International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 3 Issue 5, August 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Cryptosystem Based on Modified Vigenere Cipher using Encryption Technique

Vittal Kumar Mittal[1], Manish Mukhija[2]

[1]M.Tech Student, [2]Assistant Professor
[1,2]Department of Computer Science and Engineering,
[1,2]Modern Institute of Technology & Research Centre, Jahar Khera, Rajasthan, India

How to cite this paper: Vittal Kumar Mittal | Manish Mukhija "Cryptosystem Based on Modified Vigenere Cipher using Encryption Technique" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-5, August 2019, pp.1936-1939, **https://doi.org/10.31142/ijtsrd27878**

IJTSRD27878

ABSTRACT

In this new era of technology securing information in internet has become a crucial task. To secure such information, encryption plays an important role in information security. In this paper Vigenere cipher is considered which is to be most efficient and simplest one. Due to its repeating nature, it is vulnerable to attacks like Kasiski, known plain text etc., to find the length of encryption key. To overcome this, this research present a modified algorithm encryption technique is done by using Vigenere cipher to improve better security against cryptanalysis.

KEYWORDS: *Encryption, Vigenere cipher, Cipher ceaser, Decryption, data security*

1. INTRODUCTION

With the rapid development of information technology, secrecy and privacy are the key issues of cryptography. Through cryptography one can prevent an intruder from understanding the data during communication time. To this, encryption and related technologies are considered as one of the most powerful tool to secure data transmission over the communication network like Virtual Private Network (VPN) [4].

VPN or virtual private network is a network constructed by using public wires usually the Internet to connect to a private network, such as a company's internal network to transport the confidential data. These systems use security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted [5] [4].

So, to secure the information, cryptography is used where the encryption is the process of transforming plain text message into scrambled message by using a key and vice versa for decryption. Encryption techniques are broadly divided by two types namely, Symmetric and Asymmetric. In symmetric encryption techniques, same key is used for both encryption and decryption. In Asymmetric-key encryption two keys - public and private keys, where the public key is known to all members while the private key is kept secure by the user [7]. Thus, the security of encrypted data depends on the strength of cryptographic algorithm and the secrecy of the key.

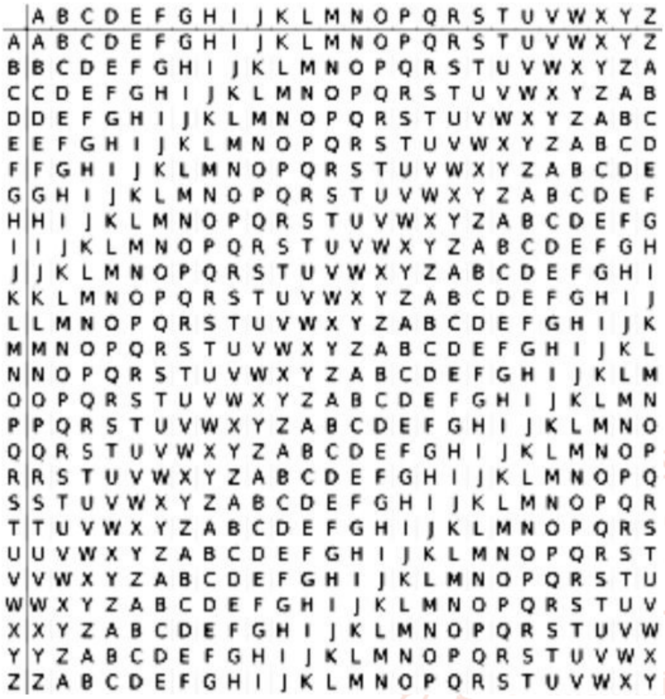
In this paper classical cipher is selected and implemented for safer communications. In classical methods, two basic techniques namely substitution and transposition are used. In substitution technique, letters of plaintext are replaced by numbers and symbols. This technique is further divided into Monoalphabetic and polyalphabetic cipher. In monoalphabetic [6] [1], it replaces each letter in the plaintext with another letter to form the ciphertext. The main problem with monoalphabetic substitution ciphers is that they are vulnerable to frequency analysis. However in polyalphabetic cipher, uses multiple substitution alphabets. That is a single character in the plaintext is changed to many characters in the cipher text. So it has the advantage of hiding the letter frequency. The best known and simplest of such polyalphabetic cipher algorithm is Vigenere cipher [1].

Vigenere cipher is one of the most popular ciphers in the past because of its simplicity and resistance to the frequency analysis test of letters that can crack simple ciphers like Caesar cipher. But with the increase in the cryptanalytic skills, Vigenere cipher is no longer taken as secure cipher and is not popularly used. The most weak point of Vigenere cipher is the use of repeated words that causes repetition of certain patterns in cipher texts at intervals equal to the length of the keyword used.

This paper is divided into following sections like, Section 2 introduce Vigenere cipher. Section 3 describes a proposed encryption method for cipher text using modified vigener cipher. Thus, the key-stream increases the tightness of security in Vigenere cipher as this makes the deciphering of the cipher text from the knowledge of the key length difficult. Implementation, generating session key and experimental results are given in section 4 and conclusions in section 5.

2. RELATED WORK

The Vigenere Cipher is an encryption scheme which was invented in the 16th century by French Blaise De Vigenere. The scheme is inspired by the Caesar Cipher in that it uses a “polyalphabetic substitution matrix” that combines two or more alphabetic tables. The Vigenere encryption [1] scheme relies on a keyword as its key along with the polyalphabetic substitution table to encode and decode a message. For instance, to encrypt the message using a Vigenère cipher table which is in fig1, by using the key will do the following; first the key is repeated sequentially until the length of the message and aligned together. Then the words are translated by locating the rows and columns of each position in the keyword and plaintext in polyalphabetic substitution table provided below to get the encrypted ciphertext. The same key is then used to decrypt the message to reveal the same message by using the reverse process [8].



	A	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	A	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
B	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
C	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	B
D	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
E	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	D
F	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
G	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	F
H	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
I	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	H
J	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
K	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	J
L	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
M	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	L
N	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
O	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	N
P	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
Q	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	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Fig1: Vigenere Table

3. Proposed Algorithm

In traditional Vigenere cipher each alphabet has one fixed numeric value but in our proposed technique we have eight tables shown in Table 1. 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:

Formula for encryption by proposed method is:

$$\mathbf{Ci = Pi + Ki \ (mod\ m)}$$

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

3.1 Encryption

1. 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.
2. Numeric value of first plain text character and key character will be added according to table 1.
3. 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.
4. Numeric value of second plain text character and key character will be added according to row 2.
5. 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.
6. 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.

3.2 Decryption

Decryption process of proposed approach works the same way as encryption does but in reverse direction. Formula for decryption by proposed method is:

$$\mathbf{Pi = Ci - Ki \ (mod\ m)}$$

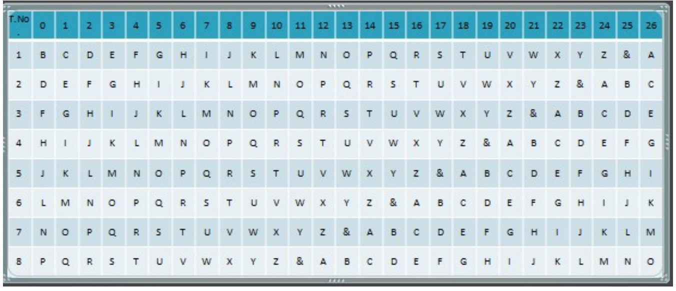
The steps for decryption process are:

1. Numeric value of first cipher text character and key character will be subtracted according to table 1
2. 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.
3. 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]

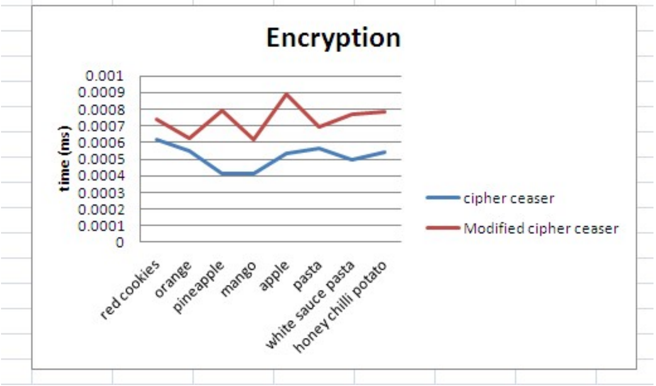
TABLE 1 PROPOSED TECHNIQUE TABLE



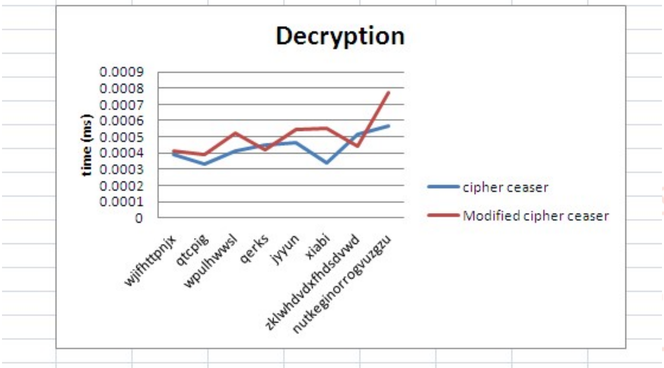
T.No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	&	A
2	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	&	A	B	C
3	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	&	A	B	C	D	E
4	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	&	A	B	C	D	E	F	G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

4. Result and Analysis

Encryption Time Graph



Decryption Time Graph



The modified cipher encryption method is considered to be secure to brute force attack, frequency attack, statistical attack and known cipher text attack, etc. Also this method is simple, robust and can encrypt /decrypt confidential data without losing any key (computational/operational) in seconds and does not suffer from any mathematical complexities.

5. CONCLUSION

Vigenere cipher regard as simplest and weakest method that mean it is very easy to detect by intruder. To overcome the limitations of this method, the proposed multilevel encryption scheme is used. Hence, the proposed algorithm becomes difficult to cryptanalyst. At the same time, the computational complexity is much lesser than most modern ciphers, making it a fit choice for light weight applications where resources are limited.

REFERENCES

[1] Stjepan Picek, Annelie Heuser, and Sylvain Guilley "Template attack vs bayes classifier. Technical", report, Cryptology ePrint Archive, Report 2017/531, 2017.

[2] Sengupta N, Holmes J, "Designing of cryptography based security system for cloud computing", International conference on cloud and ubiquitous computing and emerging technologies (CUBE), IEEE-2017.

[3] Al-Ahwal, A. and Farid, S., "The effect of varying key length on a Vigenère cipher", IOSR J. Comput. Eng., 17, 2, pp. 2278–661, 2017.

[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] S. Garg, S. Khera, and A. Aggarwal, "Extended Vigenere cipher with stream cipher. Int. J. Eng. Sci. Comput., 6, 5, 5176–5180 in 2016.

[6] Polyalphabetic Cipher Techniques Used For Encryption Purpose, http://www.ijarcsse.com/docs/papers/Volume_3/2_February2013/V3 I2-0122.pdf.

[7] Security Analysis and Modification of Classical Encryption Scheme by Maya Mohan, M. K. Kavitha Devi and V. Jeevan Prakash, I JST, Vol 8(S8), 542–548, April 2015.

[8] Security Models and Proof Strategies for Plaintext Aware Encryption.Journal of Cryptology by Birkett J, Dent AW.. 2014; 27(1):99–120.

[9] The security implementation of IPSec VPN [M] by CarIton R. Davis.

[10] http://www.webopedia.com/TERM/V/VPN.html

[11] Enhancing Security of Vigenere Cipher by Stream Cipher International Journal of Computer Applications by Fairouz Mushtaq Sher Ali, Falah Hassan Sarhan (0975 – 8887).

[12] Gerhana, Y. A., Insanudin, E., Syarifudin, U., and Zulmi, M. R. "Design of digital image application using vigenere cipher algorithm", 4th Int. Conf. Cyber IT Serv.Manag. CITSM 1–5, 2016.

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

[14] Quist-Aphetsi Kester," A Hybrid Cryptosystem Based on Vigenere Cipher and Columnar Transposition Cipher", International Journal of Advanced Technology and Engineering Research (IJATER) Vol. 3 Issue 1 pp141-147. July 2013.

[15] M. Khalid, N. Wadhwa, and V. Malhotra, "Alpha-qwerty cipher," International Journal of Advanced Computing, vol. 3, no 3, pp 107-118, May 2012.

[16] Q. A. Kester, "A hybrid cryptosystem based on Vigenère cipher and columnar transposition cipher", International Journal of Advanced Technology and Engineering Research, vol. 3, no. 1, pp. 141-147, Jan. 2017.

[17] Cryptology: From Caesar Ciphers to Public-Key Cryptosystems by Luciano, Dennis; Gordon Prichett (January 1987).. The College Mathematics Journal 18 (1): 2–17. Doi: 10.2307/2686311. JSTOR 2686311.

[18] http://en.wikipedia.org/wiki/Caesar_cipher Caesar cipher. Retrieved from

[19] A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security International Journal of Computer Applications by Gurpreet Singh, Supriya, (0975 – 8887).

[20] Luciano, Dennis; Gordon Prichett (January 1987). "Cryptology: From Caesar Ciphers to Public-Key

Cryptosystems". The College Mathematics Journal 18 (1): 2–17. doi:10.2307/2686311. JSTOR 2686311.

[21] A cryptosystem based on Vigenère cipher with varying key, by Q.- Kester, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), vol. 1, pp. pp: 108-113, 2012.

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

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

[24] Handbook of applied cryptography, by A.Menezes, P.van Oorschot, S. Vanstone, CRC Press, Inc., 1997.

[25] HMAC: Keyed-Hashing for Message Authentication, by H. Krawczyk, M. Bellare, and R. Canetti, Internet Engineering Task Force, Request for Comments (RFC) 2104, February 1997.