

NEW SYMMETRIC KEY CRYPTOGRAPHY ALGORITHM USING SIMPLE LOGARITHM AND BINARY DIGITS

Mohammed AbudallahMd Aysan*

Fareed Hassan Almalki*

Abdullah Mohammed Almalki*

ABSTRACT

Efficient cryptographic algorithms have been used for securing data communication. It is considered as one of the best tools to help people to protect their valuable information from cryptanalysts when it is stored or transmitted via insecure communication channels. Now in the modern world this number of trial runs may not be impossible for the hacker. To get rid of this problem here the authors suggest a new symmetric key algorithm. This paper proposes a symmetric key cryptosystem based on the simple mathematical logarithm function. The proposed system benefits from the algebraic properties of \log_x such as non-commutative, high computational speed and high flexibility in selecting keys which make the Discrete Logarithm Problem. Also the encrypted text converted into binary numbers to make harder to understand by the backer. This method will be suitable in any business house, government sectors, communication network, defense network system, sensor networks etc.

Keywords: Symmetric key, Logarithm, Cryptography, Discrete function etc.,

* Students, Computer Engineering & Networks Department, College of Computer Science & Information system, Jazan University, Jazan, KSA.

INTRODUCTION

Cryptography plays a significant role in hiding the true nature of data; this is achieved by inducing the factor of confusion through a series of shift and other mathematical functions. In the field of cryptography there exist several algorithms for encryption/decryption; these algorithms can be generally classified into two major groups: symmetric-encryption algorithms and asymmetric encryption algorithms [1]. Until the late 1970's, the only cryptosystems for message transmission were symmetric key systems. In symmetric key cryptography, any two users who require communicating a message must have a same key to cipher or decipher the message. In 1976, Diffie and Hellman [2] invented a key-exchange system that was entirely a new type of cryptography.

The cryptography categorized into Symmetric or private and Asymmetric or public keys encryption. In Symmetric keys encryption or secret key encryption, only one key is used to encrypt and decrypt data. In Asymmetric keys, two keys are used; private and public keys. Public key is used for encryption and private key is used for decryption (e.g. RSA). Public key encryption is biased on mathematical function, computationally intensive and is not very efficient for small mobile devices [3].

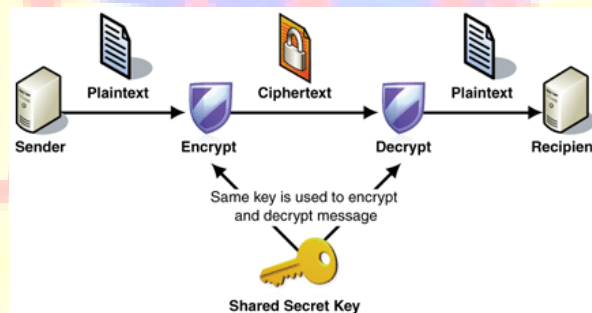


Fig 1. Symmetric key encryption

Symmetric key algorithms are well accepted in the modern communication network. The main advantage of symmetric key cryptography is that the key management is very simple. Only one key is used for both encryption as well as for decryption purpose. There are many methods of implementing symmetric key. In case of symmetric key method, the key should never be

revealed /disclosed to the outside world or to other user and should be kept secure. The key should be known to sender and the receiver only and no one else[4][8].

The structure of the research article as follows. Section II presents the studies of existing symmetric key algorithm models, the proposed structure of new algorithm discussed in section III. In section IV discussed about implementation method with sample text message and section V discussed about result analysis of proposed model. Finally conclusion and acknowledgement offered in section VI and VII respectively.

LITERATURE REVIEW

Jamal N. BaniSalameh(2012) discussed new type of algorithm called MJEA has a 64-bit block size, 8-rounds and 120-bit key. The design philosophy behind the proposed algorithm is simplicity of design which yields an algorithm that is easier to implement and achieves a good Avalanche Effect as quickly as possible. The motivation for this work is to design a novel encryption algorithm that uses good features of JEA encryption algorithm [1].

T.D.B Weerasinghe(2012) in this paper presents an analysis of some of the widely used symmetric key algorithms which fall under the categories of block and stream ciphers together with the two combined algorithms. All the algorithms are implemented in Core Java using classes available in JAVA package javax.crypto. Separate classes are written to calculate the secrecy of ciphers and the encryption time. And also the tool is created using Core Java with the help of Netbeans IDE [5].

RitikaChehal, Kuldeep Singh (2012)in this study, they used the inserting dummy symbols, rotating, transposition, shifting, complement and inserting control byte to build the data and tables in the encryption algorithm. These operations are simple and easily to implement. Without knowing the data and tables of encryption, it is difficult to do cryptanalysis. In the decryption algorithm, they used these data and tables to decrypt cipher text to plaintext. We can easily apply these algorithms to transmit data in network and the data transmission is secure[6].

PrakashKuppuswamy, Dr. Saeed Q Y Al-Khalidi (2012) this research article reflect the importance of security in network and provide the better encryption technique for currently implemented encryption techniques in simple and powerful method. In this research they proposed a modular 37 and select any number and calculate inverse of the selected integer using modular 37. The symmetric key distribution should be done in the secured manner [7].

PROPOSED MODEL

Symmetric key is implemented in two ways either as a block cipher or stream cipher. Block cipher transforms a fixed length block of plaintext say a fixed size of 64 data into a block of ciphertext data of the same length.

Asymmetric on the other hand allow encryption key of data to be made public for anyone intending to encrypt while only the recipient had access to the private key for decryption. Research on cryptographic mechanism had proved that symmetric algorithm is quicker to execute on a computer than asymmetric algorithm because of the use of one key for both operations. However in practice both keys are used together to encrypts and decrypts Computational requirements.

Table1. Synthetic value

1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L
13	14	15	16	17	18	19	20	21	22	23	24
M	N	O	P	Q	R	S	T	U	N	W	X
25	26	27	28	29	30	31	32	33	34	35	36
Y	Z	0	1	2	3	4	5	6	7	8	9

Our, New algorithm need following computational requirement to development of algorithm. First one is Plaintext, It is known as message and synthetic Data. We know that, whatever message or plaintext consist of Alphabets between A to Z and numbers which is between 0-9. Here, In New symmetric key algorithm, we introduce synthetic data, which is

based on the sender's message text. Normally the synthetic data value consists of equivalent value of alphabets and numbers which is mentioned in the table no.1.

3.1 Encryption procedure

- i. Assign synthetic value for message
- ii. Select random symmetric key (logarithm)
- iii. Calculate synthetic value with symmetric key
- iv. Convert into binary digits
- v. Send binary digits and symmetric key to the receiver end.

3.2 Decryption procedure

- i. Convert received message into decimal value.
- ii. Use symmetric key with decimal value
- iii. Now received integer value compare with the synthetic table
- iv. Derived letter is plaintext

IMPLEMENTATION

Here we are using new symmetric encryption approach based on traditional logarithm mathematical function. We have already know that symmetric encryption approach is divide in two type one is block cipher symmetric cryptography technique and another is stream cipher symmetric cryptography but here we are choosing stream cipher type because its efficiency and security. In this proposed technique we have two common key between sender and receiver, which is known as private key based on logarithm. Basically private key concept is the symmetric key concepts where plain text is converting into encrypted text known as cipher text using private key where cipher text decrypted by same private key into plain text. The encryption key is trivially related to the decryption key, in that they may be identical or there is a simple transform to go between the two keys.

In order to provide quick and simple encryption/decryption, We have chosen here sample message combination of alphabets and numbers i.e 'KINGDOM 2014'. Also, we are following

standard text value from the table. The reason for adopting table, all text messages is a combination between A-Z and 0-9. For encrypting small amount of data, there should not be any overhead to the encrypting system as well as there should not be any compromise on the security level.

4.1 Encryption

As per the above algorithm encryption has made and showed in the following table. The text message assigned by the integer value as per the synthetic table and we can choose random Logarithm function and keep the logarithm as a symmetric key. Next, the derived value convert into binary digit and send it to the receiver end it is called cipher text. The advantage of converting binary digit, It is difficult to understand by the hackers and one more important point is easy to send the binary digits to the receiver end.

Table2. Encryption process

Plain Text	Integer Value	$\text{Log}_2(X)$	Cipher text (binary value)
K	11	3.459	11.01110101100000010000011000100100
I	9	3.167	11.00101010110000001000001100010010
N	14	3.807	11.11001110100101111000110101001111
G	7	2.807	10.11001110100101111000110101001111
D	4	2.0	10
O	15	3.907	11.11101000001100010010011011101001
M	13	3.700	11.10110011001100110011001100110011
2	29	4.858	100.11011011101001011110001101010011
0	27	4.755	100.11000001010001111010111000010100
1	28	4.807	100.11001110100101111000110101001111
4	31	4.954	100.11110100001110010101100000010000

4.2 Decryption

The decryption method also very similar to the encryption but it is in reverse angle. After received binary digits and key from the sender, First receiver convert binary into integer values, then the receiver use the symmetric key and convert synthetic integer value. The final integer value compare with the synthetic value known as revealed message or decrypted text.

Table 3. Decryption process

Cipher text (binary value)	$Y=X^a$	Integer Value	Plain Text
11.01110101100000010000011000100100	3.459	11	K
11.00101010110000001000001100010010	3.167	9	I
11.11001110100101111000110101001111	3.807	14	N
10.11001110100101111000110101001111	2.807	7	G
10	2.0	4	D
11.11101000001100010010011011101001	3.907	15	O
11.10110011001100110011001100110011	3.700	13	M
100.11011011101001011110001101010011	4.858	29	2
100.11000001010001111010111000010100	4.755	27	0
100.11001110100101111000110101001111	4.807	28	1
100.11110100001110010101100000010000	4.954	31	4

RESULT ANALYSIS

The evaluation any type of cryptography algorithm with respect to various criteria includes performance, level of security, methods of operation, functionality, ease of implementation. We are using two parameters for encrypting and decrypting the message. Here we analyses proposed new algorithm with existing symmetric cryptographic algorithm.

Table 4. Execution timings

Text size (Kbytes)	AES	DES	RC2	New Algorithm
100	90	49	91	38
300	160	80	165	48
700	207	145	264	98
1000	210	235	290	120

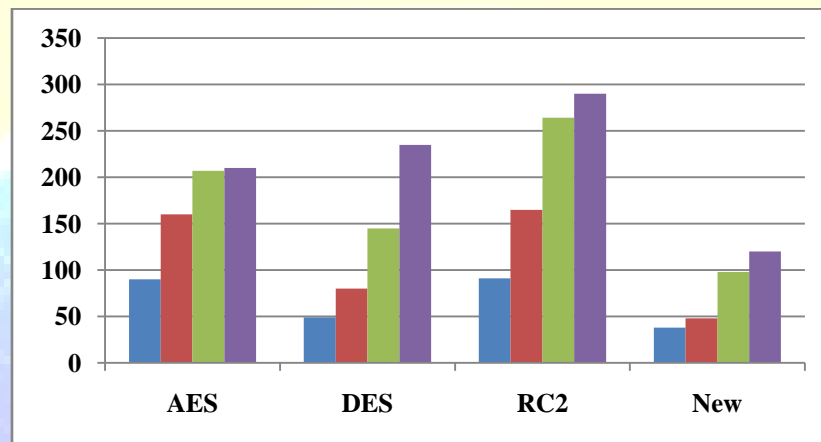


Fig2. Comparison chart

To analyze the security and secrecy of the algorithm, different dimensions of attacks which can be attempted to break the secrecy can be considered. Cipher text-only attack: In this type of attacks, the intruder has only the cipher text. Comparing to the other algorithm our proposed algorithm is very efficient performance. This algorithm we can utilize in small business industry and one time password in banking sector. It is not as much strength like block cipher but it providing high speed data transaction.

CONCLUSION

The aim of this work was to design and implement a new algorithm to address this issue so that we don't have to apply those algorithms to encrypt a small amount of data. Keeping this goal in mind the proposed algorithm has been designed in a quite simple manner. The design

philosophy behind the proposed algorithm is that simplicity of design which yields an algorithm that is easier to implement, achieves a good effect as quickly as possible, achieves better security properties and complete the encryption/decryption process with a high speed. The important thing of our proposed method is that it is not easy to break the encryption algorithm without knowing the exact key value because of the binary digits. We propose that this encryption method can be applied for data encryption and decryption in any type of public application for sending confidential data sending by binary digits to the other end.

ACKNOWLEDGEMENT




We are very grateful to Department of Computer Engineering and Networks, Jazan University to give us opportunity to work on Cryptography. Next, We would like to express my special gratitude to honorable Dean Dr. Mohammad Y Aalsalem as well as my supervisor Prakash Kuppaswamy and who gave me the opportunity to do this wonderful research article on the topic of my favorite subject Cryptography techniques, which also helped me in doing a lot of Research and I came to know about so many new things.

REFERENCES

- 1) Jamal N. BaniSalameh, "A New Symmetric-Key Block Ciphering Algorithm", Middle-East Journal of Scientific Research 12 (5), 662-673, ISSN 1990-9233, 2012.
- 2) W. Diffie and M. Hellman, New directions in cryptography, IEEE Transactions on Information Theory, 22, 644-654, 1976.
- 3) Nadeem, A., Javed, M.Y., "A Performance Comparison of Data Encryption Algorithms," IEEE Information and Communication Technologies, First International Conference, 02-27, P.P. 84- 89, 2006.
- 4) Somdip Dey, Joyshree Nath, Asoke Nath, "An Integrated Symmetric Key Cryptographic Method – Amalgamation of TTJSA Algorithm, Advanced Caesar Cipher Algorithm, Bit Rotation and Reversal Method: SJA Algorithm", IJ.Modern Education and Computer Science, 5, 1-9, 2012.

- 5) T.D.B Weerasinghe, “Secrecy and Performance Analysis of Symmetric Key Encryption Algorithms”, International Journal of Information & Network Security, Vol.1, No.2, pp. 77~87 ISSN: 2089-3299, June 2012.
- 6) RitikaChehal, Kuldeep Singh, “Efficiency and Security of Data with Symmetric Encryption Algorithms”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 8, ISSN: 2277 128X, August 2012.
- 7) PrakashKuppuswamy, Dr. Saeed Q Y Al-Khalidi, Implementation of security through simple symmetric key algorithm based on modulo 37, Council for Innovative Research International Journal of Computers & Technology, ISSN: 2277-3061, Volume 3 No. 2, Oct, 2012.
- 8) William Stallings “Cryptography and Network Security”,3rd Edition, Prentice-Hall Inc., 2005.
- 9) Janakiraman V S, Ganesan R, Gobi M “Hybrid Cryptographic Algorithm for Robust Network Security” , ICGST- CNIR, Volume (7), Issue (I), July 2007.

Author's Detail:

	Mohammed Abudallah Mohammed Aysan, Final year students of Computer Engineering & Networks Department, College of Computer Science & Information System, Jazan University, Kingdom of Saudi Arabia.
	Fareed Hassan Almalki, Final year students of Computer Engineering & Networks Department, College of Computer Science & Information System, Jazan University, Kingdom of Saudi Arabia.
	Abdullah Mohammed almalki, Final year students of Computer Engineering & Networks Department, College of Computer Science & Information System, Jazan University, Kingdom of Saudi Arabia.

