An innovative Enciphering Scheme based on Caesar Cipher

Sharad Kumar Verma[1], Dr. D.B. Ojha[2]

[1]Research Scholar, Department of CSE,
MEWAR University, Rajasthan, India

[2]Director Research
MEWAR University, Rajasthan, India

Abstract

Cryptography is used in various areas because we know that the network is not secure at all. We use electronic transactions everywhere and send the important data via network, so there is a need to secure these data from intruders. There are many algorithms developed so far but all of them has some or the other limitations. This research paper provides a new and innovative way of securing the data and removing the limitations of the traditional algorithms which provides data security. This algorithm has used the concept of Caesar cipher and improved it to become more secure. It takes lesser time in ciphering and deciphering process and provides stronger algorithm of security developed so far.

Keywords: *Cryptography, network, intruders, electronic transaction, cipher.*

1. Introduction

Cryptography (or cryptology; from Greek κρυπτός, kryptos, "hidden, secret"; and γράφω, gráphō, "I write", or -λογία, -logia, respectively) is the practice and study of hiding information. In modern times cryptography is considered a branch of both mathematics and computer science and is affiliated closely with information theory, computer security and engineering.

Until modern times cryptography was referred almost exclusively to encryption, which is the process of converting ordinary information (plaintext) into unintelligible gibberish (i.e., ciphertext).[3] Decryption is the reverse, in other words, moving from the unintelligible ciphertext back to plaintext. [1] A cipher (or cypher) is a pair of algorithms which create the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and in each instance by a key. [3]This is a secret parameter (ideally known only to the communicants) for a specific message exchange context. Keys are important, as ciphers without variable keys are trivially breakable and therefore less than useful for most purposes. Historically, ciphers were often used directly for encryption or decryption without additional procedures such as authentication or integrity checks.

One of the simplest examples of a substitution cipher is the Caesar cipher, which is said to have been used by Julius Caesar to communicate with his army. [4] Caesar is considered to be one of the first persons to have ever employed encryption for the sake of securing messages. Caesar decided that each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a shift of 3, A would be replaced by D, B would become E, and so on. Caesar cipher, also known as a Caesar's cipher, the shift cipher, Caesar's code or Caesar shift.

Example

The transformation can be represented by aligning two alphabets; the cipher alphabet is the plain alphabet rotated left or right by some number of positions. For instance, here is a Caesar cipher using a left rotation of three places (the shift parameter, here 3, is used as the key):

Plaintext:	RETURN TO HOME
Ciphertext:	UHWXUA WR KRPH

When encrypting, a person looks up each letter of the message in the "plain" line and writes down the corresponding letter in the "cipher" line. Deciphering is done in reverse.

Ciphertext:	UHWXUA WR KRPH
Plaintext:	RETURN TO HOME

The encryption can also be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,..., Z = 25.[1] Encryption of a letter *x* by a shift *n* can be described mathematically as,[2]

$$E_n(x) = (x + n) \bmod 26$$

The most pressing weakness of this cipher is simplicity of its encryption and decryption algorithms; the system can be deciphered without knowing the encryption key. [3]It is easily broken by reversing encryption process with simple shift of alphabet ordering Decryption is performed similarly,

$$D_n(x) = (x - n) \bmod 26$$

(There are different definitions for the modulo operation. In the above, the result is in the range 0...25. I.e., if x+n or x-n are not in the range 0...25, we have to subtract or add 26.)

The replacement remains the same throughout the message, so the cipher is classed as a type of monoalphabetic substitution, as opposed to polyalphabetic substitution.

Another security concern is that, if how one letter should be deciphered is already known, then the shift can be determine and decipher the entire message. A better approach would be to make use of statistical data about English letter frequencies. Correcting these weaknesses of the Caesar cipher so it becomes unbreakable using existing methods, is the reason for this paper.

2. Our Approach (Sharad Cipher)

To encrypt a message, Sharad Cipher requires plaintext, initial encryption key and location of spaces in the plaintext in the form of integer values. The initial encryption key is an integer value and it determines location of alphabet to be used for substitution in the beginning. It is based on modulo twenty six arithmetic to ensure that integer value wraps round incase encryption key supplied is more than twenty six. Encryption will start with initial encryption key by using Caesar Cipher scheme when a space occur its checks for the location value and treat this location value as cipher key and then each alphabet in the plaintext is substituted by an alphabet obtained by incrementing with the cipher key till the next space reached and space location in the plaintext is replaced by the alphabet of current cipher key value. Again when a space will come then find the location of that space and now this location value will treat as cipher key and then each alphabet in the plaintext is replaced by an alphabet cipher key positions down the alphabet till the next space and space location in the plaintext is replaced by the alphabet of current cipher key value and so on. This process will continue until the entire plaintext is not converted into ciphertext. In this cipher the encryption key will not be fixed. It will always change when a space occurs and it depends on the location of space in the given plaintext.

Decryption follows reverse operations performed during encryption. It requires decryption key, space delimited integer value(s), counter and of course the encrypted text. The decryption key will be obtained by complimenting encryption key so that reverse character substitution can be achieved. Initialization of counter takes place with the beginning of decryption till the counter matches with space locator, it generates the plain text with required space and the cipher key will be replaced by the complemented counter value. Initial value of counter is zero. Each time when an alphabet decrypts, the counter will increase by one. Ciphertext cannot be decrypted without integer values representing space locations in plaintext, encryption key and the Sharad Cipher algorithm.

Example

Suppose the plaintext is “Hello Sharad Kumar Verma”. First set the initial cipher key value and then find the locations of spaces.

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**
0	1	2	3	4	5	6	7	8	9
K	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**
10	11	12	13	14	15	16	17	18	19
U	**V**	**W**	**X**	**Y**	**Z**				
20	21	22	23	24	25				

Perform Encryption:

Initial Cipher Key: 3

Space Locator: 5 12 18

Plaintext: HELLO SHARAD KUMAR VERMA

Ciphertext: KHOORFXMFWFIMWGYMDSNWJER

Perform Decryption:

Initial Cipher Key: 3

Counter: 0

Space Locator: 5 12 18

Ciphertext: KHOORFXMFWFIMWGYMDSNWJER

Plaintext: HELLO SHARAD KUMAR VERMA

We have already discussed that ciphertext cannot be decrypted without integer values representing space locations in plaintext, encryption key, counter and the Sharad Cipher algorithm. For example if we want to decrypt ciphertext without knowing the space locations then the generated plaintext will not be the original message.

Initial Cipher Key: 3

Ciphertext: KHOORFXMFWFIMWGYMDSNWJER

Plaintext: HELLOCUJCTCFJTDVJAPKTGBO

In this case we never get the original message as it is. So we can say that the Sharad Cipher is much more than the Caesar Cipher.

3. Conclusion

As stated earlier, Caesar cipher simply shifts encrypted character by number of positions specified while leaving spaces in between words of sentence. Our algorithm works with the locations of space and the cipher key. In this cipher the encryption key is not fixed. It is always change when a space occurs and it depends on the location of space in the given plaintext. So it is not easy to hack the encryption key. Ciphertext cannot be decrypted without integer values representing space locations in plaintext, encryption key and counter value. This research paper provides a new and innovative way of securing the data and removing the limitations of the Caesar Cipher algorithms which provides data security.

References

[1] 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.

[2] Wobst, Reinhard (2001). *Cryptology Unlocked*. Wiley. p. 19. ISBN 978-0-470-06064-3.

[3] http://www.math.uic.edu/CryptoClubProject/CCpacket.pdf

[4] http://en.wikipedia. org/wiki/Caesar_cipher, Caesar Cipher