International Journal of Scientific Research and Management Studies (IJSRMS)
ISSN: 2349-3771 **Volume 1 Issue 6, pg: 192-199**

HYBRID COMBINATION OF MESSAGE ENCRYPTION TECHNIQUES ON ARABIC TEXT: USING NEW SYMMETRIC KEY AND SIMPLE LOGARITHM FUNCTION

Mohammed Abdullah, Mohammed Aysan, Prakash Kuppuswamy
Student, Computer Engineering & Networks Department, Jazan University.
Lecturer, Computer Engineering & Networks Department, Jazan University, KSA.

ABSTRACT

Cryptography is the practice and study of Encrypting/Decrypting information. In modern times cryptography is considered a branch of both mathematics and computer science and is affiliated closely with information theory, computer security and engineering. Cryptography is used in applications present in technologically advanced societies; examples include the security of ATM cards, computer passwords and electronic commerce, which all depend on cryptography. The algorithms and methods used to encrypt messages in Arabic language are few and old; there are no modern encryption algorithms to encrypt the Arabic letters. This research paper proposed the mixed encryption algorithm based on simple multiplication and logarithm function with Caesar cipher to solve the problem. Our method is easy to adopt the coding of advanced language and is safe enough. The security mechanism uses some algorithms to scramble data into unreadable text which can be only being decoded or decrypted by party those know the secret key. The proposed algorithms consume very less amount of computing resources such as CPU time, memory, battery power and cost effective.

KEYWORDS: *Symmetric key, Asymmetric key, Logarithm, Arabic language, Data security etc.*

I. INTRODUCTION

The information security might be defined as "Information security is the collection of technologies, standards, policies and management practices that are applied to information to keep it secure" [1] [10]. In recent days of Internet, the encryption of data plays a major role in securing the data in online transmission focuses mainly on its security across the internet. Different encryption techniques are used to protect the confidential data from unauthorized use [2]. Data that can be read and understood without any special measures is called plaintext or clear-text. The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable gibberish called cipher-text. The process of reverting cipher-text to its original plaintext is called decryption [5].

Confidentiality: The principle of confidentiality specifies that only the sender and the intended recipient(s) should be able to access the contents of a message.

Integrity: When the contents of a message are changed after the sender sends it, but before it reaches the intended recipient, we say that the integrity of the message is lost.

Authentication: The authentication process ensures that the origin of an electronic message or document is correctly identified.

Non-repudiation: There are situations where a user sends a message and later on refuses that she/he had sent that message. Non-repudiation does not allow the sender of a message to refuse the claim of not sending that message.

Availability: The principle of availability states that resources should be available to authorized parties at all times. Interruption puts the availability of resources in danger [1].

Secret key cryptography schemes are generally categorized as being either stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time, and implement some form of feedback mechanism so that the key is constantly changing [1] [5]. Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key cryptography, public-key cryptography, and hash functions. In all cases, the initial unencrypted data is referred to as plaintext. It is encrypted into cipher text, which will in turn (usually) be decrypted into usable plaintext [4] [5]. Julius Caesar developed cryptosystem known as Caesar Cipher [5], which was coded text (Cipher text); to secure contacts and correspondence with the leaders of armies. Later emerged many of them chines that carry out the encryption. Some of the methods used in encryption are [6].

- Caesar cipher.
- Mono alphabetic cipher
- Play fair cipher
- Hill cipher

II. LITERATURE REVIEW

Ragheb Toemeh, Subbanagounder Arumugam (2008) discussed the Cryptanalysis of polyalphabetic by applying Genetic algorithm is presented. The applicability of Genetic algorithms for searching the key space of encryption scheme is studied. In Vigenere cipher, guessing the key size is done by applying Genetic Algorithm. The frequency analysis is used as an essential factor in objective function [6].

John Justin M, Manimurugan S (2012) in this paper focuses mainly on the different kinds of encryption techniques that are existing, and framing all the techniques together as a literature survey. Aim an extensive experimental study of implementations of various available encryption techniques. Also focuses on image encryption techniques, information encryption techniques, double encryption and Chaos-based encryption techniques. This study extends to the performance parameters used in encryption processes and analyzing on their security issues [2].

Obulam Suguna Mani, U.Nanaji, Y.Swapna (2012) They proposed the mixed encryption algorithm based on bit shifting and matrix calculation to solve the problem. Our method is easy to adopt the coding of advanced language and is safe enough. The security mechanism uses some algorithms to scramble data into unreadable text which can be only being decoded or decrypted by party those know the secret key [1].

Prakash Kuppuswamy, Yahya Alqahtani (2014) In this research, they introduce effective symmetric key algorithm on Arabic characters. They proposed a modular 37 and Arabic letters assigning to the integer value also numerals 0-9 also assigned as an integer number called as synthetic value. Choose random integer and calculate inverse of the selected integer with modular 37. The symmetric key distribution should be done in the secured channel for decrypting message [5].

Mohammed Abdullah Mohammed Aysan (2014) the most popular application of EFT is that instead of getting a paycheck and putting it into a bank account, the money is deposited to an account electronically. Cryptography has been used for years to secure electronic funds transfers. However, in the electronic data interchange environment, cryptographic controls are still in their infancy. In this paper, we examine the function and operation flow of the electronic funds transfer process as well as its security control mechanism [3].

III. PROPOSED ALGORITHM

We propose a new method to hide info in any Arabic text combination of message. We use the synthetic specific value for each Arabic letters to do the mathematical calculation. Encryption is a process of coding information which could either be a file or mail message into cipher text in a form unreadable without a decoding key in order to prevent anyone except the intended recipient from reading that data. Decryption is the reverse process of converting encoded data to its original unencoded form, plaintext. The encryption and decryption algorithm mentioned in the following:-

Table 1. Synthetic value

1	2	3	4	5	6	7	8
أ	ب	ت	ث	ج	ح	خ	د
9	10	11	12	13	14	15	16
ذ	ر	ز	س	ش	ص	ض	ط
17	18	19	20	21	22	23	24
ظ	ع	غ	ف	ق	ك	ل	م
25	26	27	28	29	30	31	32
ن	هـ	و	ي	٠	١	٢	٣
33	34	35	36	37	38		
٤	٥	٦	٧	٨	٩		

Encryption method

1. Assign encrypting message as PT
2. Assign the integer value for the PT as per the synthetic table
3. Select random integer say as key1
4. Multiply synthetic value and key1 say as C1
5. Select random logarithm function say as key2
6. Calculate C1 and key2 and say as C2
7. Convert C2 as a binary equivalent digits called as cipher text CT

Decryption method

1. Convert CT as a binary to decimal number
2. Use key2 reveal the logarithm say as P1
3. Use key1 and P1 derived message as Plain Text

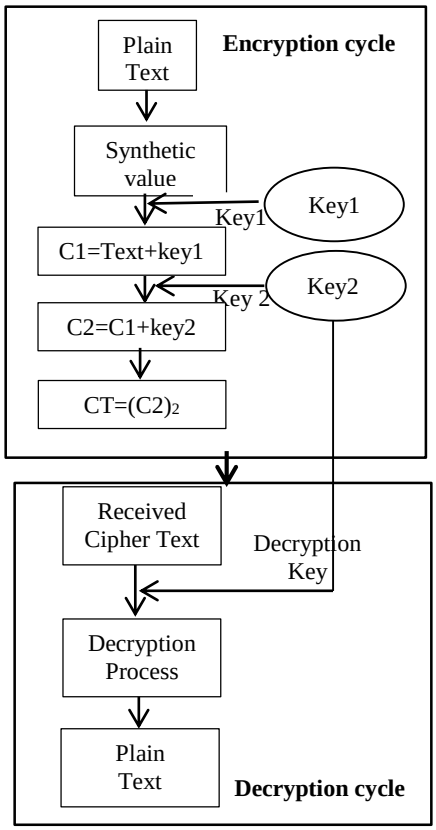

Fig1. Encryption/Decryption Architecture

IV. IMPLEMENTATION

Encryption is the formal name for scrambling program. The normal data, unscrambled, called plaintext or clear text and transform them so that unintelligible to the outside observer, the transformed data is called enciphered text or cipher text. Using encryption security professional can

virtually nullify the value of an interception and the possibilities of effective modification and fabrication. Encryption is clearly addressing the need for confidentially of data. Additionally, it can used to ensure integrity, that the data cannot be read generally cannot be easily changed in the meaningful manner. It is basis of the protocol that enables to provide security while accomplishing an important system or network task. A protocol is an agreed-on sequence of actions that leads to desirable results. For example, some operating system protocols ensure availability of resources as different tasks and users request them. Thus, encryption can also be thought of as supporting availability. That is, encryption is at the heart of methods for ensuring all aspects of computer security. JAZAN UNIVERSITY 2014 (2014 جامعة جازان) - ج ا م ع ه ج ا ز ا ن

Table 2. First Encryption process

Plain Text	**Integer Value**	**Multiply With Random Key (5)**
ج	5	25
ا	1	5
م	24	120
ع	18	90
ه	26	130
ج	5	25
ا	1	5
ز	11	55
ا	1	5
ن	25	125
2	31	155
0	29	145
1	30	150
4	33	165

Table 3. Second Encryption process

Key2 Log_3	**Cipher Text**
2.929947	10.1110111000010001000000
1.464974	1.011101110000100010
4.357763	100.01011011100101100101110
4.095903	100.00011000100011010001110
4.430621	100.01101110000111101001011
2.929947	10.1110111000010001000000
1.464974	1.011101110000100010
3.647632	11.1010010111001011001101
1.464974	1.011101110000100010
4.394921	100.01100101000110011000010
4.590723	100.10010111001110011001111
4.530018	100.10000111101011110100000
4.560877	100.10001111100101011010000
4.647632	100.1010010111001011001101

Table 4. First Decryption process

Cipher Text	**Key2** $Y=X^a$
10.1110111000010001000000	2.929947
1.011101110000101000100010	1.464974
100.010110111001010110010110	4.357763
100.000110001000110100011 0	4.095903
100.011011100011110100101 1	4.430621
10.1110111000010001000000	2.929947
1.011101110000101000100010	1.464974
11.101001011100101100110 1	3.647632
1.011101110000101000100010	1.464974
100.011001010001100110001 0	4.394921
100.100101110011100110011 1	4.590723
100.100001111010111101000 0	4.530018
100.100011111001010110100 0	4.560877
100.101001011100101100110 1	4.647632

Table 5. Second Decryption process

Multiply With Random Key (5)	**Integer Value**	**Plain Text**
25	5	ج
5	1	ا
120	24	م
90	18	ع
130	26	هـ
25	5	ج
5	1	ا
55	11	ز
5	1	ا
125	25	ن
155	31	2
145	29	0
150	30	1
165	33	4

V. RESULT AND DISCUSSION

The result is showing the effect of number of generations on the recovered letters. The result of guessing method of the key length is tabulated as comparison of fitness of some key lengths proposed, the population size is six, number of generation is 30, and text size is 1.5 kb, as in Table 4.

The following table 5 shows the comparison of our proposed algorithm with existing block cipher, stream cipher symmetric key algorithm. Figure 2 shows about key generation executing timing and encryption/decryption timing shows in the figure 3, 4. In figure 5 shows the overall performance of the existing and our proposed algorithm.

Table4. Comparison of symmetric key algorithm

Algorithm	Encryption	Decryption	Total Performance
	1000 bits		
Block Cipher	75 Sec	75 Sec	2.30 mts
Stream Cipher	60 Sec	60 Sec	2.00 mts
New algorithm	55 Sec	55 Sec	1.50 mts

Encryption

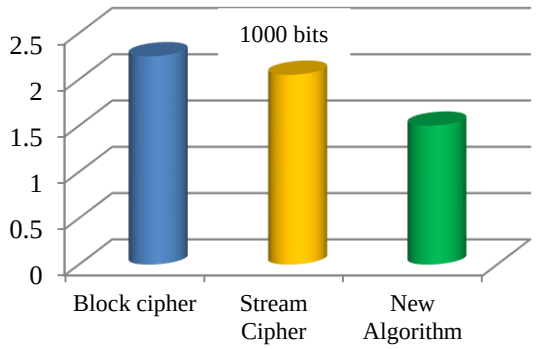

Fig.2. Encryption time

Decryption

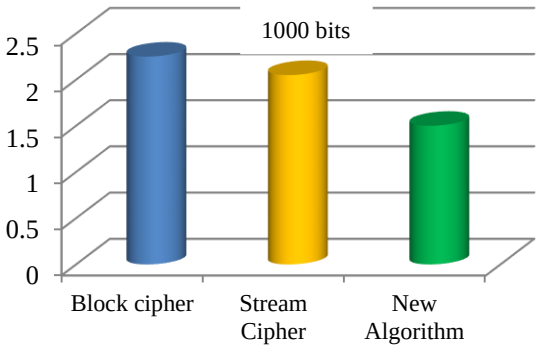

Fig.3. Decryption time

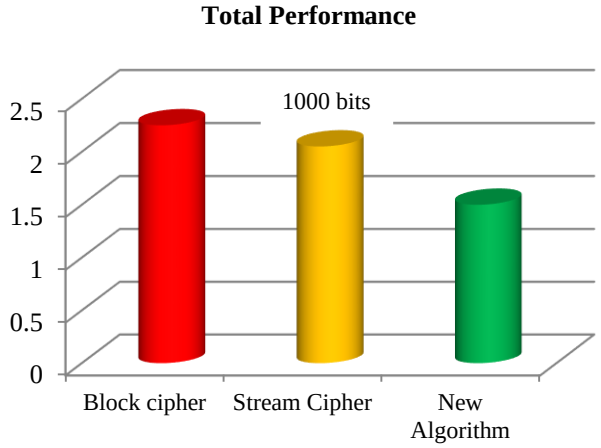

Fig.4. Total performance

VI. CONCLUSION

Encryption algorithm play an important role in communication security where encryption time, Memory usages output byte and battery power are the major issue of concern. This paper presents a performance evaluation of selected symmetric encryption algorithms. Several points can be concluded from the Experimental results. Based on the message files used and the experimental result it was concluded that our proposed algorithm consumes least encryption time and New algorithm has taken maximum time in encryption for same amount of the data. This method featured security, capacity, and robustness, the three needed aspects of data encryption and decryption. Our proposed method is evaluated and compared to a previous method showing similar performance but with the advantage of using standard methods. This Arabic text technique is useful to government privacy file transaction.

VII. FUTURE SCOPE

The growth of digital data storage and communication, cryptography plays in integral role in our society. It is a challenge to respect the serious concerns of national security and copyright protection while also safeguarding individual authorizations. The methodology is applied before encryption we can strengthen cryptographic security. Because applying logarithm function has less redundancy than the original message, cryptanalysis will be harder. The proposed system can be extended such that it can be applied to all types of business transaction, banking sector, e-cash transaction and moreover federal communication system.

REFERENCES

[1]. Obulam Suguna Mani, U.Nanaji, Y.Swapna, “A New Method in Symmetric Encryption for block cipher module: A Bit Shifting Approach”, IJAIR, ISSN: 2278-7844, 2012.
[2]. John Justin M, Manimurugan S, “A Survey on Various Encryption Techniques”, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012.
[3]. Mohammed Abdullah Mohammed Aysan, “Implementation of Electronic Fund Transfer Using New Symmetric key algorithm based on Simple Logarithm”, International Journal of Advanced Research in IT and Engineering ISSN: 2278-6244, Vol. 3, No. 4, www.garph.co.uk, April 2014.
[4]. Menezes, P. van Oorschot, and S. Vanstone, “Handbook of Applied Cryptography”, CRC Press, 1996.
[5]. Prakash Kuppuswamy, Yahya Alqahtani, New Innovation of Arabic language Encryption Technique using New symmetric key algorithm”, International Journal of Advances in Engineering & Technology, ISSN: 22311963, March, 2014.
[6]. Ragheb Toemeh, Subbanagounder Arumugam, “Applying Genetic Algorithms for Searching Key, Space of Polyalphabetic Substitution Ciphers”, The International Arab Journal of Information Technology, Vol. 5, No. 1, January 2008.

[7]. Peter Montgomery, "Modular Multiplication without Trial Division," Math. Computation, Vol. 44, pp. 519–521, 1985.
[8]. W. Hasenplaugh, G. Gaubatz, and V. Gopal, "Fast Integer Reduction," 18th IEEE Symposium on Computer Arithmetic (ARITH '07), pp. 225– 229, 2007.
[9]. Ayushi, "A Symmetric Key Cryptographic Algorithm", International Journal of Computer Applications (0975 - 8887), Volume 1 – No. 15, 2010.
[10]. Nadeem, A, Javed, M.Y, "A Performance Comparison of Data Encryption Algorithms," IEEE Information and Communication Technologies, ICICT 2005, First International Conference, P.P. 84- 89, 2005.
[11]. Cramer, Ronald; Shoup, Victor, "Design and Analysis of Practical Public-Key Encryption Schemes Secure against Adaptive Chosen Ciphertext Attack", SIAM Journal on Computing, 33 (1): 167–226, 2004.
[12]. WulingRen and Zhiqian Miao., "A Hybrid Encryption Algorithm Based on DES and RSA in Bluetooth Communication", Second International Conference on Modelling, Simulation and Visualization Methods, Sanya, 2010.
[13]. Ma Chui and Cao Pitying, "Research of Bluetooth Security Manager", IEEE conference, Nanjing, Vol.2 , PP 1681-1684, 2003.
[14]. WUxing-Hui Zhou Yu-Ping., "Analysis of data encryption algorithm based on WEB", Computer Engineering and Technology (ICCET), 2010 2nd International Conference, Chengdu, China, Volume:7, 2010.
[15]. Ijaz, I., "Design and implementation of PKI (for multi domain environment)". Int. J. Computer Theory Eng., 4(4): 505-509, 2012.

AUTHORS BIOGRAPHY

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

Prakash Kuppuswamy, Lecturer, Computer Engineering & Networks Department in Jazan University, KSA He is research Scholar-Doctorate Degree yet to be awarded by 'Dravidian University'. He has published 15 International Research journals/Technical papers and participated in many international conferences in Rep. of Maldives, Libya and Ethiopia. His research area includes Cryptography, Bio-informatics and Network algorithms.