International Journal of Advanced Research in
IT and Engineering
ISSN: 2278-6244

NEW APPROACH OF ARABIC ENCRYPTION/DECRYPTION TECHNIQUE USING VIGENERE CIPHER ON MOD 39

Yahya Alqahtani*

Prakash Kuppuswamy*

Sikandhar Shah*

Abstract: *The cryptographic methods for enhancing the security of digital contents have gained high significance in the current era. This paper sets out to contribute to the general body of knowledge in the area of classical cryptography by developing a new way of Arabic encryption using Arabic plaintext. The new innovation idea discusses modification of Vigenère cipher which works by adding a key repeatedly into the plaintext using the convention that* أ *= 0,* ب*= 1, . . . ,* ي *= 27 and 28 assigned to blank space and* ٠ *=29,* ١*=30…*٩*=38; and addition is carried out modulo 39 that is, if the result is greater than 39, we subtract as many multiples of 39 as are needed to bring us into the range [0, . . . , 38], that is, [*أ*, . . . ,* ٩*]. The paper has the following structure: section II consist of related works, section III of the methodology, section IV The algorithm section V Implementation, section VI Results and Analysis and section VII concluded the paper.*

Keywords: *Caesar cipher, Vigenere cipher, modulation, symmetric key, Plain text, Cipher text.*

*Lecturer, Department of Computer Engineering & Networks, Jazan University, Jazan, KSA.

I INTRODUCTION

Cryptology has existed for more than 2000 years. But, what is cryptology? The word cryptology is derived from two Greek words: kryptos, which means "hidden or secret," and logos, which means, "description." Cryptology means secret speech or communication. Cryptology encompasses two competing skills – concealment and solution. The concealment portion of cryptology is called cryptography. The aim of cryptography is to render a message incomprehensible to the unauthorized reader. Cryptography is often called "code making."
The solution portion of cryptology is called cryptanalysis. Cryptanalysis is often called "code breaking." The word cryptanalysis was coined (c. 1920) by the American cryptologist William Friedman. The mathematical transformation that shifts the alphabet is called a translation. The shift to the right of three spaces can be symbolized as where p represents a plaintext letter and C represents the corresponding cipher text letter. In information security, encryption is the process of transforming information using an algorithm to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted information. The reverse process is referred to as decryption [1].

There two main algorithmic approaches to encryption, these are symmetric and asymmetric. Symmetric-key algorithms [2] are a class of algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of cipher text. The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link [3]. This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption. Typical examples symmetric algorithms are Advanced Encryption Standard (AES), Blowfish, Tripple Data Encryption Standard (3DES) and Serpent [4].

Cryptographers would probably prefer a = 0, …, z = 25. There are also mathematical reasons to prefer thisnumbering, but we will use the more naïve. With a Caesar cipher, you replace each letter in a

message with a letter further along in thealphabet. A Caesar cipher shifts the alpha bet and istherefore also called a shift cipher. The key is the number of letters you shift. Caesar cipher isone of the oldest types of ciphers. It is named after Julius Caesar, who is said to have used it tosend messages to his generals over 2,000 yea rs ago [5].

The Vigenère cipher is a method of encrypting alphabetictext by using a series of different Caesar ciphers based onthe letters of a keyword. It is a simple form of polyalphabetic substitution [10][11]. The Cipher spoils the statistics of asimple Caesar cipher by using multiple Caesar ciphers. Thetechnique is named for its inventor, Blaise de Vigenère fromthe court of Henry III of France in the sixteenth century, andwas considered unbreakable for some 300 years [12][6].

II. LITERATURE REVIEW

C. R. S. Bhardwaj 2012 This dissertation discusses modification of Vigenère cipher which works by adding a key repeatedly into the plaintext using the convention that A = 0, B = 1, . . . , Z = 25; and addition is carried out modulo 26—that is, if the result is greater than 25, we subtract as many multiples of 26 as are needed to bring us into the range [0, . . . , 25], that is, [A, . . . , Z]. Mathematicians write this as: C = P + K mod 26 .For modification of Vigenère cipher, numbers, punctuations, mathematical symbols may be used for key in place of characters. Random generated numbers may be used to spread the encrypted message [7].

Adnan Abdul-Aziz Gutub, LahouariGhouti, Alaaeldin A. Amin, Talal M. Alkharobi , Mohammad K. Ibrahim (2009), This paper exploits the existence of the redundant Arabic extension character, i.e. Kashida. We propose to use pointed letters in Arabic text with a Kashida to hold the secret bit ‘one’ and the un-pointed letters with a Kashida to hold ‘zero’. The method can be classified under secrecy feature coding methods where it hides secret information bits within the letters benefiting from their inherited points. This watermarking technique is found attractive too to other languages having similar texts to Arabic such as Persian and Urdu [10].

AphetsiKester(2013) Privacy is one of the key issues addressed by informationSecurity. Through cryptographic encryption methods, one can prevent a third party from understanding transmitted raw data over unsecured channel during signal transmission. The cryptographic methods for enhancing the security of digital contents have gained high significance in the current era. Breach of security and misuse of confidential information that has been intercepted by unauthorized parties are keyproblems that information security tries to solve. This paper sets out to contribute to the general body of knowledge in the area of classical cryptography by developing a new hybrid way of encryption of plaintext. The cryptosystem performs its encryption by encrypting the plaintext using columnar transposition cipher and further using the ciphertext to encrypt the plaintext again using Vigenère cipher. At the end, cryptanalysis was performed on the ciphertext [8].

Ajit Singh,AartiNandal, Swati MalikIn recent years there is drastic progress in Internet world. Sensitive information can be shared throughinternet but this information sharing is susceptible to certain attacks. Cryptography was introduced to solve this problem. Cryptography is art for achieving security by encoding the plain text message to cipher text. Substitution and transposition are techniques for encoding. When Caesar cipher substitution and Rail fence transposition techniques are used individually, cipher text obtained is easy to crack. This talk will present a perspective on combination of techniques substitution and transposition. Combining Caesar cipher with Rail fence technique can eliminate their fundamental weakness and produce a cipher text that is hard to crack[9].

III METHODOLOGY

Algorithms are essential to the way computers process data. Many computer programs contain algorithms that detail the specific instructions a computer should perform to carry out a specified task. Additionally, if the algorithm has any parameters, these parameters must meet the requirements defined in the security constraints. If an algorithm appears in a policy for the first time, it may be assumed that the algorithm has already been suitable in the past. In the following table we have assigned synthetic value for the Arabic letters and Arabic numeral from 1 to 39 integer value for أ = 1, ب = 2, . . . ,ي = 28 and 29 assigned to blank space and ٠ =30, ١=31…٩=39.

Table 1 Synthetic table

0	1	2	3	4	5	6	7	8	9	10	11	12
أ	ب	ت	ث	ج	ح	خ	د	ذ	ر	ز	س	ش
13	14	15	16	17	18	19	20	21	22	23	24	25
ص	ض	ط	ظ	ع	غ	ف	ق	ك	ل	م	ن	هـ
26	27	28	29	30	31	32	33	34	35	36	37	38
و	ي	Blank/ Space	٠	١	٢	٣	٤	٥	٦	٧	٨	٩

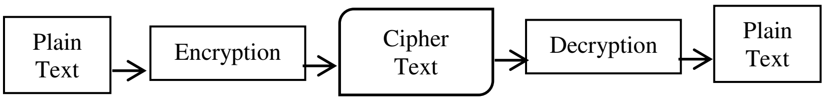

Fig 2. Encryption/Decryption

IV PROPOSED ALGORITHM& ARCHITECTURE

The encryption can also be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,..., Z = 25.Encryption of a letter x by a shift *n* can be described mathematically as

A) Existing algorithm

$E_n(x) = (x+n) \bmod 26$ ……(1)

$D_n(x) = (x-n) \bmod 26$ ……(2)

There are different definitions for the modulo operation. In the above, the result is in the range 0...25. i.e., if x+n or x-n are not in the range 0...25, we have to subtract or add 26. Their placement remains the same throughout the message, so the cipher is classed as a type of monoalphabetic substitution, as opposed to polyalphabetic substitution.

B) New algorithm

We are proposing here, some modification with existing vigenere algorithm according to the Arabic language. The encryption/decryption process represented using modular arithmetic by first transforming the letters into numbers, according to the Arabic scheme mentioned in table no.1.

$E_n(x) = (x+n) \bmod 39$……….. (3)

$E1_n(x) = (x-n1) \bmod 39$……….(4)

$D_n(x) = ((x+n)-n1) \bmod 39$…….(5)

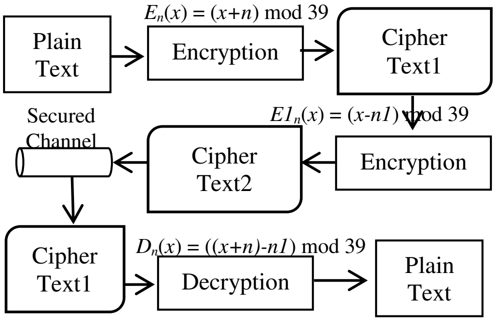

Fig 2. Proposed Encryption/Decryption Architecture

V IMPLEMENTATION

Here, we use simple Arabic text for encryption/decryption implementation process. The reason for selecting two different keys, to make complicated to understand by the intruder. 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. Thus atwo different key is chosen. The encryption of ٢ قسم الشبكات ٠١٤ (Networking Department 2014) plaintext mentioned in the below table, the first encryption using key 13 the encrypted messages is ضهـ٦صت٧نهحثجدظصه, and second stage encryption key using key -17 the cipher text is يهو٠٩٦ع٧ذغ٦نفدظ

A) Encryption process

Synthetic Value	31	29	30	33	3	0	21	1	12	22	0	28	23	11	20
Plain Text	٢	٠	١	٤	ت	ا	ك	ب	ش	ل	ا	Blank /space	م	س	ق
Key(13)	5	3	4	7	16	13	34	14	25	35	13	2	36	24	34
Encryption1	ح	ث	ج	د	ظ	ص	ه	ض	هـ	٦	ص	ت	٧	ن	ه
Key (-17)	27	25	26	29	38	35	17	36	8	18	35	24	19	7	16
Cipher Text	ي	هـ	و	٠	٩	٦	ع	٧	ذ	غ	٦	ن	ف	د	ظ

B) Decryption Process

In the decryption we using here two key simultaneously i.e (-13), (+17) on the received cipher text of يهو٠٩٦ع٧ذغ٦نفدظ . The decryption process mention in the below table, and finally revealed message is قسم الشبكات ٢٠١٤ (Networking Department 2014).

Synthetic Value	27	25	26	29	38	35	17	36	8	18	35	24	19	7	16
Cipher Text	ي	هـ	و	٠	٩	٦	ع	٧	ذ	غ	٦	ن	ف	د	ظ
Key(-13) (+17)	31	29	30	33	3	0	21	1	12	22	0	28	23	11	20
Plain Text	٢	٠	١	٤	ت	ا	ك	ب	ش	ل	ا	Blank /space	م	س	ق

VI. RESULT AND DISCUSSION

Symmetric algorithms, Message can be transmitted faster than asymmetric Key. Symmetric keys are subject to a brute force attack where all keys in the key space are tried systematically to break the encryption. As we are using Customized double encryption/decryption cryptography, there is no chance to pick up the actual signals during the transmission by the intruders.

The proposed method of Arabic language security, It is double encryption decryption method using positive key and negative key. To secure message transmission, it needs two keys. Application encodes the messages to transmit over the secured channel. Then, it use private key and decryption algorithm to decode at the receiving side to achieve original data. The algorithm executes on PC computer of CPU Intel Pentium 4, 2.2 MHz Dual Core. The programs implemented using Microsoft Visual Studio 2008. It is tested with various length of message and compare with existing traditional algorithm. The performance result and security result declared in the following tables and figures.

Table 3. Performance analysis

Algorithm	**Encryption Timing**	**Decryption Timing**	**Average Timing**
Vigenere mod26	7	7	7
Affine cipher	16	18	17
Transposition cipher	22	22	22
Proposed mod 39	9	9	9

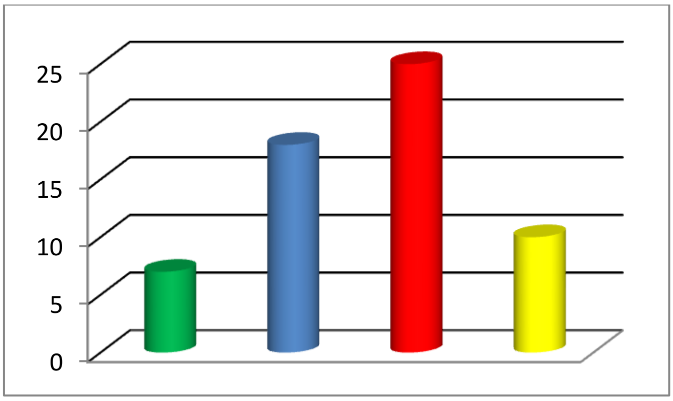

Fig 4. Comparison performance of algorithm

Table 3. Security comparison

Algorithm	Security
Vigenere mod26	7
Proposed mod 39	10

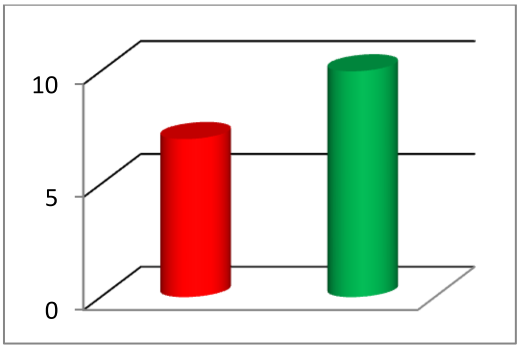

Fig 4. Security comparison

VII. CONCLUSION

Modification of Vigenère cipher is more immune to any type of outsider attack. Random generated number increase the difficulty to decipher the message. Both encryption and decryption process are carried outusing a single key. These algorithms are efficient, are secure, execute at high speeds, and consume less computer resources of memory and processor time. Symmetric-Key Encryption Techniquesin any symmetric-key encryption technique, both encryption and decryption process are carried out using a single key. In table no.4 and Figure 5, clearly mentioned that the proposed algorithm security better than vigenere mod 26, Also It is the first time we are proposing the algorithm implementation on Arabic language. Therefore it is a mile stone on Arabic language secret communication for the Arab nation.

REFERENCES

1. Nicolas Courtois, Josef Pieprzyk, "Cryptanalysis of Block Ciphers with Overdefined Systems of Equations", pp267–287, Asiacrypt, 2002.
2. Delfs, Hans,Knebl, Helmut, "Symmetric key encryption",Introduction to cryptography: principles and applications, Springer, 2007.
3. Mullen, Gary,Mummert Carl,“Finite fields and applications”, American Mathematical Society. p. 112,IEEE 1363: Standard Specifications for Public-Key Cryptography, 2007.

4. Caesar Ciphers, Fall Chris Christensen MAT/CSC 483 ,http://www.nku.edu), 2006.
5. AphetsiKester, “A Hybrid Cryptosystem based on Vigenere Cipher and Columnar Transposition Cipher”, International Journal of Advanced Technology & Engineering Research (IJATER), ISSN No: 2250-3536,Volume 3, Issue 1, Jan. 2013.
6. C. R. S. Bhardwaj, “Modification of Vigenère Cipher by Random Numbers, Punctuations & Mathematical Symbols”, IOSR Journal of Computer Engineering (IOSRJCE), ISSN: 2278-0661 Volume 4, Issue 2, PP 35-38 ,Sep.-Oct. 2012.
7. Adnan Abdul-Aziz Gutub, LahouariGhouti, Alaaeldin A. Amin, Talal M. Alkharobi , Mohammad K. Ibrahim, “Utilizing Extension Character ‘Kashida’ with pointed letters for Arabic text digital watermarking”, proceeding of: Computer Systems and Applications, 2009. AICCSA. IEEE/ACS International Conference, 2009.
8. Ajit Singh, AartiNandal, Swati Malik, “Implementation of Caesar Cipher with Rail Fence for Enhancing Data Security”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 12, ISSN: 2277 128, December 2012.
9. Beutelspacher, Albrecht, “Cryptology. Mathematical Association of America”. pp. 9–11.ISBN 0-88385-504-6, 1994.
10. Leighton, Albert C., "Secret Communication among the Greeks and Romans", Technology and Culture 10 (2): 139–154. doi:10.2307/3101474. JSTOR 3101474, April 1969.
11. Sinkov, Abraham; Paul L. Irwin, “Elementary Cryptanalysis: A Mathematical Approach”, Mathematical Association of America. pp. 13–15. ISBN 0-88385-622-0, 1966.
12. Singh, Simon, “The Code Book”, Anchor. pp. 72–77. ISBN 0-385-49532-3, 2000.