IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

A NEW MODIFIED ALGORITHM BASED ON CAESAR CIPHER CRYPTOGRAPHY FOR HINDI VERNACULAR LANGUAGE

[1]Varun L. Sahni, [2]Dr. Shrikant Mapari

[1]Student, [2]Assistant Professor

Symbiosis Institute of Computer Studies and Research, Pune, Maharashtra 411016

Abstract: Cryptography is the oldest technique to make information secure from any type of cyber-attack like DDoS, DoS, Man in the Middle Attack etc. In this paper, we have discussed about the Cryptography and its type and how existing Caesar Cipher work. Here we have proposed an algorithm based on the Caesar Cipher to encrypt the Hindi language. The propose algorithm has implemented through setting up an experiment. This proposed algorithm works on the Hindi Vernacular Language. It uses a random Shift key generation algorithm to Encrypt the message, which is randomly generated into range of **1 to 10^{50}.** The same random generated Shift algorithm will be use to decrypt the message. At the time of encryption random generated key will be displayed to the user and it used to generate Cipher text. The generated Cipher text will be sent to the receiver along with key through secure medium.

***IndexTerms*: Encryption, Decryption, Symmetric Cryptography, Caesar Cipher Text**

1. Introduction

Cryptography is a technology that stores information and communicates using codes so targeted people can understand and use it. Therefore, to stop unauthorized access to information. The prefix "crypt" means "hidden" and also the principle "graffiti" means "writing". (KOTHARI, n.d.)

Types of Cryptography

The Figure. 1.1 shows the two different types of cryptography named as “Symmetric Key Cryptography” and “Asymmetric Key Cryptography”. These two types are explained as follows:

Cryptography Classification:

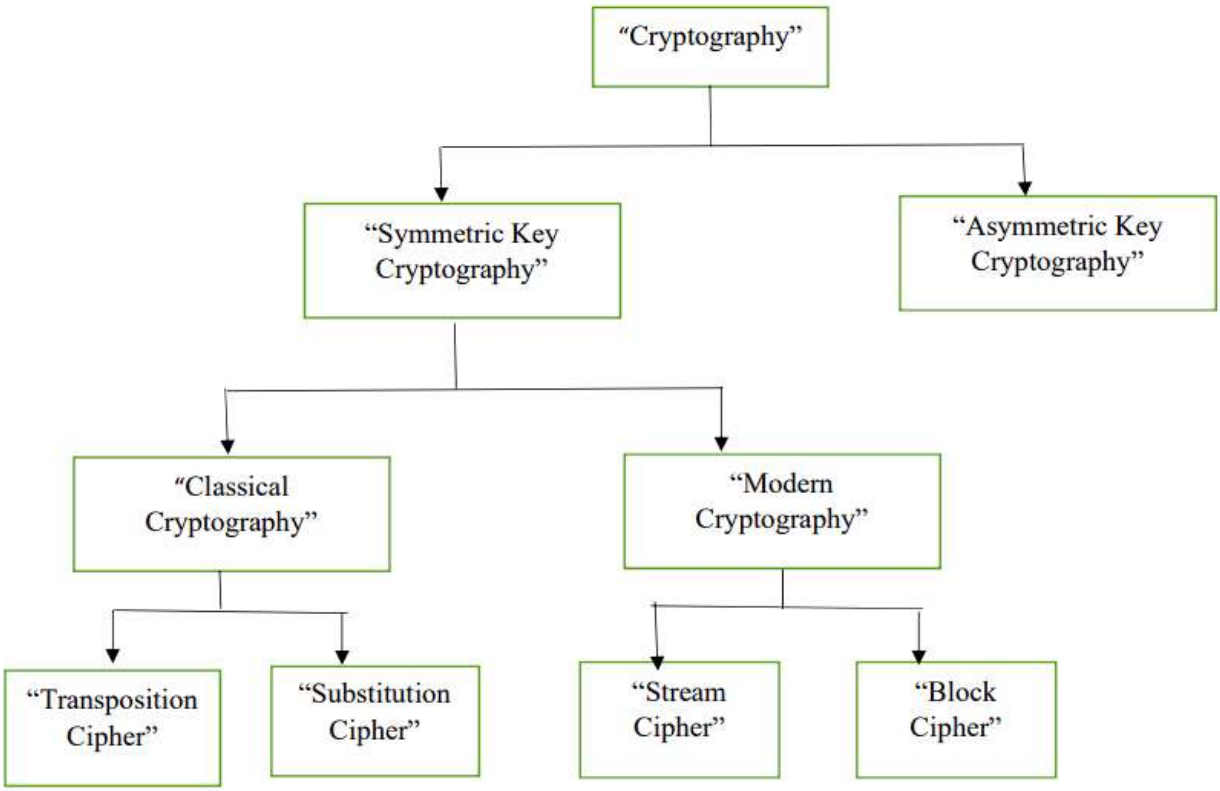

Figure 1.1

Symmetric Key Cryptography

Encryption is a simple key sharing system used by the sender and receiver to encrypt and express the message. The most popular symmetric key system is Data Encryption Standard (DES). Process of Symmetric Key Cryptography is given in Figure 1.2.

Figure 1.2

Transposition Cipher

Transposition cipher is a method of encryption in which the cipher text contains a permutation of plain text. It is the one of method of cryptography, which convert unit of plain text (usually a letter or a group of letters) in to a simple system as shown in Figure. 1.3

Plaintext = MEET ME AFTER PARTY Keyword=421635

'1'	'2'	'3'	'4'	'5'	'6'
'M'	'E'	'E'	'T'	'M'	'E'
'A'	'F'	'T'	'E'	'R'	'P'
'A'	R'	'T'	'Y'		

'4'	'2'	'1'	'6'	'3'	'5'
'T'	'E'	'M'	'E'	'E'	'M'
'E'	'F'	'A'	'P'	'T'	'R'
'Y'	'R'	'A'		'T'	

Figure 1.3

Substitution Cipher

The method of encrypting any unit of plain text with cipher text, according to the fixed system, is that the unit can be a single letter (most common), a pair of letters, a triplet of letters, a mixture of the above, and so forth.

For Example:

Plaintext:

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Keyword:

ZEBRAS

Cipher Text:

ZEBRASCDFGHIJKLMNOPQTUVWXY

Caesar Cipher

This is the first method of message encryption, which is Substitution cipher. In this the plain text is shifted three times to encrypt the message and both the sender and the receiver share the same shift.

Encryption = (Index + shift) mod 26 [In case of English language]

Decryption = (Index – shift) mod 26 [In case of English language]

Asymmetric Key Cryptography

Also known as public key cryptography, this is any cryptography system that uses paired keys, which is the public key, the most common and the only private key known by the owner. It achieves the authenticity of two functions, in which the attached private key holder sends the message and encrypted, where the private key holder can interpret the message with public key and public key encryption, and anyone can encrypt the message using the recipient. The encrypted message can only be defined with the private key of the recipient

Stream cipher

An asymmetric or secret-key encryption algorithm that encrypts one bit at the identical time as stream ciphers, encrypts the identical text (bit or byte) to different text (bit or byte) every time. Process of Stream Cipher given in Figure 1.4

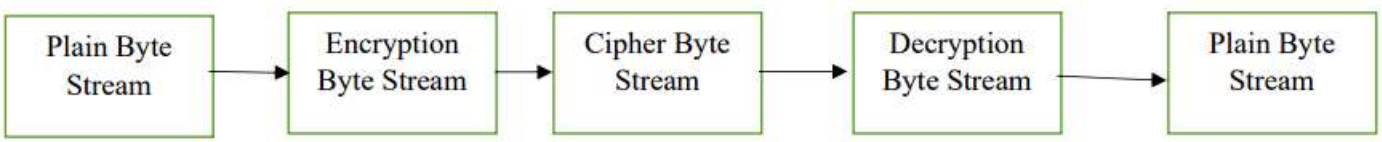

Figure 1.4

Block Cipher

Block cipher is an encryption method that applies a deterministic algorithm for a symmetric key to encrypt a block of text, instead of encrypting a bit into a stream cipher.

2. Existing work

In existing Caesar Cipher Cryptography, a plain text is shifted three time from the index of the alphabetical order, where sender and receiver both will use same common key or shift to encrypt and decrypt the message. (Benni Purnama, 2015)

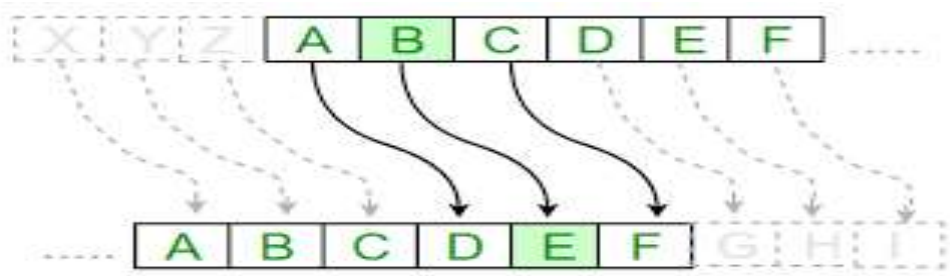

Figure 2.1 (Adapted from [https://www.geeksforgeeks.org/caesar-cipher-in-cryptography/]).

In above Figure 2.1 first sequence displays the plain text and the second sequence displays the cipher text. In which A becomes D and B becomes E and so forth.

Encryption = [Index + Shift] mod 26

Decryption = [Index – Shift] mod 26

Implementation done so far

- This algorithm is designed to prevent the discovery of correct information and this algorithm is known as privacy protection mining algorithm. (Anand Sharma, 2010)
- In this modified algorithm, the alphabet is split into two parts, and the voices are replaced with the alphabetic tone, and the consonants are replaced with the consonant alphabet.
  The drawback is that some alphabetic consonants cannot be replaced, as the alphabet is rarely used in Indonesian text. And a cipher that can read test results obtained by the algorithm. (Benni Purnama, 2015)
- This algorithm is designed to make e-passports more secure and is denoted by a symbol. It contains a small chip that stores the passport holder's data. The data has been protected widely by using the cryptography. This paper does the comparison between modular multiplication methods, which has been used for the RSA algorithm of the 1024-bit key length. **Jilinx ISE** 14.3 for targeting the **Virtax-5 FPGA** board for encrypting and decrypting the platform used. (Shruti Sharma, 2016)
- Class Ancient scientific cryptography Scissor Caesar cipher. In the Caesar cipher algorithm, the position of the initial character is changed, also known as the ROT algorithm. The main goal is to strengthen the security of the data used in the Caesar cipher algorithm combination for encryption and decryption algorithms, while the three-pass protocol is used to send the process. In this research we can send messages without sharing the encryption keys with another person and this change makes the Caesar cipher algorithm more secure (Boni Oktaviana, 2016)

3. Proposed Work

In this modified implementation of Caesar Cipher algorithm our Indian National language has been used for encryption and decryption of message. As most of the government work and circular are passed in Hindi Vernacular language and any message to be share with military official Hindi Vernacular language is use.

This modification is done by keeping the national language in mind and theory of Caesar Cipher which was established in early 2000s. This algorithm detects the vowels (**स्वर**) as well as the sign (**मात्रा**) because in Hindi language these two things together make one word (**अक्षर**) so this modified algorithm very smoothly detect vowels as well as sign and encrypt the message with the shift of random generated key. This algorithm takes the random value to encrypt them and the same random generated value is to be used at time of decryption.

Frequency of Hindi Vernacular Language

In Below Figure 3.1, Frequency graph gives the idea of occurrence of the letters in words. (Atish Jain, 2015)

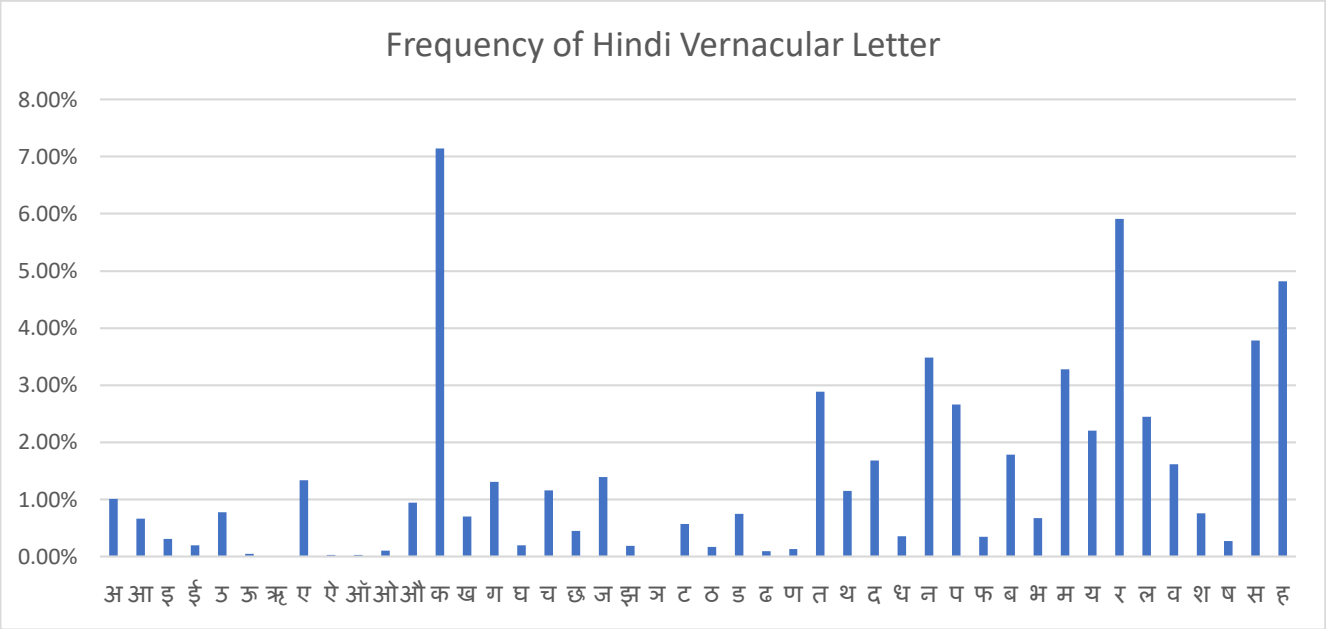

Figure 3.1

Generation of random shift

In this whole algorithm the most important part is generation of a random shift. Algorithm to generate random shift is given below.

- Importing the inbuilt package called **random** in case of python.
- Creation of **n** variable and declaring the last value of range using **pow ()** in case of python.
- Creation of **Shift** variable in which the range is declared using **random.randint()** in case of python.

Proposed Algorithm

Pseudo Code of this Algorithm

Encryption Side

1. Taking User Input
2. If message is blank again ask for input
3. If message is in Hindi Vernacular form it will encrypt else no encryption only original text will display
4. After taking input from user it will generate the random shift or key from range if **1 to 10^{50}** and encrypt the text.
5. Final Cipher text will be generated.

Decryption side

1. Final output of encryption side will be input of Decryption side
2. It will ask to the decryption key or shift
3. Final decrypted text will be displayed.

Implementation Details

Figure 3.2 includes all the important aspects of the algorithm and flow structure.

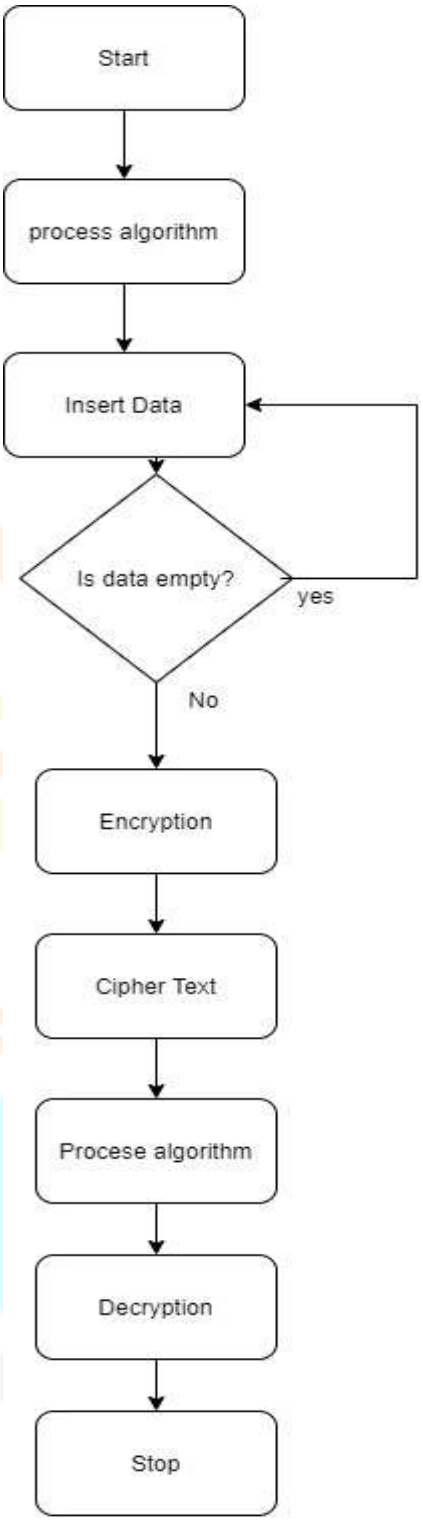

Figure 3.2

During time of processing the plain Hindi Vernacular text is encrypted into cipher text and this algorithm is smoothly encrypting and decrypting the Hindi Vernacular language. After entering the Hindi Vernacular text, a random Shifts or Key will be generated to start the Encryption process. (Sarthak Agrawal, 2018)

This algorithm has been implemented on a number of different data like Plaintext, pdf, Word file, Excel file varying types of content sizes of a wide range. But it results only to plaintext on Hindi Vernacular language.

4. Result

- **Encryption Side**

Text which needs to Encrypted is "मेरा नाम वरूण है " (branah.com, n.d.)

```
Enter Text in hindi vernicular?मेरा नाम वरूण है
Shift Key: 14653504935089090676018533818201074904065417168 58
orignal Text:मेरा नाम वरूण है
Encrypted Text: थ ◌ा ध ै ठ ै थ प ध ◌: छ म ि
```

Figure 4.1

In figure 4.1 shift key is randomly generated and the Encrypted text which is the Caesar Cipher text. This same Encrypted text will be the input of the Decryption side.

- **Decryption Side**

```
Enter Encrypted Text in hindi vernicular?थ ◌ा ध ै ठ ै थ प ध ◌: छ म ि

Enter the Shift Key to decrypt the
Message14653504935089090676018533818201074904065417168 58
Encrypted Text:थ ◌ा ध ै ठ ै थ प ध ◌: छ म ि
Decrypted text: म े र ◌ा न ◌ा म व र ू ण ह ै
```

Figure 4.2

In figure 4.2 the result is been decrypted in the form of list so each character is separated in the result. And, the shift key is need to be the same because of the random generation of shift key it is impossible to break the text.

5. Conclusion

The most important feature of this algorithm is that it is practically impossible to break the encryption algorithm without knowing the shift or key because it is generated randomly and the range of the random number is from **1 to 10^{50}**. The proposed algorithm can apply to both encryption and decryption by sending a shift or key to the sender by sending a secret message and using a secure path to the receiver.

References

Anand Sharma, V. O. (2010). IMPLEMENTATION OF CRYPTOGRAPHY FOR PRIVACY PRESERVING DATA MINING . *International Journal of Database Management Systems*.

Atish Jain, R. D. (2015). Enhancing the Security of Caesar Cipher Substitution. *International Journal of Computer Applications* .

Benni Purnama, H. R. (2015). A New Modified Caesar Cipher Cryptography Method With Legible. *International Conference on Computer Science and Computational Intelligence*.

Boni Oktaviana, A. P. (2016). Three-Pass Protocol Implementation in Caesar Cipher Classic. *IOSR Journal of Computer Engineering*.

branah.com. (n.d.). *Hindi Keyboard - हिंदी कीबोर्ड*. Retrieved from Branah: https://www.branah.com/

KOTHARI, J. (n.d.). *Cryptography and its Types*. Retrieved from Geeks for Geeks: https://www.geeksforgeeks.org/cryptography-and-its-types/

Sarthak Agrawal, P. V. (2018). AN UPGRADED SYMMETRIC KEY CRYPTOGRAPHY ALGORITHM. *ResearchGate*.

Shruti Sharma, H. Z. (2016). Implementation of cryptography algorithm for E-passport security. *International Conference on Inventive Computation Technologies* .