An Enhanced Vigenere Cipher For Data Security

Aized Amin Soofi, Irfan Riaz, Umair Rasheed

Abstract: In today's world the amount of data that is exchanged has increased in the last few years so securing the information has become a crucial task. Cryptography is an art of converting plain text message into unreadable message. Encryption algorithms play an important role in information security systems. Encryption is considered as one of the most powerful tool for secure transmission of data over the communication network. Vigenere technique is an example of polyalphabetic stream cipher; it has various limitations such as Kasiski and Friedman attack to find the length of encryption key. In this paper an enhanced version of traditional vigenere cipher has been proposed that eliminates the chances of Kaisiski and Friedman attack. Proposed technique also provides better security against cryptanalysis and pattern prediction.

Index Terms: Encryption; Stream cipher; Vigenere cipher; symmetric encryption

1. INTRODUCTION

With the rapid development of computer technology, the number of data files transmitted over internet keeps increasing. As a result, the secure transmission of secret data over public channels has become a common interest in both academic and research fields [1]. There are many aspects to security and applications, ranging from secure commerce and payments to private communications and protecting passwords. Cryptography is an essential aspect for secure communications [2]. Although the crucial goal of cryptography is to hide information from unauthorized individuals, most algorithms can be broken and the information can be exposed if the attacker has enough time, desire, and resources. So a more hardheaded goal of cryptography is to make it too work intensive for attacker. The basic terms used in cryptography are discussed below:

- **Plain text**

In cryptography, plain text is a simple readable text before being encrypted into ciphertext [3]. The data that can be read and understood without any special measure is called plaintext [4].

- *Aized Amin Soofi is currently pursuing doctorate degree in computer science from Allama Iqbal Open University, Islamabad, Pakistan. E-mail: aizedamin@yahoo.com*
- *Irfan Riaz is currently serving as lecturer in Electrical Engineering department, Government College University, Faisalabad, Pakistan. Email: shohabsons@gmail.com*

For example person A send message "how are you" to person B. In this case "how are you" will be our plain text message.

- **Cipher text**
  In Cryptography, the transformation of original message into non readable message before the transmission is known as cipher text [5]. It is a message obtained by some kind of encryption operation on plain text.
- **Encryption**
  Encryption is a process of converting plain text into cipher text. Encryption process requires encryption algorithm and key to convert the plain text into cipher [6]. In cryptography encryption performed at sender end.
- **Decryption**
  Decryption is the reverse process of encryption. It converts the cipher text into plain text. In cryptography decryption performed at receiver end.
- **Key**
  The key is the numeric or alphanumeric text used for the encryption of plain text and decryption of cipher text [5].

1.1 Objectives of Cryptography

Various goals of cryptography are presented in [7, 8]. These goals include:

- **Authentication**
  Authentication is verification of the identity of the sender at receiver end. A user or system can prove their identity to another who does not have personal knowledge of their identity.
- **Confidentiality**
  Confidentiality is most commonly addressed goal. It refers that transmitted message is only received by authorized party.
- **Integrity**
  Integrity is making it sure that the received message is in same form as it was sent. Only authorized users have privileges to modify the data.
- **Access control**
  Access control is making it sure that only authorized parties have privileges to access the given information.
- **Non Repudiation**
  Non repudiation is a method of guaranteeing message transmission between parties via digital signature or encryption. It helps to protect against the denial of authentication attempt.

1.2 Classification of Cryptography

Cryptography is classified into two basic types include symmetric cryptography and asymmetric cryptography. The classification of cryptography is shown in figure 1.

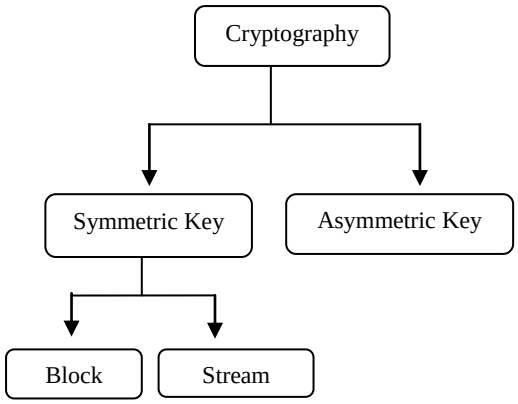

Figure1: *Cryptography classification*

a) Symmetric Key Cryptography

Symmetric key is also known as secret key or private key cryptography. Symmetric key algorithms are most commonly used algorithms. It uses [9] same key for both encryption of plain text and decryption of cipher text. It categorized into stream cipher and block cipher.

(i) Stream Cipher

Stream cipher operates on single bit in which cryptographic key and algorithm are applied to each binary digit in data stream [10]. Stream ciphers are an important class of symmetric ciphers used widely in encryption for hardware-based cryptographic systems. They are simple, efficient without compromising performance [11].

(ii) Block Cipher

In block cipher cryptographic key and algorithm are applied on block of data instead of single bit in stream [12]. It encrypts one block of data at a time by using the same key on each block [13].

b) Asymmetric Key Cryptography

Asymmetric key is also known a public key cryptography. This type of cryptography used asymmetric algorithms that encrypt and decrypt with different keys in which public key used for encryption and private key used for decryption [2]. Asymmetric algorithms are very slow in working and it is unfeasible to use them to encrypt huge data. This paper is organized as following; in section2 introduction of Vigenere cipher is presented, review of literature is presented in section 3, section 4 contains description of proposed approach and section 5 consist of conclusion and future directions.

2. VIGENERE CIPHER

The Vigenere cipher is a method of encrypting alphabetic text by using a series of different Caesar ciphers based on the letters of a keyword. It is a simple form of polyalphabetic substitution in which each alphabet can replace with several cipher alphabets [14]. Vigenere cipher was considered secure for centuries but later its weakness was identified. Friedrich Kasiski discovered a method to identify the period and hence key and plaintext [15]. The basic theme of Vigenere cipher is to conceal plaintext letter frequencies by defeating simple frequency analysis. But the crucial weakness of the Vigenere cipher is the repeating nature of its key. If a cryptanalyst correctly guesses the key's length, then the cipher text can be easily broken. Various methods like Kasiski and Friedman tests can help to determine the key length. With the advent of computer the Vigenere cipher has become even easier to break. Most cipher texts can be cracked within a few seconds even with long keys. This cipher is now considered trivial to break and provides no security by today's standards. However, it is used in many stronger encryption algorithms like the Advance Encryption Standard (AES) [16]. Vigenere algorithm can be viewed algebraically if the letters A–Z are taken to be the numbers 0–25, Vigenere encryption formula is:

$$Ci = (Pi + Ki) \bmod m$$

Where,
C = Cipher text character
P = Plain text character
K = Key phrase character
m = Length of alphabets (i.e, 26 in Vigenere cipher)

3. LITERATURE REVIEW

In [17] modified version of vigenere algorithm was proposed in which diffusion is provided by adding a random bit to each byte before the message is encrypted using Vigenere. This technique fails kasiski attack to find the length of key because the padding of message with random bits. The main drawback of this technique is that the size of the encrypted message will be increased by around 56%. In [18] a new way of implementing Vigenere algorithm was introduced by automatically changing the cipher key after each encryption step. In this method successive keys were used that were dependent on the initial key value during the encryption process. In [14] modification of Vigenere cipher by random numbers, punctuations & mathematical symbols was presented. In proposed method numbers, punctuations and mathematical symbols were used for key in place of characters to make it more difficult for brute force attack. It was concluded that if random numbers are used for key and to spread the spectrum then only skilled persons can identify the message. A novel approach was presented [19] by combing the LFSR (Linear feedback shift register) key with Vigenere cipher key. In Proposed technique the concepts and methodologies of classical Vigenere cipher plus modern LFSR stream cipher was used. Proposed technique generates the period less and pseudorandom letter key stream for encryption/ decryption. Period less and randomness of key lowers the flatness of letter frequency that makes it difficult to identify the length of key. In [20] the Caesar Cipher and Vigenere Cipher have been modified and expanded by including alphabets, numbers and symbols and at the same time introduced a complete confusion and diffusion into the modified cipher developed. It was concluded that cipher text generated by proposed hybrid technique is very difficult to break using a frequency method, brute force attack etc. A new algorithm [21] by combining Vigenere substitution cipher with Stream cipher was proposed in which repeated portions of plaintext always encrypted with the different portion of the keyword

or binary key. The letters in odd location were encrypted with stream cipher and the letters in even locations with Vigenere cipher. It was concluded that proposed algorithm hides the relation between cipher text and plain text that makes cryptanalysis much difficult.

4. PROPOSED APPROACH

In traditional Vigenere cipher each alphabet has one fixed numeric value but in our proposed technique we have eight tables shown in figure 2. In each table every alphabet represent with different numeric value. In traditional Vigenere technique the plaintext is considered as a sequence of alphabets without any space between them. It may create a problem for receiver to read the message by inserting spaces between words and receiver needs to guess the exact place to insert space in decrypted plaintext. In proposed technique we eliminate this problem by introducing different numeric value for space in each table. The encryption and decryption process by proposed approach is given below:

4.1 Encryption

Formula for encryption by proposed method is:

Ci = Pi + Ki (mod m)

In proposed approach we have length of alphabet 27, so value m will be 27.

The steps for encryption process are:

- If the length of key is smaller than the length of plain text then key will be repetitive until it becomes equal to the length of plain text.
- Numeric value of first plain text character and key character will be added according to table 1.
- Modulo 27 of the resultant value from above step will be calculated. The character correspond to the calculated modulo value will be first cipher text character.
- Numeric value of second plain text character and key character will be added according to table 2.
- Modulo 27 of the resultant value from above step will be calculated. The character correspond to the calculated modulo value will be second cipher character.
- The process explained in above steps will remain continue till eighth table. After that next plain character i.e character 9 of plain text and key will undergo through same process by using value from table 1 and so on.

Mathematically we can express encryption process by proposed algorithm as:

C1 = P1 + K1 (mod 27) [T1], C2 = P2 + K2 (mod 27) [T2], ------ , C8 = P8 + K8 (mod 27) [T8], C9 = P9 + K9 (mod 27) [T1], ------, C16 = P16 + K16 (mod 27) [T8], C17 = P17 + K17 (mod 27) [T1],------

Where, T in above mathematical relation represents table no.

4.2 Decryption

Decryption process of proposed approach works the same way as encryption does but in reverse direction. Formula for decryption by proposed method is:
Pi = Ci - Ki (mod m)

The steps for decryption process are:

- Numeric value of first cipher text character and key character will be subtracted according to table 1.
- Modulo 27 of the resultant value from above step will be calculated. The character correspond to the calculated modulo value will be first plain text character.
- The process explained in above steps will remain continue till eighth table. After that next cipher character i.e character 9 of cipher text and key will undergo through same process by using value from table 1 and so on.

Mathematically we can express decryption process by proposed algorithm as:

P1 = C1 - K1 (mod 27) [T1], P2 = C2 - K2 (mod 27) [T2], ------- , P8 = C8 - K8 (mod 27) [T8], P9 = C9 - K9 (mod 27) [T1], ------, P16 = C16 - K16 (mod 27) [T8], P17 = C17 - K17 (mod 27) [T1],------

T.No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	&	A
2	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	&	A	B	C
3	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	&	A	B	C	D	E
4	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	&	A	B	C	D	E	F	G
5	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	&	A	B	C	D	E	F	G	H	I
6	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	&	A	B	C	D	E	F	G	H	I	J	K
7	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	&	A	B	C	D	E	F	G	H	I	J	K	L	M
8	P	Q	R	S	T	U	V	W	X	Y	Z	&	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O

Figure 2: *Proposed technique tables*

The first column of figure 2 represent the table numbers and first row represent the numeric value of alphabets in each table. Space is represented by "&" in given table. In our proposed method space in the plain text will also converted into some cipher character by using the value of space from tables.

Example:
Let's suppose our plaintext is "RED COOKIES" and key phrase is "GAME".

Encryption and decryption by proposed approach

Plain Text	R	E	D	&	C	O	O	K	I	E	S
Key	G	A	M	E	G	A	M	E	G	A	M
Cipher text (encryption)	R+G (mod 27) = 21 mod 27= 21 = W [T1]	B	K	X	&	N	N	J	N	B	Z
Plain text (decryption)	W –G (mod 27)= 16 (mod 27)= 16 = R [T2]	E	D	&	C	O	O	K	I	E	S

In proposed technique each combination of plain text character and key phrase character can replaced with several cipher characters because of multiple tables but in traditional Vigenere technique there is exactly one value for each combination. Proposed approach makes our technique much stronger against kasiski and friedman attack to find the length of key. As we can see in example that proposed technique also converted the space between the words into cipher text that will be helpful for receiver to read the plain text message easily after decryption process.

5. CONCLUSIONS AND FUTURE WORK

Cryptography is the widely used method for the security of data. Vigenere cipher is one of the cryptographic method that is considered simplest and weakest due to many limitations. To overcome the limitations of Vigenere cipher we proposed an enhanced version of Vigenere cipher that is much secure against Kasiski and Friedman attacks. Cryptanalysis, frequency analysis, pattern prediction and brute attack on proposed technique are also much difficult due to use of multiples tables for encryption. Although there are many cryptographic methods but this domain still requires serious attention of research community for the improvement of data security. In future our aim is to provide validation of proposed approach by performing security and performance analysis.

REFERENCES

[1] Z.-p. Wang, et al., "Single-intensity-recording optical encryption technique based on phase retrieval algorithm and QR code," Optics Communications, vol. 332, pp. 36-41, 2014.

[2] S. William and W. Stallings, Cryptography and Network Security, 4/E: Pearson Education India, 2006.

[3] M. Rouse. (2007, Plain text. Available: http://searchsecurity.techtarget.com/definition/plaintext

[4] T. Gunasundari and K. Elangovan, "A Comparative Survey on Symmetric Key Encryption Algorithms," International Journal of Computer Science and Mobile Applications, ISSN, pp. 2321-8363, 2014.

[5] M. Agrawal and P. Mishra, "A comparative survey on symmetric key encryption techniques," International Journal on Computer Science and Engineering (IJCSE), vol. 4, pp. 877-882, 2012.

[6] V. Beal. (2009, Encryption. Available: http://www.webopedia.com/TERM/E/encryption.html

[7] O. P. Verma, et al., "Peformance analysis of data encryption algorithms," in Electronics Computer Technology (ICECT), 2011 3rd International Conference on, 2011, pp. 399-403.

[8] E. Surya and C. Diviya, "A survey on Symmetric Key Encryption Algorithms," International Journal of Computer Science & Communication Networks, vol. 2, pp. 475-477, 2012.

[9] N. Courtois and J. Pieprzyk, "Cryptanalysis of Block Ciphers with Overdefined Systems of Equations," in Advances in Cryptology — ASIACRYPT 2002. vol. 2501, Y. Zheng, Ed., ed: springer Berlin Heidelberg, 2002, pp. 267-287.

[10] R. Wash, "Lecture notes on stream ciphers and RC4," Reserve University, pp. 1-19, 2001.

[11] S. Burman, et al., "LFSR based stream ciphers are vulnerable to power attacks," in Progress in Cryptology–INDOCRYPT 2007, ed: springer, 2007, pp. 384-392.

[12] M. Rouse. (2006, Block Cipher. Available: http://searchsecurity.techtarget.com/definition/block-cipher

[13] G. C. Kessler, "An overview of cryptography," ed: Gary C. Kessler, 2003.

[14] C. Bhardwaj, "Modification of Vigenère Cipher by Random Numbers, Punctuations & Mathematical Symbols," Journal of Computer Engineering (IOSRJCE) ISSN, pp. 2278-0661, 2012.

[15] A. J. Menezes, et al., Handbook of applied cryptography: CRC press, 2010.

[16] C. Sanchez-Avila and R. Sanchez-Reillo, "The Rijndael block cipher (AES proposal): a comparison with DES," in Security Technology, 2001 IEEE 35th International Carnahan Conference on, 2001, pp. 229-234.

[17] P. I. Wilson and M. Garcia, "A Modified Version of the Vigenère Algorithm," IJCSNS, vol. 6, p. 140, 2006.

[18] Q.-A. Kester, "A cryptosystem based on Vigenère cipher with varying key," International Journal of

Advanced Research in Computer Engineering & Technology (IJARCET), vol. 1, pp. pp: 108-113, 2012.

[19] A. Razzaq, et al., "Strong Key Machanism Generated by LFSR based Vigenère Cipher," presented at the 13 International Arab Conference on Information Technology, 2013.

[20] O. Omolara, et al., "Developing a Modified Hybrid Caesar Cipher and Vigenere Cipher for Secure Data Communication," Computer Engineering and Intelligent Systems, vol. 5, pp. 34-46, 2014.

[21] F. H. S. Fairouz Mushtaq Sher Ali, "Enhancing Security of Vigenere Cipher by Stream Cipher," International Journal of Computer Applications, vol. 100, pp. 1-4, 2014.