IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 3, Ver. V (May-Jun. 2014), PP 01-05
www.iosrjournals.org

Enhancement Caesar Cipher for Better Security

Programmer Enas Ismael Imran[1,] Programmer Farah abdulameerabdulkareem[2]
Baghdad University-College of Education for Women-Computer Dept.

Abstract: *Cryptography is an art and science of converting original message into non readable form. Fast progression of digital data exchange in electronic way, information security is becoming much more important in data storage and transmission. Cryptography has come up as a solution which plays a vital role in information security system against malicious attacks. In this project, encryption will be implemented information that makes it hard to be readable and secure. For that matter, encryption method known as Caesar cipher, one of the simplest and most widely used encryption techniques. In this encryption, it uses the three methods in which each letter in the plaintext is replaced by some fixed number of position down the alphabet. The result from this project is a data which is encrypted and be decrypted to its readable form. As a conclusion, Caesar cipher algorithm can be implemented in many encryption projects to make data secure and better.*

Keywords:*Cryptography, Encryption, Decryption, Plaintext, Ciphertext*

I. Introduction

Security is one of the important aspects in computing. In data transfer,security must be considered as one of the method implemented to ensure secure data transfer. Data transfer is transferring information from a location or host to another host, or server. To have a secure data transfer, few method can be applied, and one of them is encryption of data, prepare it to be transferred in encrypted way and decrypted when the data want to be used.

As the importance and the value of exchanged data over the Internet or other media types are increasing, the search for the best solution to offer the necessary protection against the data thieves' attacks along with providing these services under timely manner is one of the most active subjects in the security related communities. The primary goal of any system is that the data cannot be modified by any external user or intruder [1]. To avoid such a type of situation convert data into a non readable form at sender side and convert that data in readable form again at receiver side. The technique and science of creating non readable data or cipher so that only authorized person is only able to read the data is called Cryptograph [2].It is the art and science of protecting information from undesirable individuals by converting it into a form non-recognizable by its attackers while stored and transmitted [3]. In Cryptography, Caesar cipher is one of the most widely known encryption decryption algorithm. Caesar cipher is a type of substitution type cipher in this kind of cipher each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. The encryption is represented using modular arithmetic [4].

Some of important definition in cryptography science

- Data security- how to prevent someone else from knowing the contents of a message while it is
being transmitted.
- Encryption - transform information into a different,unintelligible form.
- Decryption - restore the original information from theencrypted form.
- Plaintext - original data.
- Ciphertext - encrypted data.
- Cryptanalysis -techniques for deciphering a message without knowledge of the enciphering details.
- Cryptology- areas of cryptography and cryptanalysis.

II. Objective

The objectives of the research are to:
i. Implement three methods of encryption using Caesar Cipher algorithm.
ii. Develop a prototype that helps to test the output from the encryption process.
iii. To compare the propose encryption method with Caesar Cipher.
iv. Create strong encryption by using the different algorithm.

III. Scope

L Caesar cipher algorithm is applied to increase the strength of security.
ii. Create encryption and decryption method for the propose encryption.

IV. Cryptography

Cryptology is not a new; it has existed for more than 2000 years. The word cryptology is derived from two Greek words: kryptos, which means "hidden or secret and graphein" (to write), is the art and science of making communication unintelligible to all except the intended recipients [5]. In the language of cryptography, the message one intends to send is called the plaintext while the message that is actually sent is called the cipher text. Ciphers make textual communication a mystery to anyone who might unduly intercept it. Hence, a cipher is a method used to encode characters to hide their values. Cipher is employed in design of cryptosystem. A cryptosystem is a system, method, or process that is used to provide encryption and decryption [6]. There are two main categories of cryptography depending on the type of security keys used to encrypt/decrypt the data. These two categories are: Asymmetric and Symmetric encryption techniques.

4.1 Symmetric Encryption

When same key is used to encrypt and decrypt the message then it is known as symmetrical key cryptography. It is also known as private key cryptography; users have the provision to update the keys and use them to derive the sub keys. It is much effective and fast approach as compared to asymmetrical key cryptography. In symmetrical key cryptography; key has been generated by the encryption algorithm and then send it to the receiver section and decryption takes place [7, 8]. There are few challenges in the technique; the key should be transmitted over the secure channel from sender to receiver. The point is that if the secure channel already exits then transmit the data over the same channel, what is the need of encryption in such case. Practically no secured channel exits therefore key has been transmitted along the data which increases the overheads and effective bandwidth gets reduced. Secondly, the channel noise put harm to the key and data during the transmission [3].

4.2 Asymmetric Encryption

It is also called as public key cryptography. It uses two keys:
public key, which is known to the public, used for encryption and private key, which is known only to the user of that key, used for decryption. The public and the private keys are related to each other by any mathematical means. In other words, data encrypted by one public key can be encrypted only by itscorresponding private key [9].

This capability surmounts the symmetric encryption problem of managing secret keys. But on the other hand, this unique feature of public key encryption makes it mathematically more prone to attacks. Moreover, asymmetric encryption techniques are almost 1000 times slower than symmetric techniques, because they require more computational processing power [10].

There are two techniques for converting data into non readable form:

1. Transposition technique
2. Substitution technique.

Caesar cipher is an example of substitution method [11].

V. Why do we need cryptography?

Cryptography is defined as "the science or study of the techniques of secret writing, esp. code and cipher systems, methods, and the like." Cryptography is needed so that text can be kept secret. It is easy to imagine situations in ancient times where a writer who sent a message via courier would want to make sure that if the runner were intercepted, the interceptors could not read the message. Cryptography and encryption have been particularly important throughout history in times of war when a general would not want the enemy to figure out the plans he was distributing among his troops. Recently, the uses of cryptography have grown drastically. Cryptography is still important in times of war, but with the advent of computers and with it the vast amount of information being shared on the internet, there has been a need to create better, more efficient encryption strategies to protect private information, such as credit card numbers, private communications, and so on[12].

VI. Cryptographic systems are characterized by:

1. The type of operations used for transforming plaintext to ciphertext (substitution, transposition). Fundamental requirement - no information be lost.
2. The number of keys used (1 key - symmetric, single-key, secret-key; 2 keys – asymmetric, two-key, public-key).
3. The way in which the plaintext is processed (block cipher, stream cipher). Stream cipher may be viewed as a block cipher with block size equal to 1 element [13].

VII. CaesarCipher

Caesar cipher is an example of substitution method [11]. It is said to have been used by Julius Caesar to communicate with his army. Caesar is considered to be one of the first persons to have ever employed encryption for the sake ofsecuring messages. Caesar decided that shifting each letter three places down the alphabet in the message would be his standard algorithm, and so he informed all of his generals of his decision, and was then able to send them securedmessages.

One of the strengths of the Caesar cipher is its ease of use and this ease of use would be important for Caesar since his soldiers were likely uneducated and not capable of using a complicated coding system. Further enhancement to original three places shifting ofcharacter in Caesar cipher uses modulo twenty six arithmetic for encryption key that is greater than twenty six[14].

In cryptography, a Caesar cipher, also known as a Caesar's cipher or the shift cipher or Caesar's code or Caesar shift, is one of the simplest and basic known encryption techniques.

It is a type of replace cipher in which each letter in the plaintext is replaced by a letter with a fixed position separated by a numerical value used as a "key".

Caesar Cipher is or was probably the very first encryption methodology[15].

VIII. The Cryptographer’s Suggestion to Increase the Security of a Message

The more secure you want your messages to be, the more frequent you have to change the secret key.

For instance, during World War 2 the Germans changed the keys of their Enigma encryption machine multiple times a day to ensure secure communication. Even these days, cryptographers follow the principle that it is more important to keep the key secret than which cryptosystem you use. For example, it was more important for the Germans to keep the used Enigma keys secret than the usage of the Enigma machine as a cryptosystem. In fact, the wondrous Enigma machine was known in detail before the beginning of World War 2. Full credit goes to the brilliant British mathematician Alan Turing and his team who cracked the Enigma at Bletchley Park, England in 1940 which, according to some historians, might have ended the war earlier.

Consequently, in order to vary the secret keys and thus gain security, we will not limit ourselves to Caesar’s 3-letter-shift preference. We will allow any number of left or right shifts as a secret key and classify them as a Caesar Cipher, in respect for Gaius Julius Caesar [16].

IX. ProposedAlgorithms

To encrypt a text proposed algorithm requires Text and encryption key. The encryption key is an integer value and it determines alphabet to be used for substitution. It is based on modulo twenty six arithmetic to ensure that integer value wraps round in case encryption key supplied is more than twenty six. Decryption follows reverse operations per Formed during the process of encryption. It requires decryption key, and encrypted text. The decryption key should be complement to the encryption key so that reverse character substitution can be achieved. As stated earlier, Caesar cipher simply shifts encrypted character by number of positions. In this paper we can use three methods, where key size isfixed. First method is depend on the address of message, second depend on the length of first word in message and third method is depend on number of words in first line. Furthermore, the characters of the encrypted text are scrambled in such a way that if an attempt is made to decrypt the cipher text it would not be easy to decrypt the text.

9.1 Encryption Algorithm

Step1: Take the plain text as input.
Step2: Use the key with one of the methods which I mentioned earlier.
Step3: Get the encrypted text.

9.2 Decryption Algorithm

Step 1: Insert cipher text.
Step2: insertthe key depend on one of the methods which I mentioned earlier.
Step 3: Get the plain text
.

X. Cryptography of Caesar Ciphers

Proper Definition of the Encryption Function of the Caesar Cipher:

The Encryption Function of the Caesar Cipher is **F: P → C = P+3 MOD 26,**
where C and P are the integers from 0 to 25.

What does modular arithmetic (MOD) mean for our Caesar Cipher?

1) Since our alphabet consists of 26 letters we use the modulus 26. This can be viewed as a clock that holds 26 hours (just like the Caesar disk)
2) The number of turns on the Caesar disk which are congruent MOD 26 produce the same cipher letter.

Here is the key for a simple substitution cipher:
Plaintext letters: abcdefghijklmnopqrstuvwxyz
Ciphertext letters: YNROTKMCPBDVXZALEWUSFQJHGI
Could you remember the plaintext/ciphertext correspondences? Probably not; you would probably need a written copy of the key. But, having a written copy of the key could lead to problems with key security – the key might be lost or stolen. It is desirable to have a key that need not be written down. (Of course a person who has memorized the key might be coerced to give it up, but that it a different story.)
Caesar's cipher, to which reference was made in the David Kahn quote at the beginning of this section, was a simple substitution cipher, but it had a memorable key. For Caesar's cipher, "letters were replaced by letters standing three place further down the alphabet " Here is the key to Caesar's cipher:
Plaintext letters **ABCDEFGHIJKLMNOPQRSTUVWXYZ**
Ciphertextletters **DEFGHIJKLMNOPQRSTUVWXYZABC**
The key can be memorized because there is a pattern to it , the ciphertext alphabet is just the plaintext alphabet shifted to the right three places and sender and receiver just need to remember the shift.
Of course, other shifts could be used. All such shift, or translation, ciphers are now usually called Caesar ciphers. Here is the plaintext/ciphertext correspondence for a Caesar cipher depend on address of message, if the message contain an address we just account the number of words in address of message.

Example:
A: Encryption
Step 1: Suppose that address of message is **Baghdad the Beautiful city**
Step 2: Now apply Caesar cipher to encrypt the plain text. Shifting the key by four depend on number of words in address.
Plaintext**Baghdad the Beautiful city**
Ciphertext**Feklhehxlifieyxmjypgmxc**
Where **ciphertext= plaintext +4 mod 26**

B:Decryption
If we know the key we can decrypt the ciphertext to plaintext, as we mentioned in the first method the key here is four depend on address of message.
Ciphertext**Feklhehxlifieyxmjypgmxc**
Plaintext **Baghdad the Beautiful city**
The second method is depending on the length of first word in message.

Example:
A: Encryption
Step 1: Suppose original message is **Baghdad the Beautiful city**
Step 2: Now apply Caesar cipher to encrypt the plain text. Shifting the key by seven depend on number of character in first word (Baghdad).
Plaintext **Baghdad the Beautiful city**
Ciphertext**Ihnokhkaolilhbapmbsjpaf**
Where **ciphertext= plaintext +7 mod 26**

B: Decryption
If we know the key we can decrypt the ciphertext to plaintext, as we mentioned in the second method the key here is seven depend on number of character in first word.
Ciphertext**Ihnokhkaolilhbapmbsjpaf**
Plaintext **Baghdad the Beautiful city**
The third method isdepend on number of words in first line

Example:
A: Encryption
Step 1: Suppose original message is **Baghdad the Beautiful city in iraq**
Step 2: Now apply Caesar cipher to encrypt the plain text. Shifting the key by six depend on number of words in first line.

Plaintext **Baghdad the Beautiful city in iraq**
Ciphertext**hgmnjgjznkhkgazolarioaeotoxgw**
Where **ciphertext= plaintext +6 mod 26**

B: Decryption

If we k now the key we can decrypt the ciphertext to plaintext, as we mentioned in the third method the key here is six depend on number of words in first line .

Ciphertext**hgmnjgjznkhkgazolarioaeotoxgw**
Plaintext **Baghdad the Beautiful city in iraq**

For each of these ciphers, the method of encryption is the Caesar cipher (which is a special case of the simple substitution cipher) and the key is the shift. At the end,we note thatencryptionis changingdepending on theinput key.

XI. Conclusion And Scope Of Future Work.

In this paper we have shown that Caesar cipher being one of the simplest and widely used encryption techniques can be fortified beyond what common Caesar cipher algorithm can achieve. Many methods are used for Security purpose based on Caesar cipher algorithms. In our future work we can use various types of keys in one method also we can add more algorithms to enhance the security.

Reference

[1]. SomdipDey, JoyshreeNath and AshokeNath, “An Advanced Combined Symmetric Key Cryptographic Method using Bit Manipulation, Bit Reversal, Modified Caesar Cipher (SD-REE), DJSA method, TTJSA method: SJA-I Algorithm”, International Journal of Computer Applications (IJCA). Vol. 46, No. 20. Pp. 46-53, May, 2012.

[2]. Gaurav Sharma, Ajay Kakkar, "Cryptography Algorithms and approaches used for data security”, International Journal of Scientific & Engineering Research Vol. 3, Issue 6, 2012.

[3]. Hamdan.O.Alanazi, B.B.Zaidan and A.A.Zaidan, “New Comparative Study Between DES, 3DES and AES within Nine Factors”, JOURNAL OF COMPUTING. Vol.2 , Issue 3. Pp.152-157, MARCH, 2010.

[4]. S G Srikantaswamy, Dr. H D Phaneendra, “Improved Caesar Cipher with Random Number Generation Technique and Multistage Encryption”, International Journal on Cryptography and Information Security (IJCIS). Vol. 2, No.4. pp. 39-49, December 2012.

[5]. ”CRYPTOGRAPHY”, https://en//.wikipedia.org/wiki/cryptography.

[6]. Ochoche Abraham, Ganiyu O. Shefiu, “AN IMPROVED CAESAR CIPHER (ICC) ALGORITHM”, International Journal Of Engineering Science & Advanced Technology (IJESAT). Vol. 2, Issue -5. pp .1198 – 1202, October 2012.

[7]. Jason Crampton, “Time-Storage Trade-Offs for Cryptographically-Enforced Access Control”, Lecture Notes in Computer Science, Springer, 2011, Vol. 6879/2011, pp. 245-261.

[8]. Jiannong Cao, Lin Liao, Guojun Wang, “Scalable key management for Secure Multicast Communication in the Mobile Environment” Pervasive and Mobile Computing Vol. 2, pp.187–203, 2006.

[9]. Jawahar Thakur, Nagesh Kumar, ”DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis”, International Journal of Emerging Technology and Advanced Engineering,Vol. 1, Issue 2, pp. 6-12, 2011.

[10]. “ENCRYPTION”,http://www.cse.wustl.edu/~jain/cse567-06/ftp/encryption_perf/index.htm.

[11]. VinodSaroha, SumanMor and AnuragDagar, “Enhancing Security of Caesar Cipher by Double Columnar Transposition Method”, International Journal of Advanced Research in Computer Science and Software Engineering. Vol. 2, Issue 10. pp .86-88, October 2012.

[12]. Stalling, William.”Cryptography andNetwork Security: Principles andPractice”. 5th ed, Prentice Hall, 2006.

[13]. “Classical-Encryption Techniques”, mrajacse.files.wordpress.com/chapter-2.

[14]. Sinkov A., “Elementary “Cryptanalysis-A mathematical Approach”, Mathematical Association of America, 1966.

[15]. SomdipDey ,”SD-AREE: A New Modified Caesar Cipher Cryptographic Method Alongwith Bit-Manipulation to Exclude Repetition from a Message to beEncrypted”, Department of Computer Science,St. Xavier’s College, Kolkata, West Bengal, India.

[16]. “Caesar.doc”,www.ti89.com/cryptotut/text/.