ADVANCED SYMMETRIC KEY CRYPTOGRAPHY ALGORITHM FOR INFORMATION SECURITY

Sameera Shaik[1], Sharma S[2], Vishnu S[3], Srilakshmi U[4]

[1]Dept of Computer Science, VFSTR University, [2]School of Electronics, VFSTR University, [3]School of Electronics, VFSTR University, [4]Dept of Computer Science, VFSTR University, India. E. mail: {sks_cse harma_ece Vishnu_ece,sri_cse}@vignanuniversity.org

ABSTRACT

Information is one such thing, which has become crucial weapon in the race towards the pinnacle of development and evolution. To protect this information from unauthorized access and/or damage or misuse, the concept of information security has been emerged. When the information is transferred from sender to receiver over a network, a hacker can break and expose the actual message that is confidential. To achieve all these things, several cryptographic techniques are generated. A cryptographic technique converts the confidential information into a form, which can't be understood by a hacker or unintended individuals, which is known as encryption technique and it makes use of a particular algorithm to encrypt the message. The encrypted message is decrypted in the receiver side by using respective decryption algorithm. In this paper, a new algorithm has been proposed and compared with existing ones in terms of encryption algorithm, throughput of key generation and decryption algorithm.

Index Terms— Information, confidentiality, encryption, decryption, key generation

1. INTRODUCTION

When the information is transferred from sender, the intended receiver of the message should obtain the information that maintains its confidentiality, availability, integrity and authenticity.

- Confidentiality-information should not be accessible by unauthorized users
- Availability– information should be available for intended receiver
- Integrity–information should not be altered by attacker while transmission
- Authenticity–only authorized users can access the information

Privacy and security issues of the transmitted data have become an important concern in multimedia applications. The security of information and protection ability is vital role to the growth of Internet and to the growth of e-commerce. How to protect privileged sensitive information from being stolen? The answer was cryptography. Cryptography is the study of hiding information by converting the plain text (or sensitive information) into a cipher text (or unintelligible text), so that it cannot be understood by a hacker or unintended individual and then converting it back to its original form, by using able encrypting and decrypting algorithms [3]. Robustness, memory usage, security, non-repudiation and design etc. are the para-meters considered while adopting cryptographic technique.

Key is needed to perform these algorithms on plain text and cipher text. Therefore, cryptography has three steps– Key generation, encryption process and decryption process. Key based cryptographic methods are mainly classified into two types: Symmetric and asymmetric. Same key is used for both the encryption and decryption processes in case of Symmetric key cryptography whereas separate keys are used in Asymmetric Key cryptography. Symmetric key cryptography further divided into two: Steam ciphers and block ciphers. Steam ciphers take the input in byte-by-byte fashion whereas block ciphers take the input as a group of fixed size block. Steam ciphers are smaller in hardware and faster in software.

The paper is divided as follows: Section 2 describes the various cryptographic schemes whereas section 3 discusses about the proposed approach. In section 4, the proposed approach performance is compared with the existing ones. Section 5 describes the conclusion.

I. LITERATURE SURVEY

Cryptography has this much importance in real world because all the sectors need secure data transmission [1]. With a variety features, there exist wide variety of cryptographic schemes like symmetric key cryptography, DNA cryptography, Quantum cryptography, Multivariate cryptography etc. Among which blowfish, AES, DES and 3DES algorithms are very popular. Substitution, bitwise XOR, shifting and many more operations are performed in all these algorithms [5].

Symmetric key cryptography is of two types: Steam cipher and block cipher. Steam ciphers are very simple with less complexity when compared with block ciphers and both of these come under symmetric cryptography. Steam ciphers are used in applications where the large amount of data is to be processed with high throughput. Vernam-cipher is a symmetric steam cipher in which plain text is combined with pseudorandom key to form cipher text.

Book cipher is a very popular cryptographic algorithm in which a book or a part of book is considered as symmetric key [1]. It converts the plain text into cipher text by replacing the word in the plain text with the position of that word in the symmetric key (book). If the book 'Bible' is used as symmetric key then it is known as 'Bible cipher'. What if the book doesn't contain the word which is to be encrypted? This is the main disadvantage of Book cipher and in most of the cases it can be overcome by making use of dictionary.

Advanced Encryption Standard (AES) algorithm makes use of 128 bits block size with 128, 192 or 256

bits of key size. Here number of cycles is the key variant. It can be easily unlocked by applying brute force attack [7]. Data Encryption Standard (DES) algorithm has 64 bits block size with 54 bits of key size and the small size of key is the disadvantage of this algorithm [13]. 3DES comes into picture, which is similar to DES, but the encryption level is increased by 3 times, which in turn increases the time complexity and decreases the performance of the algorithm [7]. Blowfish is one of the best algorithms that has variable key lengths with 64 bits block size.

In One Time Pad (OTP), a onetime pad is used which is generated randomly in which random groups are present in every time pad. Each time pad is exactly is used once and key size is fixed [1]. The main difference between Vernam-cipher and OTP is that later possesses true randomness whereas former repeats after a period of times.

The following are the issues found during the study of all algorithms [13].

- The shorter the length of key lacks the high security compare to longer length of key and decreases the speed of algorithm execution.
- Complex structure of algorithm increases the execution time. Therefore, the structure of algorithm has to be simple and less complex in order to make algorithm run faster.
- Mathematical or logical operations performed on plain text, key and cipher text decide the overall performance of any algorithm.

All these issues are taken into consideration in the proposed algorithm to improve the performance.

II. PROPOSED ALGORITHM

This algorithm, block size and key size both are equal (128 bits). Simple logical and arithmetical operations like logical XOR and shifting are used. Few steps in this algorithm are repeated n times where n is not fixed so that attackers cannot hack it easily which in turn increases the security when compared with existing algorithms. Following are the steps for encryption and decryption techniques

A. Encryption

a. Enter the plain text and convert 16 characters of plain text into binary format. Therefore, length of plain text is 128 bits (8 bits per character).
b. Divide the obtained binary text into two parts (each of size 64 bits) and arrange them in reverse order.
c. Combine both the parts and apply XOR operation with the given key of size 128 bit.
d. For second round, perform circular left shift operation on key.
e. Divide result of size 128 bits into 16 parts each of size 8 bit then divide each of 8 bit into two parts each of size 4 bit.
f. Collect all the right 4bit parts and left 4bit parts into two 64-64 bits separately.
g. Now perform XOR operation on left 64 bits and right 64 bits and store the result in left 64 bits. Keep the right part as it is(no change).
h. Combine both parts and resultant is of size 128 bits.(repeat steps 3 to 7 for n times)
i. Divide the resultant into 16 parts each of size 8 bits.
j. Divide each of 8 bits into two parts each of size 2 bits and 6 bits. Perform circular left shift operation on all 6 bits.
k. Combine all these parts and obtain cipher text of size 128 bits (16 characters).

B. Decryption

a. Convert 16 characters of cipher text into binary format of size 128 bits(8 bits per each character) and divide obtained 128 bits into 16 parts each part of size 8 bits.
b. Divide each of 8 bits into two parts each of size 2 bits and 6 bits. Perform circular right shift operation on all 6 bits and combine all parts to get 128 bits.
c. Divide obtained 128 bits into two parts each of size 64 bits.
d. Perform logical XOR operation on left and right part. Store the result in left part and keep the right part as it is.
e. Divide 128 bits into 16 parts each of size 8 bits then divide each of 8 bits into parts each of size 4 bits.
f. Collect all the left 4 bits into one part and all the right 4 bits into another part and combine these two parts to get 128 bits format.
g. Perform logical XOR operation on 128 bits with the key of size 128 bits and perform circular right shift operation on key for second round. (Repeat steps 4 to 7 for n times)
h. Divide 128 bits into two parts each of size 64 bit. Arrange them in reverse order and combine both the parts and get the plain text of size 128 bits (16 characters).

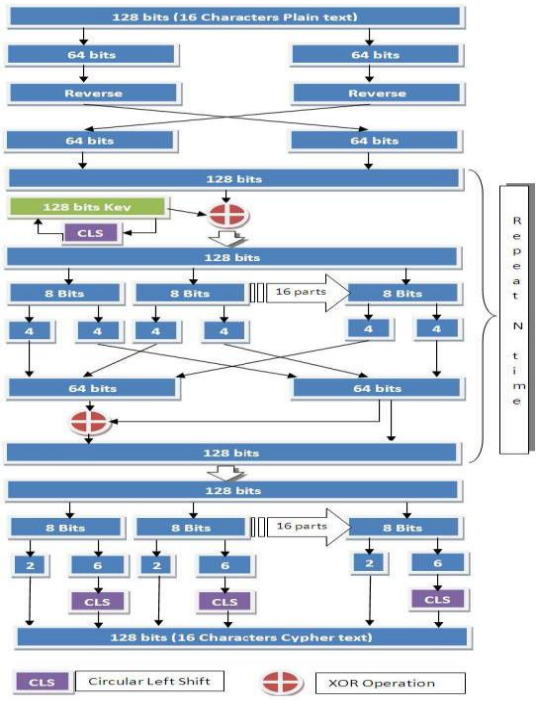
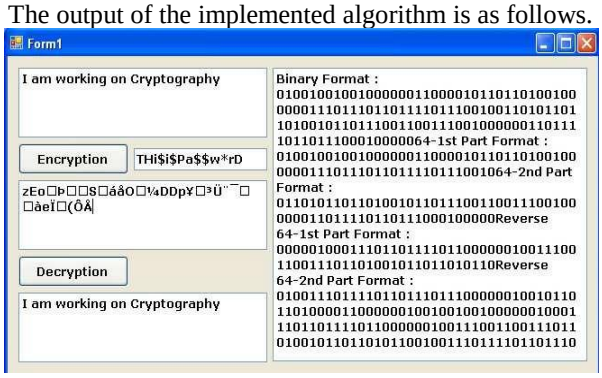


Fig1. Proposed Algorithm

The output of the implemented algorithm is as follows.



If the attacker tries to hack the algorithm using brute force attack, as the length of the key is 128bit, it takes 2.5×10 years to hack which is not possible.

Process of Algorithm	Compared with Other Algorithms				
	AES	*DES*	*Triple DES*	*Blowfish*	*My Algo.*
	Throughput 100KB				
Key Generation	0.31	0.33	0.33	0.34	0.2
Encryption	0.34	0.35	0.36	0.32	0.33
Decryption	0.34	0.35	0.36	0.32	0.33
	Throughput 1MB				
Key Generation	0.31	0.33	0.33	0.34	0.2
Encryption	0.41	0.45	0.65	0.39	0.4
Decryption	0.42	0.45	0.65	0.39	0.4
	Throughput 10MB				
Key Generation	0.25	0.25	0.25	0.25	0.2
Encryption	1.2	1.5	3.25	1.1	1.1
Decryption	1.2	1.5	3.25	1.1	1.1

Fig 3. Result analysis

III. RESULT ANALYSIS

As discussed earlier, cryptography is a 3-step process: key generation, encryption and decryption. All these 3 steps are considered to analyze the performance of proposed algorithm compared with existing ones. The algorithm is tested on system having P4 processor with 1 GB RAM. Fig. 3 shows the throughput of 100KB, 1 MB and 10 MB. From the following figure, it can be observed that the proposed algorithm is giving faster results when compared with the existing ones.

CONCLUSION

Proposed algorithm is showing best performance when compared with the algorithms, ensuring high security and privacy. As the performed logical and arithmetical operations are very simple, it has less complexity. High security is achieved as the length of the key used is very high (128 bit). For the future work, simpler logical and arithmetical operations will be added to the algorithm in order to achieve even more throughput.

REFERENCES

[1] Aswin Achuthshankar, Aswathy Achuthshankar, A Nov-el Symmetric Cryptography Algorithm for Fast and Secure Encryption. J. Clerk Max - well, A Treatise on Electricity and Magnetism, 3rd ed. Oxford: Clarendon vol. 2 Pp.68–73 (1982).

[2] What is Symmetric-Key Cryptography? Webopedia http://www.webopedia.com/TERM/S/symmetric_key_cryptogra phy.html K. Elissa, Title of paper if known, unpublished.

[3] Abhishek Anand, Abhishek raj, Rashikohli, Proposed Symmetric Key Cryptography Algorithm for Data Security.

[4] Brown Lawrie, Steflik Dick, Symmetric Encryption Algorithms, CS- 480b, Lecture slides (ppt.).

[5] Aissa B., Nadir D. and Mohamed. R, Image encryption using stream cipher algorithm with nonlinear filtering function, IEEE Int. Conf. on High Performance Com-puting and Simulation (HPCS), July (2011).

[6] Christian Mainka, Juraj Somorovsky, Jorg Schwenk Penetration Testing Tool for Web Services Security, Honolulu HI, P ublished in Services (SERVICES) Eighth World Congress on IEEE, Pp. 163-170, June 24 (2012) ISBN: 978-1-4673-3053-4

[7] The Cryptography Guide: Triple DES, Cryptography World. Retrieved (2010).

[8] Nikhil Agarwal, Manoj Kumar, Dr. M.A Rizvi, Transposition Cryptography Algorithm using Tree Data Structure.

[9] Mitali, Vijay Kumar, Arvind Sharma, A Survey on Various Cryptography Techniques, IJETTCS 3(4): July-August (2014)

[10] Symmetric-Key Cryptography https://simple. Wikipedia. org/wiki/Symmetric-key_algorithm

[11] Symmetric Key–How Stuff Works http://computer.howstuffworks.com/encryption2.htm

[12] Dudhatra Nilesh, Prof. Malti Nagle, The New Cryptography Algorithm with High Throughput.