesKDibhEb3
Encrypted message: ?®§§¤ë?¤¹§¯ê
Enter the Secret Key to decrypt the message:
eH7WdNjADe8BrIesKDibhEb3
Decrypted message: Hello World!
```

Discussion

The symmetric algorithm implemented in this paper is scalable in nature and will work for an unlimited amount of plain text. It also generates a 24-bit long string which changes after every operation. The key the recipient used earlier cannot be used to decrypt the same message if it happens to be sent the second time. This makes it more secured than the traditional Cipher Based Mode algorithm that requires the user to generate an 8-bit binary number before the plaintext is encrypted. This is the major strength of this algorithm.

each time it is used. This will definitely make the recipient to depend on the sender key each time even when the message sent is the same.

CONCLUSION

The encrypted text is a mixture of several unreadable characters making it difficult for anyone to cipher at first glance. This will certainly keep the message secret and meaningless to others. In this paper, four symmetric algorithms were reviewed and an enhanced symmetric algorithm is proposed which uses a single key for both encryption and decryption. The key length is a fixed 24-bit sized algorithm which changes every time the encryption is done. Hence achieving the tripod goals of confidentiality, integrity and authenticity which is required for sending and receiving messages securely across networks.

REFERENCES

Arya, P. K., Aswal, M. S., & Kumar, V. (2015). Comparative Study of Asymmetric Key Cryptographic Algorithms. *International Journal of Computer Science & Communication Networks*, 17-21.

Ayushi. (2010). A Symmetric Key Cryptographic Algorithm. *International Journal of Computer Applications, 1*(15), 1-4.

Basagni, S., & Lee, S. (2002). Mobile Ad Hoc Networking Research, Trends and Applications. *Wireless Communications and Mobile Computing*.

Bhalla, S., Monga, K. S., & Malhotra, R. (2012). Optimization Of Computer Networks Using Qos . *International Journal Of Engineering Research And Applications (IJERA) 2(3). ISSN: 2248-9622*.

Cisco IOS Release. (2009). Quality of Service Solutions Configuration Guide Congestion Management Overview. Cisco Systems.

Dawson, E., Gustafson, H., Henrickson, M., & Millan, B. (2002). *Evaluation of RC4 Stream Cipher*. Information Security Research Centre. Queensland University of Technology .

Ebrahim, M., Khan, S., & Khalid, U. B. (2013). Symmetric Algorithm Survey: A Comparative Analysis. *International Journal of Computer Applications; ISSN: 0975 8887, 61*(20), 12-19.

Jasmeet, S., & Singh, V. (2009). Quality of Service in Wireless LAN Using OPNET Modeller.

Kebande, V. R. (2013). Routing and Reducing Perturbation in Mobile ad Hoc Networks (Manets) for Efficient Communication. *International Journal of Advanced*

Computer Research 4(4):, 195-199.

Manoj, K., Parmanand, S., & Singh, S. (2009). Performance of QoS Parameter in Wireless Ad hoc Network (IEEE 802.11b). *Proceedings of the World Congress on Engineering and Computer Science.*

Masram, R., Shahare, V., Abraham, J., & Moona, R. (2014). Analysis and Comparison of Symmetric Key Cryptographic Algorithms based on Various File Features. *International Journal of Network Security & Its Applications, 6*(4), 43-52.

Merrion, S. (2000). Rijndael – The Future of Enc ryption. *Global Information Assurance Certification Paper*.

Pehlivanoğlu, M. K., & Duru, N. (2015). Email Encryption using RC4 Algorithm. *International Journal of Computer Applications Vol 130 Issue 13*, 25-29.

Saranya, K., Mohanapriya, R., & Udhayan, J. (2014). A Review on Symmetric Key Encryption Techniques in Cryptography. *International Journal ofScience, Engineering and Technology Research, 3*(3), 539-544.

Sobrinho, J., & Krishnakumar, A. (1999). Quality-of-Service in Ad Hoc Carrier Sense Multiple Access Wireless Networks. *IEEE Journal on Selected Areas in Communications, 17(8)*, (pp. 1353-1368).

Yadav, S. K. (2010). Some Problems in Symmetric and Assymetric Cryptography. *PhD Thesis, Department of Mathermatics; Dr. B. R. Ambedkar University, Agra*.