Publisher homepage: www.universepg.com, ISSN: 2663-7804 (Online) & 2663-7790 (Print)
https://doi.org/10.34104/ajeit.019.06013
Australian Journal of Engineering and Innovative Technology
Journal homepage: www.universepg.com/journal/ajeit

Hybridization of Vigenere Technique with the Collaboration of RSA for Secure Communication

Md. Tarequl Islam[1]* and Md. Selim Hossain[1]

[1]Department of Computer Science and Engineering, Khwaja Yunus Ali University, Sirajgonj, Bangladesh
*Correspondence: tareq.cse@gmail.com

ABSTRACT

The security factor is one of the major concerns in today's world. As security is the breath of communication, as much as we can make our communication system secure, the system will be more trustworthy and be more restricted to snap as well as can save guard from the unauthorized attempt. Either symmetric or asymmetric encryption was used in the earlier method to ensure data security. However, any of them alone makes the system either unsecured or time-consuming. In our thesis work, we have used both the techniques together to make the system as much as reliable and also to make it faster using the hybridization of asymmetric RSA encryption and symmetric modified vigenere technique. This hybridization method sends the vigenere table as an encrypted string using an asymmetric process with the collaboration of the RSA encryption algorithm where the string will be encrypted by the public key generated by the receiver. Later the string will be decrypted using the receiver's private key. Therefore, we can claim that the extended vigenere method with the collaboration of RSA makes the overall communication more secure, stable, reliable, and faster.

Keywords: Asymmetric, Cryptography, Poly-alphabetic, RSA, Information security, and Vigenere

INTRODUCTION

Cryptography is the system in which an algorithm is recycled to convert the information into an arrangement that is not readable to anyone except the sender and receiver who participate in this mechanism. The algorithm must be reliable, efficient and easy to understand by the sender and receiver involved in this communication system or encryption process (Saraswata *et al.*, 2016). Here we have used the asymmetric crypto technique RSA with an extended vigenere method to secure the information before transmit. In RSA methodology, every plaintext is encrypted by the receiver's public key and the encrypted ciphertext is decrypted by using the receiver's private key. As the private key does not participate in the transmission so there is no way to identify this private key by the intruder. However, RSA technique alone can make the system secure but slow in the process. To overcome the existing RSA problem we have proposed an extended vigenere based RSA technique to make the system reliable and faster. Here the **Fig 1** shows the overall encryption and decryption process of cryptography.

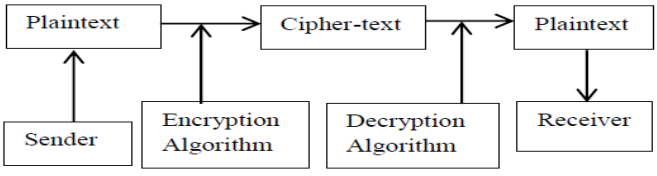


Fig 1: Process of encryption and decryption.

BACKGROUND AND RELATED WORKS

Various techniques are usually used to convert the original message into cipher-text (Nacira and Abdelaziz, 2004). Among them, the most commonly we are using to encrypt data and secure communication technique is the poly-alphabetic substitution technique which enables to provide more security. In this, a character or letter needs not to be replaced with the same character or letter for its occurrence in the whole message like a mono-alphabetic cipher technique. We propose a new table named modified vigenere table of the poly-alphabetic cipher method. In this proposed table we include the numbers, rare character along with the alphabets. Here, the alphabets (A-Z), the digits (0-9), space, rare characters are appended after the total alphabets with values 69. We take common value from the proposed vigenere table with the key addition by the sender and cipher-text will be generated using a modified vigenere table. The general formula of the above-specified process of encryption is C = (P+K) mod 69 (Nacira and Abdelaziz, 2004; Patni, 2013).

We have proposed a new vigenere table, the general formula for the above decryption process is as follows: P = ((C) - K) mod 69. In the modified vigenere cipher, most frequent letters are put first and then less frequent letters on both the column and row side. In our previous thesis paper (Hossain and Islam, 2018), we have an updated Vigenere table that consists of 69 rows and 69 columns. Here key space is 69! Which is over 1.7112245242×1098 (Menezes *et al.*, 1996; Senthil *et al.*, 2013). If eavesdropper can able to observe 1,000,000 keys per second, it would still need over 5.426×1072 trillion years to check all possible keys, so it is not a practical approach but it is indeed impossible to break the keys by brute force attack.

PROPOSED METHODOLOGIES

A. RSA Encryption for Vigenere Key

RSA Key generation (Public-Key Encryption): Individual entity creates an RSA public key and a corresponding private key. Each entity receiver (R) should do the following:

1. Generate two large random (and distinct) primes p and q, each roughly the same size.
2. Compute n = pq and φ = (p − 1)(q − 1).
3. Select a random integer e, 1 < e < φ, (gcd (φ, e)= 1)
4. Use the extended Euclidean algorithm to compute the unique integer d, φ > d > 1, such that (ed) mod φ = 1
5. R's public key is (n, e) and the private key is (n, d).

RSA Public-Key Encryption: Sender (S) encrypts a message m for R, which R decrypts by using the private key. For Encryption S should do the following:

a. Obtain R's authentic public key (n, e).
b. Represent the message as an integer m in the interval [0, n − 1].
c. Compute Cipher Text, $c = m^e \ mod \ n$.
d. Send the ciphertext S to R.

B. Encryption Algorithm for Plaintext

1) Pick two elements from plaintext message. If the numbers of elements are odd then space will be taken as one symbol.
2) Put one element in the horizontal axis and one element along the vertical axis of the proposed modified vigenere table.
3) Select the common element (cipher-text) that will be originated by putting the element horizontally and vertically.
4) Add key before the cipher-text that has been provided by the user on the row or column side of the modified vigenere table.
5) Repeat the overhead process for the next elements to get the cipher-text of the whole message.
6) Now, the ciphertext will be added by the hash value to create individual block cipher. Here the hash value is dependent on the previous hash value.

C. RSA Decryption for Vigenere Key

To recover plaintext m from ciphertext c, R should do the following:

Use the private key d to recover plain text $m = c^d mod \ n$.

D. Decryption Algorithm for Ciphertext

1) Pick two elements from the cipher-text.
2) Assign the first element is the key element by which we can identify the row or column to get a particular row or column from the modified vigenere table.

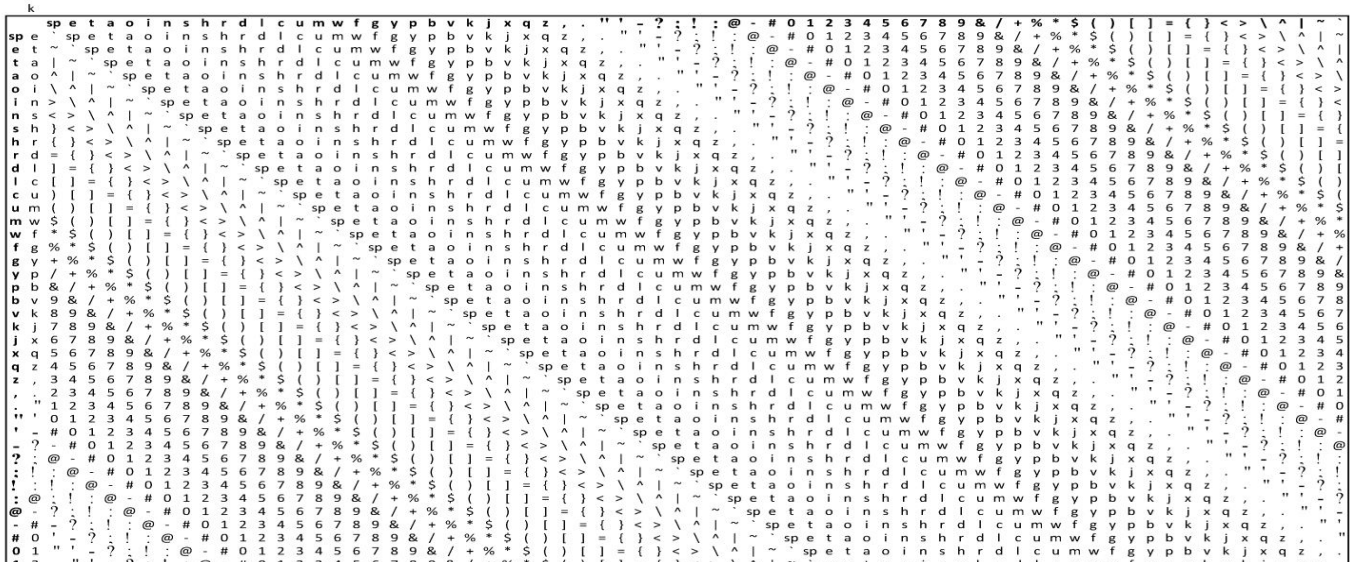
3) After assigning the key element in the row or column, we will then assign the common element by which we will get the original message by selecting the row and column elements.

E. Working Principle

In our extended vigenere technique (Hossain and Islam, 2018), we encrypt the plaintext by substituting symbols in the plain text by the symbols generated by vigenere Table 69×69. There are 69 rows and 69 columns of character symbols of symmetric sequence in both rows and columns. In the previous method, both the parties had to have the same vigenere table on hand prior to start the procedure (Hire, 2012; Digital Vision Ltd, 2001). Character symbols can be placed randomly with the fixed sequenced 69 characters in row-wise. By using key and vigenere table we generate ciphertext for the corresponding plaintext. In both, the parties should have the same table and key. In this research paper, we use the randomly generated sequence of rows and columns of 69 character symbols along with 69 random key spaces and the receiver doesn't have to have the vigenere table. In every aspect, we assemble randomly generate 69 character sequences and encrypt by RSA algorithm where receiver public key is used for encryption and the private key is used for decryption (Kester, 2013; Kester, 2012).

Sender then sends ciphertext of randomly generated character sequence and substituting cipher-text by vigenere table. Then the receiver receives the cipher-text which would be decrypted by private key first and generate corresponding vigenere table along with key space and substituting back to original plaintext by using generated vigenere table. In this method, the key space is 69!, and the random character symbol is also 69! Therefore, which are over $69! \times 69!$ If one can able to check 1,000,000 keys/sec, it would require over 9.2855×10^{164} trillion years to check all possible keys, so cryptanalysis by brute force is impossible.

Table 1: Modified Vigenere Tableau.



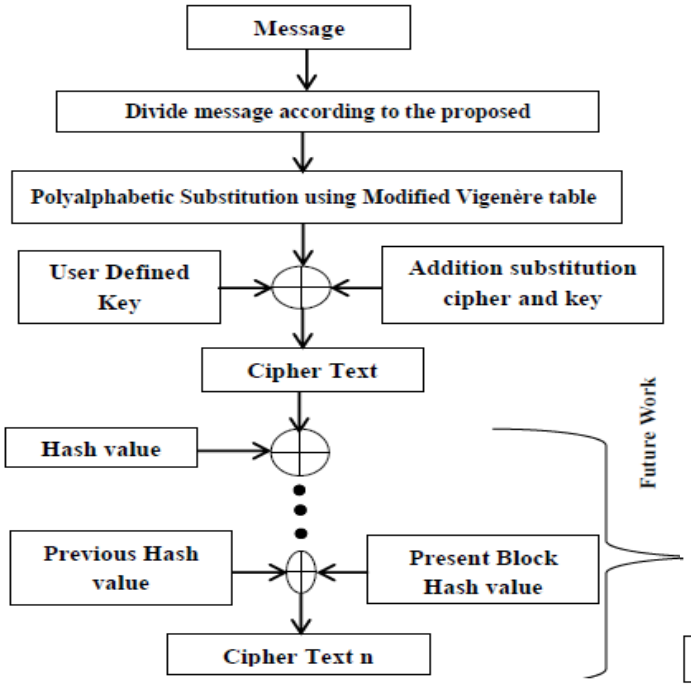


Fig 2: Block diagram of modified vigenere diagram.

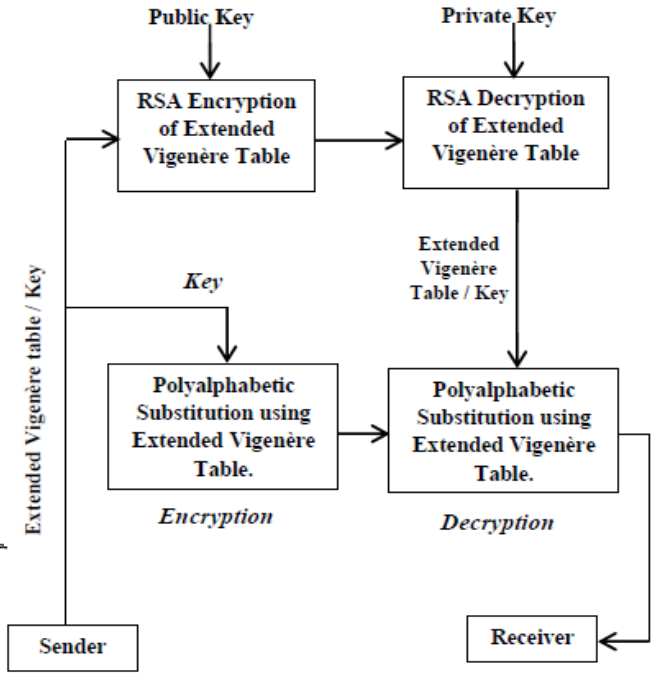


Fig 3: Block diagram of hybrid vigenere asymmetric encrypti.

Table 2: Character weight Mapping.

Character	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
Weight	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
Character	0	1	2	3	4	5	6	7	8	9	,	.	;	'	"	_	?	:	!	@	#	/	+	-	*	(
Weight	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52

Character	)	{	}	[	]	<	>	|	\	~	`	&	%	$	=	^	sp
Weight	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69

In this technique, the receiver generates two large prime numbers p and q. Depend on those prime numbers, the modulo factor n, φ, public key e, and private key d will be generated and will share the public key (n, e) to the sender. The sender will form a string of sequential characters from the randomly generated table. Every character will be mapped with the corresponding weight of integer value. All the weights will be encrypted by the public key. Encrypted weight will be converted into the binary form of x digit block. The block size is a receiver choice which depends on the large prime factor p and q [2x = pq]. Sender then sends this ciphertext (binary string) to the receiver. The receiver will decrypt the ciphertext and generate the original plain text. For decryption, the ciphertext is divided into blocks of length x and revert the binary value to an integer which will be decrypted using the receiver's private key. As an example, the receiver generates two prime numbers p=7, q=11 and compute e=17 and d=53 by using the RSA key generation algorithm and sends public key (n, e) = (77, 17) to sender. The sender generates random vigenere table which is formed as a character sequence according to the following observation.

cabefdighjklmonpqrtsu052134v96w87xzy,.;'_"?:!@#/ +-(*){[<}>]\~|`&$^=% and is mapped to the corresponding weight of the characters as:

3,1,2,5,6,4,9,8,7,10,11,12,13,15,14,16,17,18,20,19,21,
27,32,29,28,30,31,22,36,33,23,35,34,24,26,25,37,38,3
9,40,42,41,43,44,
45,46,47,48,49,50,52,51,53,54,56,58,55,59,57,61,62,6
3,64,66,68,67,65,69

Sender will encrypt each integer weight by RSA encryption algorithm $c = m^e \bmod n$. Therefore, the encrypted value is -

75,1,18,3,41,16,4,57,28,54,44,45,62,71,42,25,19,72,48
,24,21,69,65,50,63,46,26,22,64,66,67,7,34,40,38,9,60,
47,30,17,70,13,43,11,12,51,31,27,14,8,68,39,37,10,56,
53,55,5,29,52,6,35,15,33,73,23,32,20

Each encrypted integer is now converted as binary number of length x where x is the length of each binary number by using the formula $2^x = n$. Sender then sends these encrypted binary strings as cipher text to the receiver.

10010110000001001001000000110101001001000000
000
01110010011100011011001011000101101011111010
00111010101000110010010011100100001100000011
00000101011000101100000101100100111111010111
00011010 0010110 1000000 1000010
10000110000111010001001 01
0000100110
00010010111100010111100111100010001 10
00110000110101001 1 00010110001100
01100110011111
00110110001110000100010000100010011101001010
0001
01001110000110101011011100001010011101011010
00000110010001100011110100001100100100101110
1000000010100

The receiver will divide first the received binary string by x digits of the block, convert to decimal and decrypt each decimal integer by using the private key (n, d) = (77, 53) and the decryption formula $m = c^d \bmod n$. Then the receiver will get back to the character sequence of the vigenere table by replacing the weight value to the corresponding character. Finally, the receiver will generate same vigenere table which is used by the sender to encrypt the original plaintext and decrypt.

F. Mathematical Equation

It is proved that the quantity of information depends on the possibility of happening to those events. Let us consider, I is the quantity of information of a message m and P is the possibility of the incident of that event then mathematically, the relation between *I* and *P* will be,

$I = \log_2 (1/P)$.

In another way, we can say that the amount of information in a message is proportional to the time required to transmit the message. Now let us consider in mind that the possibility of endeavors of letters e and q in an English message is Pe and Pq respectively. We can explain it in the following way,

$Pe \geq Pq$

$\Rightarrow 1/Pe \leq 1/Pq$

$\Rightarrow \log_2 (1/Pe) \leq \log2 (1/Pq)$

$\Rightarrow Ie \leq Iq$

If the capacity of a channel is C then the time required to transmit e,

$Te = Ie/C$ ……. (1)

Similarly, the time required to transmit

$Tq = Iq/C$ ……. (2)

From the equation of (1), and (2) we get

$Ie/C \leq Iq/C$

$\Rightarrow Te \leq Tq$

$\therefore Te \leq Tq$

Now again we consider a ciphertext consists of length N, the period p, and I_c the index of coincidence,

$$p \approx \frac{N*0.027}{(N-1)*Ic+1-N*0.0145}$$

Let us consider that the texts start, we can define it by the following equation,

$$\sum_{\alpha=A}^{Z} M_{\alpha}^{(i)} = M$$

Where $M_{\alpha}^{(i)}$ denotes the number of occurrences of the letters in column i if the ciphertext were written in rows of length *p* and M is the number of rows [9].

The proof then starts, $2D_c = \sum_{i=1}^{p} \sum_{\alpha=A}^{Z} M_{\alpha}^{(i)} \left(M_{\alpha}^{(i)} - 1\right) + 2 \sum_{i=1}^{p} \sum_{j=i+1}^{p} \sum_{\alpha=A}^{Z} M_{\alpha}^{(i)} M_{\alpha}^{(j)}$

Where D_c is the number of pairs of equal letters in the cipher-text. We can further explain it by the following equation (Brassard, 2005).

$$2D_c \approx M^2 * p * 0.065 - pM + M^2 * 0.0145 * p\ (p-1)$$

RESULT AND DISCUSSION

Here the key will be provided according to the demand of the sender to the vigenere table to decrypt the encrypted message. Multiple substitutions of alphabets are found in poly alphabetic cipher. The Vigenère table that is our research topic is probably a well-known example of a poly alphabetic cipher.

The Enigma machine is more complex but is still fundamentally using poly alphabetic substitution cipher. An example has been given below to convert plain-text to cipher-text and cipher-text to plaintext by the following table using a modified vigenere table.

Table 3: Comparison of vigenere and proposed method.

Parameters	**Vigenere Method**	**Proposed Method**
Method	Vigenere	Proposed
Plaintext	n	n
Cipher-text	n	n/2
Key	n	n/2
Brute force attack	4.03×10^{26}	$1.7112245242\times10^{98}$
Cryptanalysis by Brute force (1,000,000 keys per second)	12 trillion years	9.2855×10^{164} trillion years
Arrangement of symbols	Alphabetic order	Random based order
Numbers of rows and columns	26/26	69/69

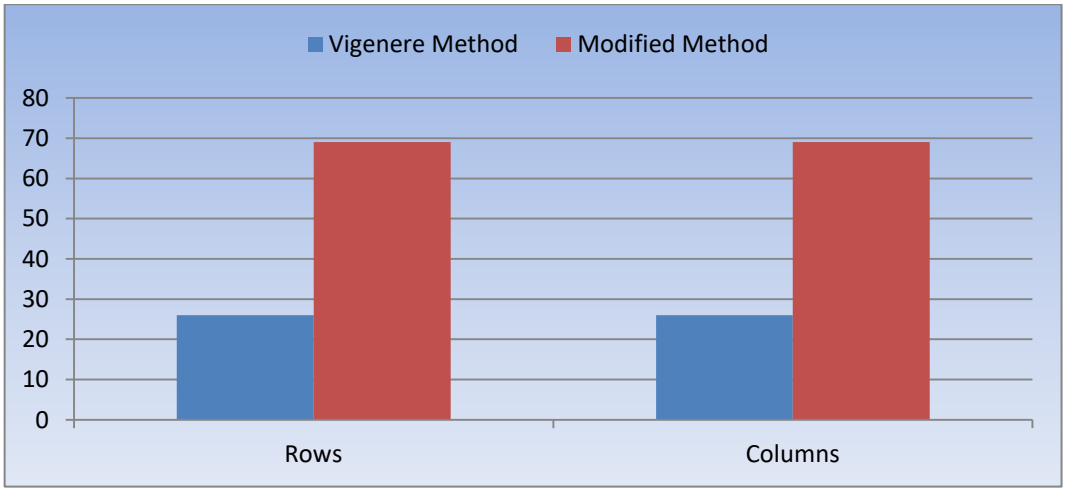


Fig 4: Rows and columns of vigenere and modified method.

Table 4: Example of encryption and decryption.

Plaintext	**Cryptography is the best method for the security of data**
Proposed algorithm	Cr yp to gr aphy is th e be st me th od fo r se cu ri ty of da ta
Cipher-text	u^ psp ae y{ ow rr ne ai t~ v9 h> w(rr ii g) d= h<usp d\ aw il l} asp
Minimum Cipher-text	u^ p ae y{ ow rr ne ai t~ v9 h> w(rr ii g) d= h< u d\ aw il l} a
Plaintext	Cryptography is the best method for the security of data

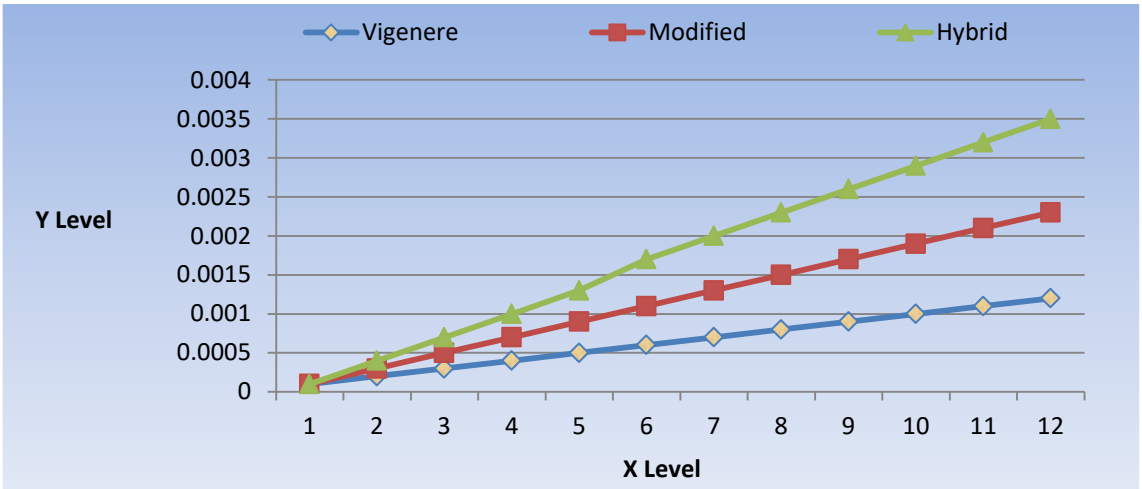


Fig 5: Cryptanalysis comparison by Brute force.

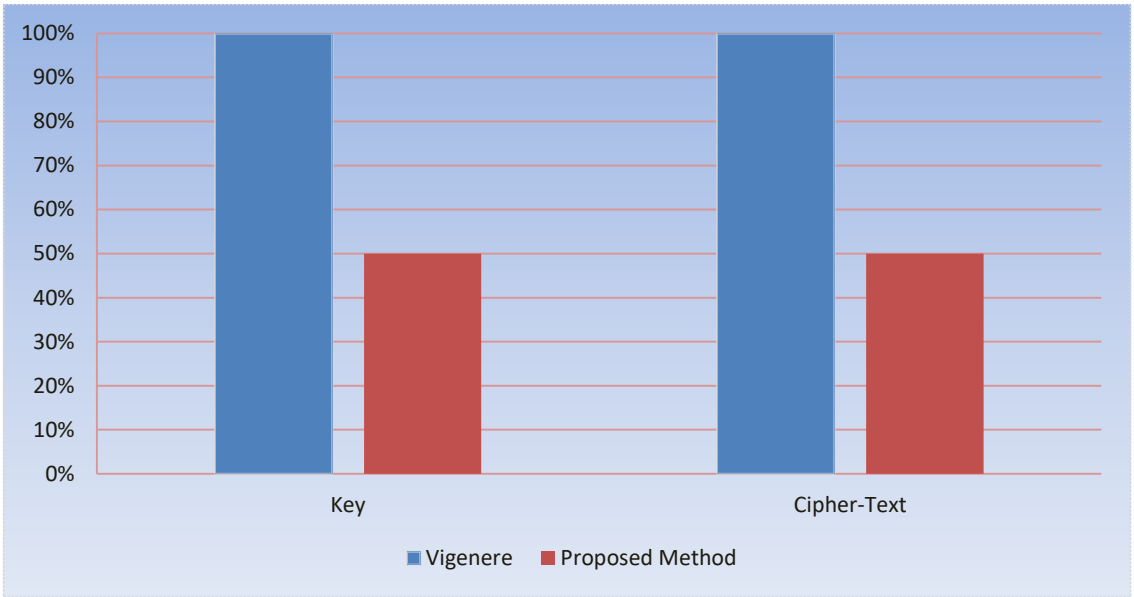


Fig 6: Cipher-text and key comparisons.

CONCLUSION AND FUTURE WORK

The above analysis and description depict that the vigenere table highlights on the poly alphabetic cipher technique. Our research is to extend the vigenere table by including the alphabets, digits, special and rare symbols in the proposed vigenere table as a result numbers, special and rare symbols will be encrypted by the process of proposed table as well as the number of randomly generated vigenere table will be large and almost unpredictable to intruders. It also reduces the sizes of cipher-text, keys and here symbols are arranged by increasing the numbers of rows and columns. In the previous proposal of our research paper was the symmetric key encryption process. To overcome this problem, we have made the proposal asymmetric by combing our previous proposed modified vigenere method with the RSA algorithm to ensure the security of communication to keep pace with the current world.

In the future, the concept of hash value based on block chain cryptography will be added with cipher-text to mark the procedure of cryptanalysis more complex.

ACKNOWLEDGEMENT:

Many thanks to the co-author supported with proper assistance and help for analysis and writing to conduct successful research study.

CONFLICTS OF INTEREST

The authors declare they have no competing interests with respect to the research.

REFERENCES

1) Brassard G., (2005) "Brief history of quantum cryptography: a personal perspective", IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, 16-19 Oct. 2005. https://doi.org/10.1109/ITWTPI.2005.1543949
2) Digital Vision Ltd, "IEEE POTENTIALS", February/March, 2001.
3) Hire D.N., (2012) "Secured Wireless Data Communication", *International J. of Computer Applications*, **54**(1), 272-277.
4) Hossain MS, and Islam MT, (2018) "An Extension of Vigenere Technique to Enhance the Security of Communication", *International Conference on Innovations in Science, Engineering and Technology* (ICISET), Chittagong, Bangladesh.
5) Islam KA, Deeba F, and Hassan MKA. (2019). Dust Ion Acoustic Solitary Waves in Multi-Ion Dusty Plasma System with Adiabatic Thermal Change, *Aust. J. Eng. Innov. Technol.*, **1**(5), 1-5. https://doi.org/10.34104/ajeit.019.0105
6) Kester Q. A., (2013) "A Hybrid Cryptosystem Based on Vigenère Cipher and Columnar Transposition Cipher", *International J. of Advanced Technology and Engineering Research (IJATER)*, **3** (1), 848-854.
7) Kester Q. A., (2012) "A cryptosystem based on Vigenère cipher with varying key", *International J. of Advanced Research in Computer Engineering & Technology (IJARCET)*, **1** (10), 1-6.
8) Lewand R. E., (2000) "Cryptological mathematics (mathematical association of America text books)", The Mathematical Association of America.
9) Menezes, Oorschot P. V., and Vanstone S., (1996) "Handbook of Applied Cryptography", CRC Press.
10) Nacira G. H., Abdelaziz A., (2004) "The θ-Vigenere Cipher Extended to Numerical Data", Proceedings of International Conference on Information and Communication Technologies.
11) Omran S. S., Al-Khalid A. S., and Al-Saady D. M., (2011) "A Cryptanalytic Attack on Vigenère Cipher Using Genetic Algorithm", IEEE Conference on Open System, September 25-28, Langkawl, Malaysia.
12) Patni P., (2013) "A Poly-alphabetic Approach to Caesar Cipher Algorithm", *International J. of Computer Science and Information Technologies*, **4** (6), 954-959. http://ijcsit.com/docs/Volume%204/Vol4Issue6/ijcsit2013040647.pdf
13) Saraswata, Khatria C., Sudhakara, Thakrala P., Biswasa P., (2016) "An Extended Hybridization of Vigenere and Caesar Cipher Techniques for Secure Communication." 2nd International Conference on Intelligent Computing, Communication and Convergence, ICCC-2016.
14) Senthil K., Prasanthi K. and Rajaram R., (2013) "A Modern Avatar of Julius Ceasar and Vigenere Cipher", IEEE International Conference on Computational Intelligence and Computing Research.
15) Stallings W., (2005) "Cryptography and Network Security", Prentice Hall, November 16.

Citation: Islam MT and Hossain MS. (2019). Hybridization of vigenere technique with the collaboration of RSA for secure communication, *Aust. J. Eng. Innov. Technol.*, **1**(6), 6-13.
https://doi.org/10.34104/ajeit.019.06013