# Vigenere Cipher with dynamic Vigenere table - Digenere Cipher

Gurwinder Kaur[1], Harshdeep Trehan[2], Dr. Naveen Dhillon[3]
[1]*Research Scholar, Ramgarhia Institute of Engineering and Technology, Phagwara*
[2]*Assistant Professor, Ramgarhia Institute of Engineering and Technology, Phagwara*
[3]*Principal, Ramgarhia Institute of Engineering and Technology, Phagwara*
*(E-mail: gurwinderk807@gmail.com)*

***Abstract*—** Cryptography is the science of converting a clear message into an isolated "nonreadable message," where the message is encrypted on the sender side and decrypted on the receiver side. It is a current research domain at the juncture as it can be crucial to protecting incredibly delicate and undercover records from illicit misdeeds throughout the dispatch over the network. In this paper, the Vigenère cipher utilizes a 95 X 95 Vigenère table with a-to-Z alphabets and special symbols while designing a new way of executing the Vigenère cipher encryption algorithm by automatically altering the Vigenère table after each encryption phase. A cipher established on the traditional Vigenère method is not secure, whereas we can see that the above-proposed cipher has an amplified degree of security.

***Keywords*—***Encryption; Vigenere cipher; Cryptography; Data security;*

## I. INTRODUCTION

Cryptography is a Greek word that means secret writing. Today this term refers to the science and art of converting messages to make them unassailable and unsusceptible to attacks [1]. For security and privacy, we ought to encrypt the message on the sender side and decrypt it on the receiver side. The term Plaintext in cryptography is used for the actual message to be transformed through the cryptography function. On the other hand, the message which has been transformed is called Cipher text. An encryption algorithm is a procedure that works with a key to convert the Plaintext into cipher text. The decryption algorithm operates reversely and converts the Ciphertext into Plaintext [2].

The core of cryptographic operations is cryptographic keys. A key is a piece of variable data used in conjunction with a cryptographic algorithm to execute its operations such as encryption, decryption, or signing and verification in such a way that an entity with the details of the key can imitate or reverse the procedure. However, an entity without a key cannot decipher. In a well-designed cryptographic scheme, the assurance of the algorithm depends only on the security of the keys used [2].

Classification of Cryptography

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

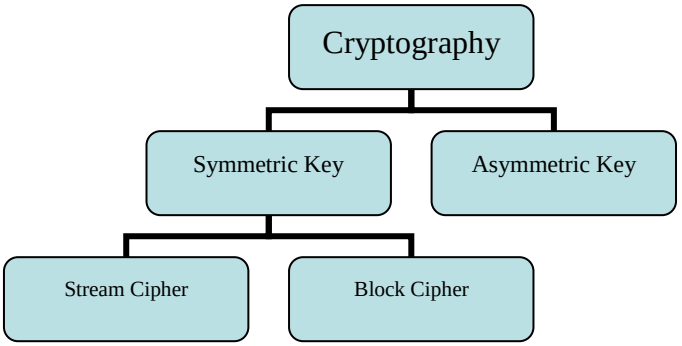


Fig. 1

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

(i) Stream Cipher: Stream cipher operates on a single bit, and each binary digit in the data stream is passed through the cryptographic algorithm independently [10]. The stream cipher is an important class of symmetric ciphers used widely in encryption for hardware-based cryptographic systems. They are simple and efficient without compromising performance [11].

(ii) Block Cipher: In block cipher, a cryptographic key and algorithm are applied to the block of data instead of a single bit in the 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 as public-key cryptography. This type of cryptography uses asymmetric algorithms that encrypt and decrypt with different keys in which the public key is used for encryption, and the private key is used for decryption [3]. Asymmetric algorithms are very slow in working, and it is unfeasible to use them to encrypt huge data.

Vigenere Cipher: Vigenère cipher is an algorithm designed for a long time and is included in the class of classic algorithms because it operates on a character scale instead of bits and has a simple encryption and decryption calculation process. Nevertheless, the Vigenere cipher can be categorized as a

modern cryptographic algorithm if the encryption and decryption process is carried out using the XOR technique to operate on a bit scale. Although simple, this algorithm is quite safe, and because of its simplicity, the Vigenère cipher algorithm is an algorithm that is very light in terms of algorithm complexity, so this algorithm only requires a tiny share of computing aids and time for the encryption and decryption process. In the encryption and decryption process, the algorithm Vigenere cipher requires an encoding table that will encode every character of plain text and ciphertext, and based on this table, the encryption and decryption process is carried out with a predetermined key. One of the disadvantages of the Vigenere cipher algorithm is that the encoding table is easy to guess. The encoding table is arranged in sequential order so that eavesdroppers will easily know or guess the encoding table's arrangement. Therefore, if the encryption and decryption keys fall into the hands of the eavesdropper, the eavesdropper can be sure of decrypting the ciphertext back into plain text.

For this reason, this study will investigate how to scramble the encoding table with completely randomized randomization so that if the key falls into the hands of eavesdroppers, the confidentiality of the message can still be maintained. Vigenère cipher is also one of the symmetric algorithms with the same encryption and decryption key so that it is like an algorithm another symmetric. One of the other weaknesses of the Vigenère cipher algorithm is the key distribution problem. It means that the Vigenere cipher has a problem with how to send the decryption encryption key completely securely. There is no truly secure way to distribute the key from a sender to a receiver so that recipients can decrypt the ciphertext [4].

## II. RELATED WORK

C.R.S Bhardwaj (2012) proposed two modifications to the traditional Vigenere cipher. First, the encryption key must be any character, for example, mathematical symbols (+,-,*,/,%), numbers (0,1...9), or punctuations instead of characters. Second, an arbitrary number is introduced as the key to spreading the spectrum so that only experts can understand the message [5]. Khalid et al. (2012) extended the original Vigenere table to 92 characters. It includes 66 additional characters to the original table and redesigned the mapping structure for characters. Though it includes a large character set and introduces case sensitivity to the encryption process, it still suffers from encrypting the space, single quote, and backslash because they are not part of the table [6]. Kester (2013) proposed algorithm first applies the columnar transposition technique to re-arrange the plain text along with the keyword and then applies Vigenere cipher to produce output cipher text [7]. Senthil et al. (2013) presented an algorithm that uses the prime number, its primitive roots, and their generator to bring some addition to the Vigenere cipher and Julies Caesar cipher techniques. The shift and substitution method produces the cipher text [8]. Fairouz et al. (2014) proposed an algorithm that applies some complex transformations to generate the cipher text. It applies the substitution technique on even location characters and transposition techniques to the odd position characters. The summation of the numeric value of even location characters and keys produces the cipher characters for even locations where odd location character treats as separately. They generate a random number for odd locations for the key and convert both numeric values to the ASCII equivalent. Both ASCII equivalent is transformed into binary equivalent and performs exclusive or operation on them. The resultant binary number converts to the equivalent ASCII, then back to the character to generate the odd position cipher characters [14].

Omolara et al. (2014) presented a method that applies to Caesar and Vigenere cipher using two keys: Numbered and a lettered key. Caesar cipher applies a key: Lettered key, which uses a shift of the numbered key. Then, the plain text applies the Vigenere cipher with a new key. The binary value of cipher is Exclusive-ORed with the key: Numbered key. The resultant Exclusive-ORed value is converted back to its ASCII value and then to the character to produce the final output cipher text [15]. Nishith and Kishore (2014) proposed algorithm requires two keys and uses substitution and transposition techniques. First, it applies a Vigenere cipher using the first key. Then columnar transposition technique applies twice on the plain text, which is the resultant cipher text of the previous step [16]. Aized et al. (2016) proposed a technique that employs multiple tables, and each alphabet has more than one numeric value. The proposed algorithm was developed for 27 characters. The extra character is a space denoted by the character "&" [17]. Aditi et al., (2016) presented an algorithm that is a mixture of Vigenere and Caesar cipher. Keywords and message letters are represented by the initial rows and columns of the table. First, pick a keyword character and its corresponding plain text character as a row and column-wise and get the intersection entry of the row (key) and column (plain text) index. Add 3 to the entry value to produce the cipher text. The size of the character set is 36. The additional characters are numeric value (0-9) [18]. Deepanshu et al. (2018) proposed algorithm is a mixture of the Vigenere cipher and Modified Caesar cipher technique based on 36 characters. They include numbers (0-9) in the original tables. The initial row and column represent the keyword and plain text characters, respectively. The intersection entry of the key (row) and plain text (column) characters is added to the key value (called Ukey) to produce the cipher character [19]. This study shows that various methods have been proposed but still suffer from some shortcomings. Partha Chakraborty et al. enlarge character sets by working with more characters so that the proposed 95 × 95 Vigenere table includes the maximum number of characters and extends the original Vigenere table to cover all characters increasing the difficulty level of cracking the algorithm [20].

## III. PROPOSED APPROACH

In the traditional Vigenere cipher, a static Vigenere table is used to map the equivalent value to char. However, in our technique, the Vigenere table is rotated after the encryption of each character in the plaintext. Each character of plaintext and key has been assigned a specific number concerning the Vigenere table.

### *A. Encryption*

- Repeat the key until the key length is less than the length of the plaintext.

- Initialize a variable i = 1 and repeat steps 3 to 7 until i is less than or equal to the length of the plaintext.
- Read ith char in the plain text message (P) and convert it to its numeric equivalent in the assignment table.
- Read the ith char in the key (K) and convert it to its numeric equivalent in the assignment table.
- Add the numeric equivalent of the plain text (P) to the numeric equivalent of the key (K) alphabet.
- Takes modulo 95 on the sum derived from the previous step and translates numeric equivalent back to the corresponding alphabet in the assignment table, which is the output cipher text(C).
- Circular left-shift the assignment table and increment i by 1.

*B. Decryption*

- Repeat the key until the key length is less than the length of the ciphertext.
- Initialize a variable i = 1 and repeat steps 3 to 7 until i is less than or equal to the length of the ciphertext
- Read ith char in the cipher text message (C) and convert it to its numeric equivalent in the assignment table.
- Read the ith char in the key (K) and convert it to its numeric equivalent in the assignment table.
- Subtract the numeric equivalent of the cipher text (C) alphabet to the numeric equivalent of the key (K) alphabet.
- Add 95 to subtraction if the result is less than 0
- Takes modulo 95 on the subtraction derived from the previous step and translates numeric equivalent back to the corresponding alphabet in the assignment table, which is the plain text message.
- Circular left-shift the assignment table and increment i by 1.

## IV. EXPERIMENTAL RESULTS AND DISCUSSION

To examine the proposed encryption and decryption algorithm, we consider the Plain text message: I love my country and the keyword: India. The generation of output ciphertext and plaintext is given below:

*A. Encryption*

**Plaintext:** I love my country

**Keyword:** India

**Ciphertext:** Qf!*^ha8+Ka%`85k)

*B. Decryption*

**Ciphertext:** Qf!*^ha8+Ka%`85k)

**Keyword:** India

**Plaintext:** I love my country

| Char | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Numeric Equivalent | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| Char | U | V | W | X | Y | Z | a | b | c | d | e | f | g | h | i | j | k | l | m | n |
| Numeric Equivalent | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 |
| Char | o | p | q | r | s | t | u | v | w | x | y | z | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Numeric Equivalent | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 | 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 |
| Char | 8 | 9 | ~ | ` | ! | @ | # | $ | % | ^ | & | * | ( | ) | - | _ | + | = | { | } |
| Numeric Equivalent | 60 | 61 | 62 | 63 | 64 | 65 | 66 | 67 | 68 | 69 | 70 | 71 | 72 | 73 | 74 | 75 | 76 | 77 | 78 | 79 |
| Char | [ | ] | \| | \ | : | ; | “ | ‘ | | < | > | , | . | ? | / | | | | | |
| Numeric Equivalent | 80 | 81 | 82 | 83 | 84 | 85 | 86 | 87 | 88 | 89 | 90 | 91 | 92 | 93 | 94 | | | | | |

Table 1. Extended Vigenere table with numeric equivalent

| Plaintext (P) | I | | l | o | v | e | | m | y | | c | o | u | n | t | r | y |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Numeric Equivalent | 8 | 87 | 35 | 37 | 43 | 25 | 82 | 31 | 42 | 79 | 18 | 29 | 34 | 26 | 31 | 28 | 34 |
| Keyword (K) | I | n | d | i | a | I | n | d | i | a | I | n | d | i | a | I | n |
| Numeric Equivalent | 8 | 38 | 27 | 31 | 22 | 3 | 33 | 22 | 26 | 17 | 93 | 28 | 17 | 21 | 12 | 88 | 23 |
| Sum%95 $(P_i+K_i)\%95$ | 16 | 30 | 62 | 68 | 65 | 28 | 20 | 53 | 68 | 1 | 16 | 57 | 51 | 47 | 43 | 21 | 57 |
| Ciphertext (C) | Q | f | ! | * | ^ | h | a | 8 | + | K | a | % | ` | 8 | 5 | k | ) |

Table 2. Encryption process

| Ciphertext (C) | Q | f | ! | * | ^ | h | a | 8 | + | K | a | % | ` | 8 | 5 | k | ) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Numeric Equivalent | 16 | 30 | 62 | 68 | 65 | 28 | 20 | 53 | 68 | 1 | 16 | 57 | 51 | 47 | 43 | 21 | 57 |
| Keyword (K) | I | n | d | i | a | I | n | d | i | a | I | n | d | i | a | I | n |
| Numeric Equivalent | 8 | 38 | 27 | 31 | 22 | 3 | 33 | 22 | 26 | 17 | 93 | 28 | 17 | 21 | 12 | 88 | 23 |
| Sub%95 $(C_i-K_i)\%95$ | 8 | 87 | 35 | 37 | 43 | 25 | 82 | 31 | 42 | 79 | 18 | 29 | 34 | 26 | 31 | 28 | 34 |
| Plaintext (P) | I | | l | o | v | e | | m | y | | c | o | u | n | t | r | y |

Table 3. Decryption process

Now, we generate some cipher text that uses the same plain text with different keys and different plaintext with identical keys based on our presented algorithm:

| | **Plaintext(P)** | **Keyword(K)** | **Ciphertext(C)** |
|---|---|---|---|
| Different keys on the same plaintext | I love my country | India | Qf!*^ha8+Ka%`85k) |
| | | india | qf!*^7a8+K0%`85~) |
| | | INDIA | QFmtrhAiy}aqlifkv |
| Same key on the different plaintexts | I love my country | India | Qf!*^ha8+Ka%`85k) |
| | I Love My Country | | Qfm*^hai+KA%`85k) |
| | I LOVE MY COUNTRY | | QfmtrHaiyKAqlifKv |

Table 4. Avalanche Effect

We applied the proposed algorithm on different plaintexts with the same key and the same plaintext with different keys. It is effortlessly seen from above table 4 that with a slight change in the plaintext or key, the proposed algorithm shows a tremendous avalanche effect.

## V. CONCLUSION

This research paper concluded that the security and privacy through the Vigenere cipher could be increased by adding complex functions. The extended Vigenere table makes it impossible to carry credential harvesting attacks like brute force and others on the Vigenere cipher. By integrating a

simple circular left rotation function into the Vigenere cipher, its performance has increased enormously. A more complex mathematical function can be counted to the cipher to supplement its complexity and performance in the future.

## VI. REFERENCES


[1] Menezes A. J., Oorschot P. C. and Vanstone S. A. handbook of applied cryptography, CRC Press, 1996.

[2] Stalling W. "Network Security Essentials (Applications and Standards)", Pearson Education, 2004.

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

[4] Agung Purnomo Sidik, International Journal of Basic and Applied Science 10 (2) 2021

[5] C. R. S. Bhardwaj, "Modification of Vigenère Cipher by Random Numbers,Punctuations & Mathematical Symbols," IOSR Journal of Computer Engineering (IOSRJCE), vol. IV, no. 2, pp. 35-38, Sep.-Oct 2012.

[6] Neeta Wadhwa and Vaibhav Malhotra Md. Khalid Imam Rahmani, "ALPHA-QWERTY CIPHER: AN EXTENDED VIGENÈRE CIPHER," Advanced Computing: An International Journal ( ACIJ ), vol. 3, no. 3, May 2012.

[7] Quist-Aphetsi Kester, "A HYBRID CRYPTOSYSTEM BASED ON VIGENÈRE CIPHER AND COLUMNAR TRANSPOSITION CIPHER," International Journal of Advanced Technology & Engineering Research (IJATER), vol. 3, no. 1, January 2013.

[8] K.Prasanthi and R.Rajaram K.Senthil, "A Modern Avatar of Julius Ceasar and Vigenere Cipher," in IEEE International Conference on Computational Intelligence and Computing Research, 2013.

[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] Fairouz Mushtaq Sher Ali and Falah Hassan Sarhan, "Enhancing Security of Vigenere Cipher by Stream Cipher," International Journal of Computer Applications (0975 – 8887), vol. 100, no. 1, August 2014.

[15] A.I. Oludare and S.E. Abdulahi O.E. Omolara, "Developing a Modified Hybrid Caesar Cipher and Vigenere Cipher for Secure Data Communication," Computer Engineering and Intelligent Systems, vol. 5, no. 5, 2014.

[16] Nishith Sinha and Kishore Bhamidipati, "Improving Security of Vigenère Cipher by Double Columnar Transposition," International Journal of Computer Applications (0975 – 8887), vol. 100, no. 14, August 2014.

[17] Irfan Riaz and Umair Rasheed Aized Amin Soofi, "An Enhanced Vigenere Cipher For Data Security," INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH, vol. 5, no. 3, March 2016.

[18] Chahat Khatria, Sudhakara, Prateek Thakrala and Prantik Biswasa Aditi Saraswata, "An Extended Hybridization of Vigenere and Caesar Cipher Techniques for Secure Communication," in 2nd International Conference on Intelligent Computing, Communication & Convergence (ICCC-2016), Bhubaneswar, Odisha, India., 2016, pp. 355-360.

[19] Chandan Agrawal, Parth Sharma, Munish Mehta and Poonam Saini Deepanshu Gauta, "An Enhanced Cipher Technique using Vigenere and Modified Caesar Cipher," in 2nd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 2018.

[20] Khairun Nahar and Partha Chakraborty "A Modified Version of Vigenere Cipher using 95 × 95 Table" International Journal of Engineering and Advanced Technology (IJEAT)