IMPLEMENTATION OF SECURITY THROUGH SIMPLE SYMMETRIC KEY ALGORITHM BASED ON MODULO 37

[1]Prakash Kuppuswamy
Lecturer
Department of Computer Engineering & Networks,
JAZAN University, KSA.

[2] Dr. Saeed Q Y Al-Khalidi
Vice Dean
College of Computer Science and Information Systems,
JAZAN University, KSA.

ABSTRACT

The demand for adequate security to electronic data system grows high over the decades. Security is the one of the biggest concern in different type of networks. Due to diversify nature of network, security breaching became a common issue in different form of networks. Solutions for network security comes with concepts like cryptography in which distribution of keys have been done.

Encryption and key generation became a vital tool for preventing the threats to data sharing and tool to preserve the data integrity so we are focusing on security enhancing by enhancing the level of encryption in network. This study’s main goal is to reflect the importance of security in network and provide the better encryption technique for currently implemented encryption techniques in simple and powerful method. In our research we have 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. Also, we examine the performance of our new SSK algorithm with other existing symmetric key algorithm.

Keyword

SSK(Simple symmetric key), Block cipher, Plain Text (PT), Cipher Text (CT), Key generation.

1. INTRODUCTION

Symmetric or secret key cryptography, a single key is used for both encryption and decryption. Sender uses the key using some set of rules to encrypt the plaintext and sends the ciphertext to the receiver. The receiver applies the same key or rule set to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric key algorithm. The biggest difficulty with this approach, of course, is the distribution of the key.

Secret key cryptography schemes are generally categorized as being either stream ciphers or block ciphers. Stream ciphers operate on a single bit at a time and implement some form of feedback mechanism so that the key is constantly changing. A block cipher is so-called because the scheme encrypts one block of data at a time using the same key on each block. In general, the same plaintext block will always encrypt to the same ciphertext when using the same key in a block cipher whereas the same plaintext will encrypt to different ciphertext in a stream cipher.

Security issues are an important topic in data encryption/decryption methods. Several research papers have been analysed the security aspects in SSK (Simple symmetric key) algorithm. The SSK algorithm is also work with E-mail and Internet technologies for encryption of data transmissions. The communication between a sender and a receiver provides authentication to both parties to secure communication. [5]

2. RELATED WORKS

Hackers seem any target to data repositories due to availability of data on a single place. Encryption/Decryption has become a key component in any business competitive strategy. Organizations are gaining opportunities and benefits such as global presence and improved competitiveness from web-based security. Algorithm provides the capability to generate and verify signatures. Signature generation makes use of a private key to generate a digital signature.[6]

The different methods are used in order to increase security are listed as below.

A.V.N.Krishna, Dr. A.Vinaya Babu in the year 2005 proposed new algorithm is combination of substitution cipher and ceaser algorithm. In this set of mono alphabetic substitution rule is used. This sequence is used to the character in the plain text by a particular chosen rule. In this method sequence of key used with each plain text message also the result combination produced alphabets and numbers, So that it is possible to retrieve the original message and key generation time is huge.[3]

Ayushi in the year 2010 proposed symmetric algorithm Generate the ASCII value of the letter and corresponding binary value and reversing the binary and taking 4 digit divisor and proposed two reverse operation for making more secure. In this there is no standard key generation method and we have to convert value as a ASCII equivalent. It is suitable for small amount of data transaction.[2]

Vishwa gupta,Gajendra Singh, Ravindra Gupta in January 2012 Proposed Algorithm (with 265 bit block size in this thesis) and new Symmetric key Cryptography Algorithm using extended MSA method. This entire method based on block cipher and key generation, encryption and decryption time is more.[1]

3. PROPOSED METHOD

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 (encrypted text) 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.

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. Alphabet value 'A' is assigned as integer number 1 and 'B=2 ……so on. Next we consider integer value '0' assigned as 27 and 1=28……9=36 also the space value considers as an integer number 37.

Second, inverse function, usually written as f-1(x), is a reflection of the original function, f(x), around the line y=x. basically, every x value is changed to a y value and every y value is change to an x value [4].

3.1 Key generation method

1) Select any natural number say as 'n'
2) Find the Inverse of the number using modulo 37(key 1) say 'k'.
3) Again select any negative number (for making secured key)'n1'.
4) Find the inverse of negative number using modulo 37(key 2)'k1'.

3.2 Encryption method

1) Assign synthetic value for message
2) Multiply synthetic value with random selected natural number
3) Calculate with modulo 37
4) Again select random negative number and multiply with it
5) Again calculate with modulo 37
   CT =(PT* n*n1)mod 1

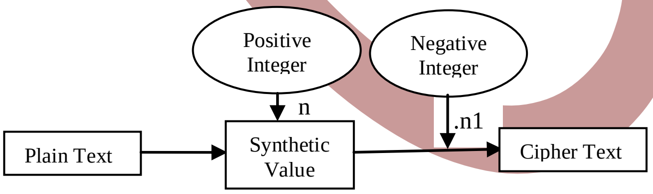

Fig 1: Encryption Structure

3.3 Decryption method

1) Multiply received text with key1 & key2
2) Calculate with modulo 37
3) Remainder is Revealed Text or Plain Text
   PT = (CT*n^{-1}*$n1^{-1}$)mod 1

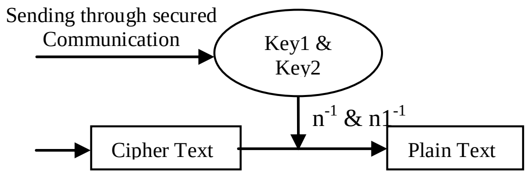

Fig 2: Decryption Structure

4. IMPLEMENTATION

Here we are using symmetric encryption approach. 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 the proposed technique we have two common key between sender and receiver, which is known as private key. 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, the bits size of the secret key has to be chosen effectively. 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.

Table 1. Integer Assigning

D	**E**	**P**	**A**	**R**	**T**	**M**	**E**	**N**
4	5	16	1	18	20	13	5	14
T	**O**	**F**	**N**	**E**	**T**	**W**	**O**	**R**
20	15	6	14	5	20	23	15	18
K	**I**	**N**	**G**	**2**	**0**	**1**	**2**	
11	9	14	7	29	27	28	29	

4.1 Key Generation

1) We are selecting random integer number n=3
2) Then inverse of 3=25(verification 3x25 mod 37=1) So, Key1=25
3) Again we are selecting random negative number n1= -8
4) Then inverse of –8 = 23(verify -8 x 23=-184 mod 37 = 1) So, Key2 =23

4.2 Encryption

Here, assumed Plain Text is "Department of Networking 2012", as we discussed in earlier all the alphabets replaced by synthetic value between 1 and 36.

Table 2. Encryption method

Plain Text	**Integer Value**	**CT=(M*n) mod 37**	**CT=(CT*n1) mod 37**	**Cipher Text**
D	4	12	15	O
E	5	15	28	1
P	16	11	23	W
A	1	3	13	M
R	18	17	12	L
T	20	23	1	A
M	13	2	21	U
E	5	15	28	1
N	14	5	34	7
T	20	23	1	A
O	15	8	10	J
F	6	18	4	D
N	14	5	34	7
E	5	15	28	1
T	20	23	1	A
W	23	32	3	C
O	15	8	10	J

R	18	17	12	L
K	11	33	32	5
I	9	27	6	F
N	14	5	34	7
G	7	21	17	Q
2	29	13	7	G
0	27	7	18	R
1	28	10	31	4
2	29	13	7	G

4.3 Decryption

Here received Cipher Text is "O1WMLAU17AJD71ACJL5F7QGR4G" and its equivalent synthetic value is 15,28,23,13,12,1,21,28,34,1,10,4,34,28,1,3,10,12,32,6,34,17,7,18,31,7. Now, we decrypt the received cipher text using key1 and key2 i.e. inverse of n and n1.

Table 3. Decryption method

Cipher Text	Integer Value	PT=(CT*k1*k2) mod 37	Cipher Text
O	15	4	D
1	28	5	E
W	23	16	P
M	13	1	A
L	12	18	R
A	1	20	T
U	21	13	M
1	28	5	E
7	34	14	N
A	1	20	T
J	10	15	O
D	4	6	F
7	34	14	N
1	28	5	E
A	1	20	T
C	3	23	W
J	10	15	O
L	12	18	R
5	32	11	K
F	6	9	I
7	34	14	N
Q	17	7	G
G	7	29	2
R	18	27	0
4	31	28	1
G	7	29	2

5. RESULTS AND DISCUSSIONS

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 analysed proposed SSK algorithm with existing symmetric cryptographic algorithm.

Table 4. Performance Analysis

Algorithm	Block Cipher	DJSA	Proposed Algorithm
No. of Characters	100	100	100
Key Generation	0.34	0.32	0.10
Encryption Time	1.02	0.58	0.50
Decryption Time	1.02	0.58	0.40

New symmetric algorithm is very authoritative and straight forward. In this algorithm for the encryption, we can take any number of positive and negative integers. When compare to other algorithm, Block cipher or DJSA encryption cycle taking long duration and based on computational complexity.

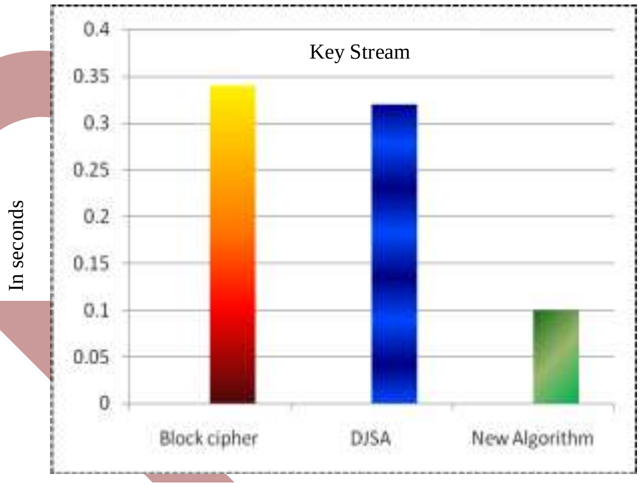

Fig 3: Key Generation Performance

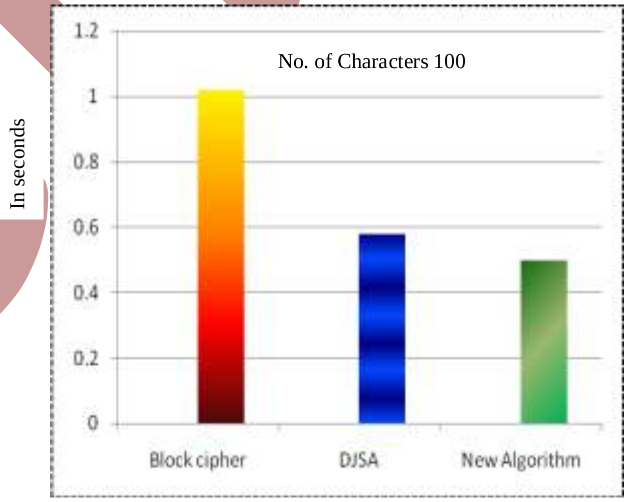

Fig 4: Encryption Performance

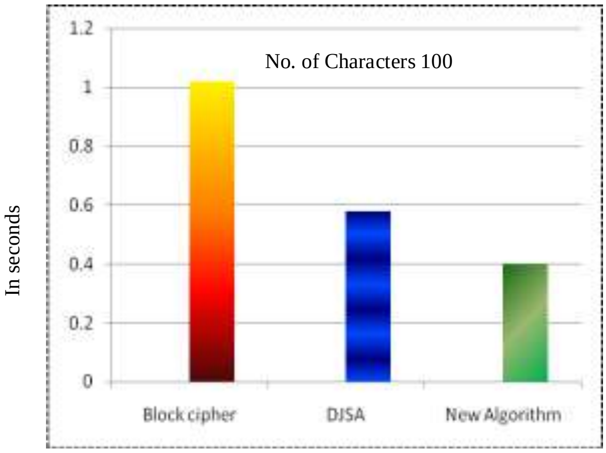

Fig 5: Decryption Performance

SSK uses a combination of positive and negative integer in encryption cycle to create the necessary diffusion and confusion of data. In the decryption part, we can use both the key simultaneously at single stretch.

6. CONCLUSION

From the result it is clear that our “proposed technique” is batter result producing as compared “DJSA symmetric key algorithm” and “Block cipher symmetric key algorithm. Cryptography is used to achieve few goals like Confidentiality. The Algorithm is very simple in nature and there are two inverse functions present in this algorithm. So, It would make it more secured. . For large amount of data transaction and commercial communication purpose this algorithm will work very smoothly. For a very large amount of data those algorithms wouldn’t be cost effective since those are not designed for large amount of data in minimal cost. The important thing of our proposed method is that it is almost impossible to break the encryption algorithm without knowing the exact key value. We propose that this encryption method can be applied for data encryption and decryption in any type of public application for sending confidential data.

7. REFERENCES

[1] Vishwa gupta, Gajendra Singh,Ravindra Gupta, “Advance cryptography algorithm for improving data security”, IJARCE Volume 2, Issue 1, January 2012.

[2] Ayushi, “A Symmetric Key Cryptographic Algorithm” International Journal of Computer Applications (0975-8887), Volume 1, 2010.

[3] A.V.N.Krishna, Dr. A.Vinaya Babu, “Pipeline Data Compression and Encryption Techniques in E- Learning environment” Journal of Theoretical and Applied Information Technology, in 2005.

[4] David A. Santos, “Linear Algebra Notes”, Revision, dsantos@ccp.edu, January 2, 2010.

[5] Anup K. Ghosh “E-Commerce security: No Silver Bullet”, IFIP Conference Proceedings Vol. 142, P:3– 16, 1998.

[6] P. C. O. A.J Menezes, and S.A. Vanstone, “Handbook of Applied Cryptography”: CRC Press, 1996.

[7] A.Nath, S.Ghosh, M.A.Mallik, “Symmetric key cryptography using random key generator”, Proceedings of International conference held at Las Vegas (USA) 12-15 July, 2010.

[8] Majdi Al-qdah & Lin Yi Hui “Simple Encryption /Decryption Application”, published in International Journal of Computer Science and Security, Volume-1, 2008.

[9] T Morkel, JHP Eloff “ ENCRYPTION TECHNIQUES: A TIMELINE APPROACH”, published in Information and Computer Security Architecture (ICSA) Research Group proceeding.

[10] Md. Nazrul Islam, Md. Monir Hossain Mia, Muhammad F. I. Chowdhury, M.A. Matin “Effect of Security Increment to Symmetric Data Encryption through AES Methodology” Ninth ACIS International Conference on Software Engineering,IEEE 2008.

	Dr. Saeed Q. Y. Al-Khalidi, Vice-Dean of College of Computer Sciences and Information Systems, Jazan University. He published many National & International papers, Journals. Also, he participated as a Reviewer in many international conferences worldwide. He completed Master Degree and Doctor of Philosophy in University of East Anglia. His research interests include: Information System development, approaches to systems analysis and the early stages of systems development process, IT/IS evaluation practices, E-readiness assessment.
	Prakash Kuppuswamy Lecturer, Computer Engineering & Networks Department in Jazan University, KSA He is research Scholar proceeding in ‘Dravidian University’. He has been published few journals/Technical papers and participated many international conference in Rep. of Maldives, Libya and Ethiopia. His research area Cryptography, Bio-informatics, Network algorithms etc.,