# NEW INNOVATION OF ARABIC LANGUAGE ENCRYPTION TECHNIQUE USING NEW SYMMETRIC KEY ALGORITHM

Prakash Kuppuswamy, Yahya Alqahtani
Lecturer, Department of Computer Engineering & Networks,
Jazan University, Jazan, KSA.

## *ABSTRACT*

*Security is the one of the biggest concern in different type of network communication as well as individual countries. Cryptography algorithms become much more important in data transmission through unsecured channel. One third of the world using Arabic language, unfortunately, there is no cryptography algorithm to encrypt/decrypt for the Arabic communication country. The main goal of this research is to introduce effective symmetric key algorithm on Arabic characters. In our research we have 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. The procedure of encryption and decryption is simple and effective. We are selecting 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. Here we are attempting simple symmetric key algorithm on Arabic language with ground-breaking sense.*

***KEYWORDS:*** *Symmetric, Private key, Asymmetric, Public key, Modular, Inverse etc.,*

## I. INTRODUCTION

Cryptography is the science of writing messages in secret code and an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription [5].

Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet [5].

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. In a typical situation where cryptography is used, two parties (Alice and Bob) communicate over an insecure channel. Alice and Bob want to ensure that their communication remains incomprehensible by anyone who might be listening. Furthermore, because Alice and Bob are in remote locations, Alice must be sure that the information she receives from Bob has not been modified by anyone during transmission. In addition, she must be sure that the information really does originate from Bob and not someone impersonating Bob. Cryptography is used to achieve the following goals [1]:

- Authentication
- Privacy/confidentiality
- Integrity
- Non-repudiation

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].
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 (or symmetric) cryptography, public-key (or asymmetric) 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 [5].

## II. LITERATURE REVIEW

Ayushi (2010) proposed symmetric key algorithm using ASCII characters. Message in plain text can be understood by anybody knowing the language as long as the message is not codified in any manner. So, now we have to use coding scheme to ensure that information is hidden from anyone for whom it is not intended, even those who can see the coded data [1].
Prakash Kuppuswamy, C. Chandrasekar (2011) proposed scheme based on the block cipher. All the encryption is based on the Alphabets and numbers. Here, we are creating synthetic data value, based on the 26 alphabets and 0-9 numerals. Encryption as cipher text use invertible square matrix, blocking the message according to the selected square matrix i.e. if the square matrix is 3 x 3 make the message or plain text 3 blocks, and select 'e' as any natural number and multiply with selected matrix and message, use modulation 37, then the remainder is our cipher text or encrypted message [2].
Prakash Kuppuswamy, Saeed Q Y Al-Khalidi(2012) proposed new symmetric key algorithm using 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 [3].
Prakash Kuppuswamy, Saeed Q Y Al-Khalidi (2013) in their research discussed about new cryptographic blinding signature protocol algorithm. The requirements for securing blind signature are privacy, authentication, integrity maintenance and non-repudiation. These are crucial and significant issues in recent times for E-voting which is transacted over the internet through e-commerce channels. A new method of security is suggested which is a based on block cipher algorithm [4].

## III. PROPOSED ALGORITHM

It is an attempt to encrypt the Arab languages for the Arab world secure communication. Usually Arabic reading and writing starts from left to right. Here we are taken Arab text for experimental purpose using right to left as used in the way of English letter. The proposed algorithm definitely produces outstanding result when it comes to the practical in the real world application.
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. We know that, whatever user ID consist of Arabic alphabets consist 28 letters and numbers 10 i.e. between 0-9. We are making synthetic table using Arab letters and numerals given in the table 1.

**Table 1.** Synthetic table

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

### 3.1 Key generation

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 user ID
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 37

### 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

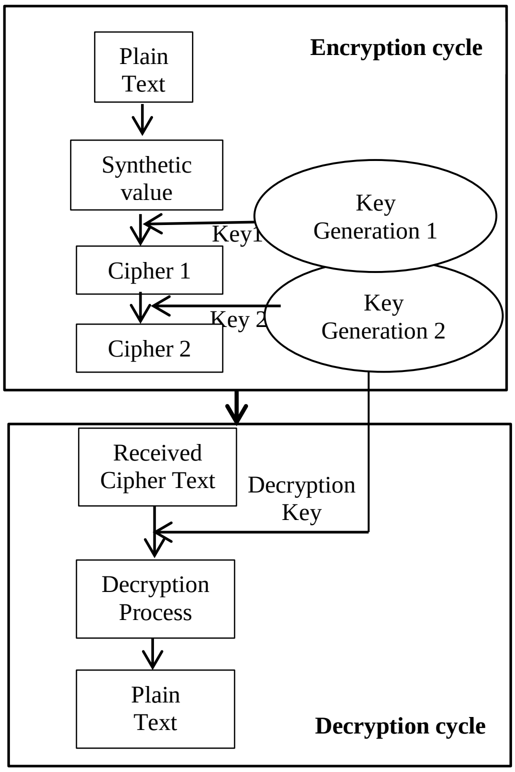

**Figure 1.** Encryption/Decryption Architecture

## 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.** Arabic Plain text & synthetic value

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | ← | ← | ← |
| **1** | **5** | **24** | **16** | **22** | **1** | **5** |
| ا | ج | هـ | ع | م | ا | ج |
| **31** | **28** | **27** | **29** | **23** | **1** | **11** |
| 4 | 1 | 0 | 2 | ن | ا | ز |

## 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 method

For encryption purpose we are arranging text in a sequence table and we are selecting random encryption key1 assumed here as n=3 and key2 n1= -8, Then we are using modulation 37 with plain text. The calculation of encrypted text mentioned in the following table. Calculated message known as cipher text or encrypted text.

**Table 3**. Encryption table

| Text | Integer Value | CT=(M*n) mod 37 | CT=(CT*n1) mod 37 | Encrypted Arab text |
|---|---|---|---|---|
| ج | 5 | 15 | 28 | 1 |
| ا | 1 | 3 | 13 | ش |
| م | 22 | 29 | 27 | 0 |
| ع | 16 | 11 | 23 | ن |
| هـ | 24 | 35 | 16 | ع |
| ج | 5 | 15 | 28 | 1 |
| ا | 1 | 3 | 13 | ش |
| ز | 11 | 33 | 32 | 5 |
| ا | 1 | 3 | 13 | ش |
| ن | 23 | 32 | 3 | ت |
| 2 | 29 | 13 | 7 | خ |
| 0 | 27 | 7 | 18 | ف |
| 1 | 28 | 10 | 31 | 4 |
| 4 | 31 | 19 | 33 | 6 |
| | | | | |

## 4.3 Decryption method

For encryption purpose we are arranging text in a sequence table and we are selecting random encryption key1 assumed here as n=3 and key2 n1= -8, Then we are using modulation 37 with plain text. The calculation of encrypted text mentioned in the following table. Calculated message known as cipher text or encrypted text.

**Table 4**. Decryption table

| Text | Integer Value | PT=(CT*25*23) mod 37 | Encrypted Arab text |
|---|---|---|---|
| 1 | 28 | 5 | ج |
| ش | 13 | 1 | ا |
| 0 | 27 | 22 | م |
| ن | 23 | 16 | ع |
| ع | 16 | 24 | هـ |
| 1 | 28 | 5 | ج |
| ش | 13 | 1 | ا |

| | | | |
|---|---|---|---|
| 5 | 32 | 11 | ز |
| ش | 13 | 1 | ا |
| ت | 3 | 23 | ن |
| خ | 7 | 29 | 2 |
| ف | 18 | 27 | 0 |
| 4 | 31 | 28 | 1 |
| 6 | 33 | 31 | 4 |
| | | | |

## V. Result & Discussion

Proposed method of Arab data Encryption technique, it is combination of positive and negative random integers. The purpose of selecting random positive, negative integers, also, it provides more security and protect the data from the invader. To secure transaction between the two parties application, Key Distribution center generates key for the two parties, one pair key for the encryption key and other pair key using for the decryption cycle. Key has the different attributes like positive and negative number. Message encodes the package to transmit over the network. Then, it decodes at the receiving side using decryption key to achieve original data. It provides authentication and integrity checks to sender and receiver data packages to protect against threats.

The algorithm executes on PC computer of CPU Intel Pentium 4, 2.2 MHz Dual Core. The programs implemented using Microsoft Visual Studio 2008 (C#). It is tested with three messages and with different in length (1000, 2000, 3000bits).

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.

**Table5.** Comparison of symmetric key algorithm

| Algorithm | Key Generation | Encryption | Decryption | Total Performance |
|---|---|---|---|---|
| | 1000 bits | | | |
| Block Cipher | 60 Sec | 75 Sec | 75 Sec | 3.30 mts |
| Stream Cipher | 45 Sec | 60 Sec | 60 Sec | 2.45 mts |
| New algorithm | 15 Sec | 55 Sec | 45 Sec | 1.45 mts |

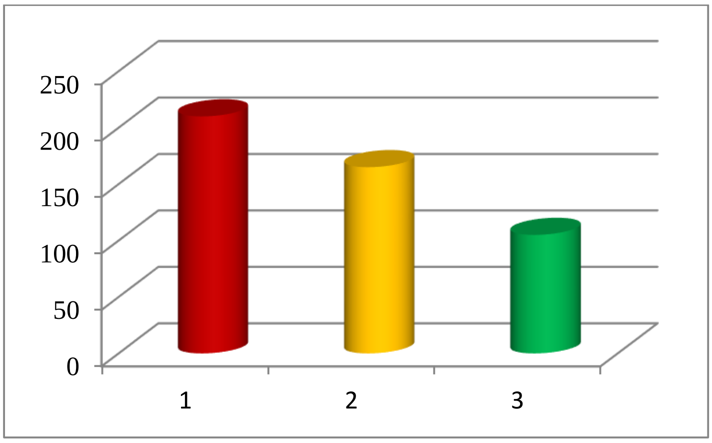

**Figure 2**. Key generation timing

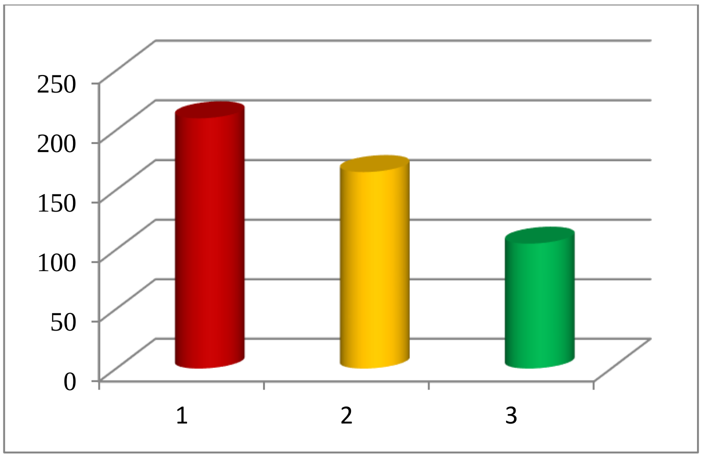

**Figure 3**. Encryption timing

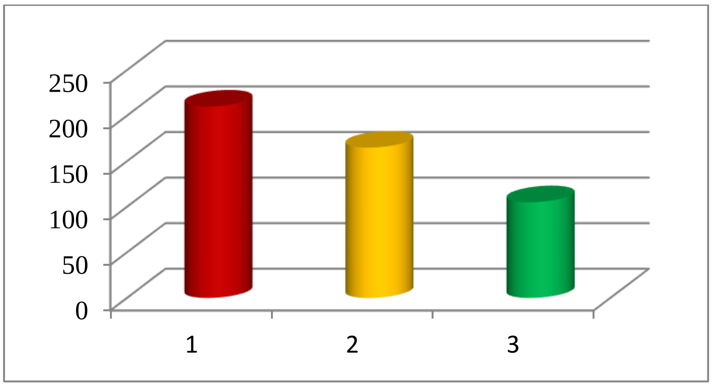

**Figure 4**. Decryption timing

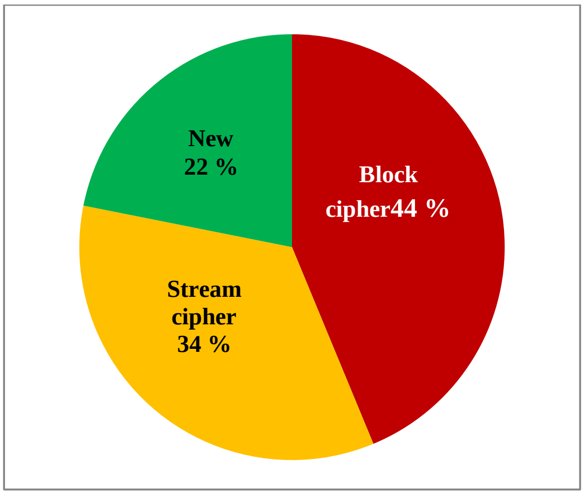

**Figure 5**. Total time consumption performance

For the experimental purpose, we have taken various length of message of 1000bits, 3000bits, and 5000bits. The result of our experimental setup shows in the table 6 and figure 6. It is clear that, the length of the message increases and the average execution timing minimizing.

**Table6**. Performance of various lengths

| Message length | Performance |
|---|---|
| 1000 bits | 1.45 minutes |
| 3000 bits | 4.45 minutes |
| 5000 bits | 6.30 minutes |

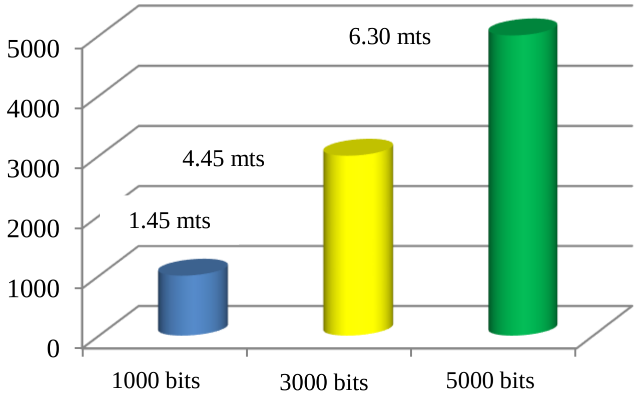

**Figure 6**. Performance of various lengths

## VI. Conclusion

The aim of this work was to design and implement a new algorithm to secure Arabic communication. Cryptography is used to achieve few goals like Confidentiality, Data integrity, Authentication etc. A pair of key is used for both encryption and decryption. The proposed method is increase the performance of symmetric algorithm security rabidly. It has been tested the algorithm for various sizes of messages and parameters. The experimental results shows that the proposed method is improved the interacting performance, while providing high quality of security service for most needed Arab communication system. Several points can be concluded from the experimental results. It has been concluded that the proposed method consumes least encryption time (computing time) and others has taken maximum time in encryption for same amount of the data. It can notice that as more guards added for any information system, then more secure system is resulted. It is clear from percent of efficiency of security methods shown in the table 1. Proposed new algorithm provides more secure and decrease the cost of implementation.

## VII. Future Scope

In future we will suggest the proposed method to develop for selective region encryption to provide good security on the Arab language encryption to the government and private sector. This method can be extended to e-commerce and e-cash transaction.

## References

[1]. Ayushi, “A Symmetric Key Cryptographic Algorithm”, International Journal of Computer Applications (0975 - 8887),Volume 1 – No. 15, 2010.

[2]. Prakash Kuppuswamy, C. Chandrasekar, “Enrichment of security through cryptographic public key algorithm based on block cipher”,Indian Journal of Computer Science and Engineering (IJCSE),ISSN : 0976-5166 Vol. 2 No. 3 Jun-Jul 2011.

[3]. Prakash Kuppuswamy, Dr.Saeed Q Y Al-Khalidi, “Implementation of Security through simple symmetric key algorithm based on modulo 37”, International Journal of Computers & Technology, ISSN: 2277-3061 Volume 3 No. 2, OCT, 2012.

[4]. Prakash Kuppuswamy, Dr.Saeed Q Y Al-Khalidi, “Secured blinding signature protocol based on linear block public key algorithm”, International Journal of Computer Application, volume 61, Number 14, March 2013.

[5]. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.

[6]. Alia, M.A., Yahya, A., “Public–Key Steganography Based on Matching Method”, European Journal of Scientific Research, 223-231, 2010.

[7]. Schneier, B., Applied Cryptography, New York : John Wiley & Sons, 1996.

[8]. Kumar, S., &Wollinger, T. Fundamentals of Symmetric Cryptography, Embedded Security in Cars, 125-143, 2006.

[9]. MiroslawMalek, Mohan guruswamy, Howard Owens and Minhirpandya, "A Hybrid Algorithm Technique" TR-89-06, March 1989.

[10]. Palanisamy, V. and Jeneba Mary, A, Hybrid cryptography by the implementation of RSA and AES, International Journal of Current Research,Vol. 33, Issue, 4, pp.241-244, April, 2011.

[11]. Ijaz Ali Shoukat, Kamalrulnizam Abu Bakar and Subariah Ibrahim, "A Generic Hybrid Encryption System", Research Journal of Applied Sciences, Engineering and Technology 5(9): 2692-2700, ISSN: 2040-7459; e-ISSN: 2040-7467 Maxwell Scientific Organization, 2013.

[12]. M.N. Praphul, K.R.Nataraj, "FPGA Implementation of Hybrid Cryptosystem", International Journal of Emerging Science and Engineering (IJESE) ISSN: 2319–6378, Volume-1, Issue-8, June 2013.

## AUTHORS

**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 20 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.

**Yahya Alqahtani**, Lecturer, Computer Engineering and Networks Department in Jazan University, KSA. He completed Master Degree in 'Central Connecticut State University', USA. In specialization of Computer Information Technology. His research area includes Cryptography, IDS's, and Internet Security.