Implementation of Strong Encryption Method Using Caesar Cipher Algorithm

M.CHALAPATHI RAO [1]

[1]Assoc. Prof. in Department of CSE.Vaageswari College of Engineering, Karimnagar.

Abstract

In this paper, we have imported some innovative advancement to the popular Caesar cipher algorithm, which perfectly eliminates its constitutional weaknesses. Here we ignore spaces from the cipher text and the process of creating the cipher text by the advanced encryption method using Caesar Cipher Algorithm (CCA). In this encryption, it uses the substitution cipher in which each letter in the plaintext is replaced by some fixed number of position down the alphabet. This method is names after Julius Caesar who using this method to communicate with his generals. It involves encryption and scrambling of the letters in the cipher text, so even if it is decrypted the result would be gibberish. The results form of a data which is encrypted and are decrypted to its readable form. Caesar cipher algorithm can be implemented in advanced encryption to make data secure and better.

Key words: Encryption, Decryption, Caesar Cipher, Scramble, Concatenate, Cipher text, Gibberish.

1. Introduction

Cryptography is the study of mathematical techniques for all aspects of information security. Cryptanalysis is the complementary science concerned with the methods to defeat these techniques. Cryptology is the study of cryptography and cryptanalysis. In cryptography, a cipher is an algorithm for performing encryption or decryption a series of well defined steps that can be followed as a procedure. An alternative, less common term is enciphered. To encipher or encode is to convert information from plain text into cipher or code. In non-technical usage, a 'cipher' is the same thing as a 'code'; however, the concepts are distinct in cryptography. In classical cryptography, ciphers were distinguished from codes. The most useful one of substitution cipher is Caesar cipher. It was used by Julius Caesar to communicate secretly with his army. The power of the Caesar cipher is its ease of use and his soldiers were likely uneducated and not able to use complex coding system. The action of a Caesar cipher is to replace each plain text letter with one fixed number of places down the alphabet. Caesar Cipher settled that left shift of three. Scrambling is the function of replacing a character (or byte) of data with a different character (or byte) of data. Data that can be read and understood without any special measures is called plaintext or clear text. The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable gibberish called cipher text. You use encryption to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of reverting cipher text to its original plaintext is called decryption. In sentence the word concatenating group of characters from stream of sequence. For the key, we use the number of places k that each letter should be shifted to the right; this equivalent to using the letter with which the cipher alphabet starts. When considering this type of cipher from a mathematical perspective, we transform our plaintext from letters to numbers. Further advancement to actual three places shifting of character in Caesar cipher uses modulo twenty six arithmetic for encryption key that is greater than twenty six.

$$E\,(a) = (a - k) \bmod 26$$

Similarly, the decryption function (which takes in the cipher text number b) is:

$$D\,(b) = (b - k) \bmod 26$$

After encryption/decryption, we can convert the numbers back into letters. This mathematical process may seem pointless when working by hand, but it is much more easily implemented on a computer. The biggest weakness of this cipher is simple in use of encryption and decryption algorithms it can easily to be broken by reversing encryption process without knowing the encryption key for this reason improve encryption strength is a metric of the potency of an encryption regulate guessing message. Let us represent motivation for the caser cipher and its neigh borings in section 2. Then we will furnish detailed information about our related work in section 3.Demonstration of results are framed in section 4. Lastly section 5 concludes.

2. Motivation

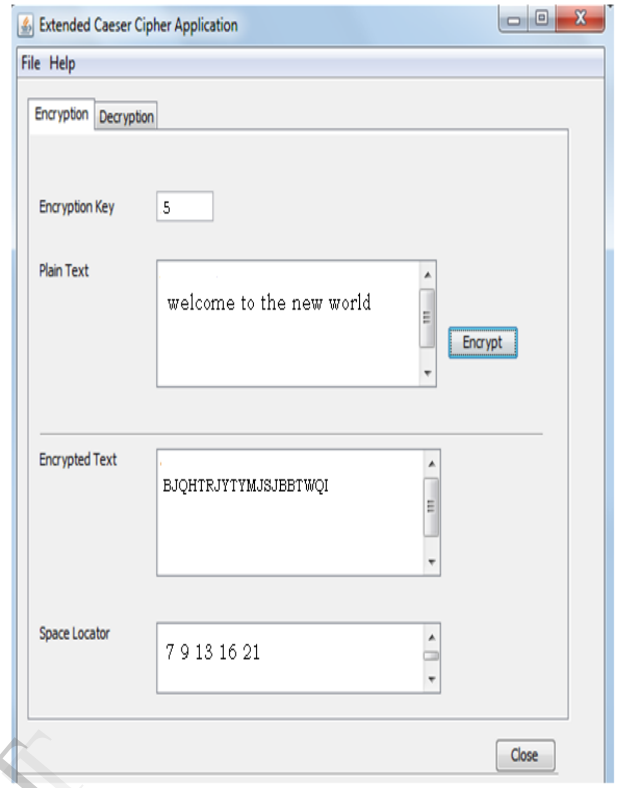
Today more no of hackers are came to light even possible techniques are being our surroundings for preventing them we greatly use advanced technologies in such away we improve encryption and decryption capabilities with the increasing use of the secure transmission of data and information over the internet, the need of strong encryption increasing day by day. In this work of encryption technique we present a new way. Generalization of Caesar cipher text is generated by shifting plaintext letters by secret value [1]. General system of substitution technique is called mono-alphabetic substitution each letter of the plaintext is mapped onto some other letter, but in every case always mapped to the same a letter in the cipher text represents a single clear text letter [2]. For encrypting a message, Caser Cipher needs plaintext and a key for encryption. The encryption key is an integer value and it represents location of alphabet for substitution. The result shows encryption process generates two various outputs viz. encrypted text and space delimited integer values of location within the plain text has some spaces [3]. Decryption is to avoid generated spaces during encryption process by using opposite method to procure decrypted message. It needs decryption key, space delimited integer value(s) and of course the encrypted text [4]. For encrypting/decrypting, we've got a maximum key size of 26 possible keys. That's 26 possible combinations. Even in a non-modern computer era, this is an easy brute force. Secondly, the plaintext is encrypted evenly, which means you wouldn't even need to try all of the keys for the whole cipher text just a few words would be enough to tell if you've found the key or not. The encryption is also performed on a single character basis leaving it opens to frequency analysis attacks. The reason the Caesar Cipher is so well known is it's implicit simplicity, it's history (being one of the first encryption methods), and it's great way of showing the many different flaws an encryption process can have[5]. The decryption key should be accompaniment of the encryption key so that reverse character substitution can be produced. As mentioned earlier, Caesar cipher shifts scrambled character by number of positions during giving spaces in between words. This is the motivation leading behind of this paper by removing the spaces between words of sentences where that is encrypted; the stream of encrypted message is done from plain text. The formed encrypted message having deficiency of meaning so that encrypted plain text is not possible to read even spaces removed among the words. The removed spaces are taken during encryption operation and generated spaces are to be removed from decryption process not apparently shown extracted space [6]. The viewed Characters in the decrypted text are rearranged so that reading effect of all characters where grouped is impossible after removing space the attackers may not get an exact meaning in grouped characters. Moreover, the characters of the encrypted text are scrambled if an attack is made to decrypt the cipher text generated by Caesar cipher algorithm (CCA) the result would be gibberish [7].

3. Literature Survey

This literature survey explains the concept of the ways to find out all information that will be used in order to develop this system and analyzed. In general security is the quality or state of being secure and free from danger. In other words, building protection against adversaries, from those whose to do harm, intentionally or otherwise, it objective. Data security can be defined as technological and managerial procedures applied to computer systems [1]. The Caesar cipher is named after Julius Caesar, who, according to Suetonius, used it with a shift of three to protect messages of military significance. While Caesar's was the first recorded use of this scheme, other substitution ciphers are known to have been used earlier. If he had anything confidential to say, he wrote it in cipher, that is, by so changing the order of the letters of the alphabet that not a word could be made out. If anyone wishes to decipher these, and get at their meaning, he must substitute the fourth letter of the alphabet, namely D, for A, and so with the others. His nephew, Augustus, also used the cipher, but with a right shift of one, and it did not wrap around to the beginning of the alphabet: Whenever he wrote in cipher, he wrote B for A, C for B, and the rest of the letters on the same principle, using AA for X. Caesar ciphers can be found today in children's toys such as secret decoder rings. A Caesar shift of thirteen is also performed in the ROT13 algorithm, a simple method of obfuscating text widely found on Usenet and used to obscure text (such as joke punch lines and story spoilers), but not seriously used as a method of encryption.[2]. The Caesar cipher was in use: the Russian army employed it as a replacement for more complicated ciphers which had proved to be too difficult for their troops to master; German and Austrian cryptanalysts had little difficulty in decrypting their messages [4]. There is evidence that Julius Caesar used more complicated systems. It is unknown how effective the Caesar cipher was at the time, but it is likely to have been reasonably secure, not least because most of Caesar's enemies would have been illiterate and others would have assumed that the messages were written in an unknown foreign language [5]. In 2011, Rajib Karim was convicted in the United Kingdom of "terrorism offences" after using the Caesar cipher to communicate with Bangladeshi Islamic activists discussing plots to blow up British Airways planes or disrupt their IT networks. Although the parties had access to far better encryption techniques, they chose to use their own scheme(implemented in Microsoft Excel), rejecting a more sophisticated code program called Mujhaddin Secrets "because 'kaffirs', or non-believers, know about it, so it must be less secure"[6].

4. Results Demonstration

To demonstrate the potency of CCA, we tested our system with some online application Fig-1 CCA encryption interface of Fig-2 to decrypt the cipher text in Fig- 3 and Figure 4 shows resultant frequency graph. Each character was decrypted and the outcome was gibberish; no meaning could be presupposed provoke decrypted message because of the improvements that we have made to the Caesar Cipher algorithm. One biggest power of CCA is that it requires less computer resources when compared to other encryption algorithms. Strong encryption of encrypted data will increase the complexity of data encryption enormously, which will be very complicated to decrypt it. Caesar ciphers can be found today in children's toys such as secret decoder rings. A Caesar shift of thirteen is also performed in the ROT13 algorithm, a simple method of obfuscating text widely found on Usenet and used to obscure text (such as joke punch lines and story spoilers), but not seriously used as a method of encryption.



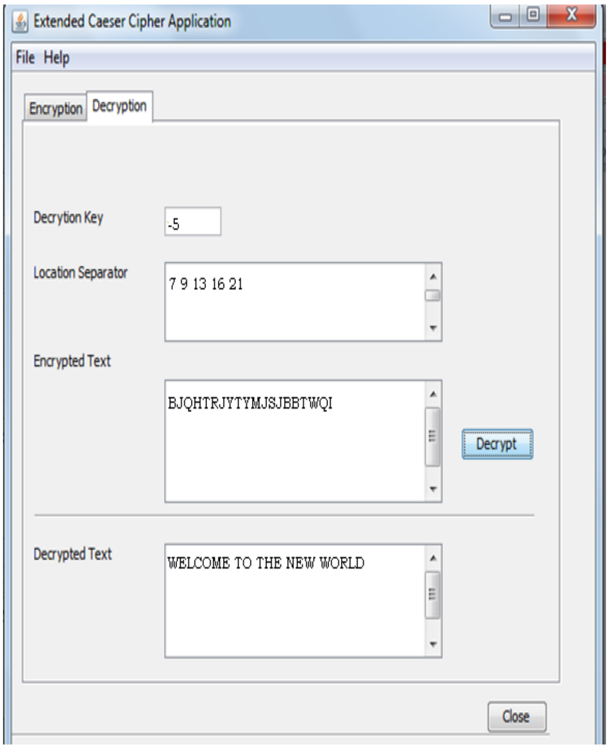
Encryption Key: 5

Plain Text: welcome to the new world

Encrypted Text: BJQHTRJYTYMJSJBBTWQI

Space Locator: 7 9 13 16 21

Fig-1: CCA Encryption Interface



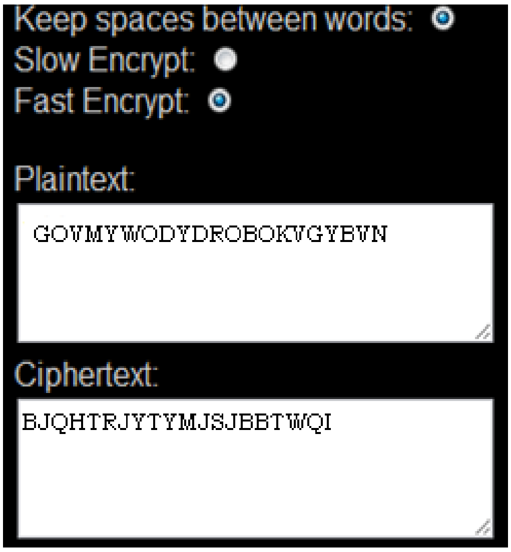
Decrytion Key: -5

Location Separator: 7 9 13 16 21

Encrypted Text: BJQHTRJYTYMJSJBBTWQI

Decrypted Text: WELCOME TO THE NEW WORLD

Fig-2: Decryption Interface



Keep spaces between words: ●
Slow Encrypt: ○
Fast Encrypt: ●

Plaintext:

GOVMYWODYDROBOKVGYBVN

Ciphertext:

BJQHTRJYTYMJSJBBTWQI

Fig-3: Decrypting Cipher text using the Caesar cipher On The Black Chamber website

The Caesar cipher can be easily broken even in a cipher text-only scenario. Two situations can be considered: First an attacker knows (or guesses) that some sort of simple substitution cipher has been used, but not specifically that it is a Caesar scheme; Second an attacker knows that a Caesar cipher is in use, but does not know the shift value. In the first case, the cipher can be broken using the same techniques as for a general simple substitution cipher, such as frequency analysis or pattern words.[13] While solving, it is likely that an attacker will quickly notice the regularity in the solution and deduce that a Caesar cipher is the specific algorithm employed. In the second instance, breaking the scheme is even more straightforward. Since there are only a limited number of possible shifts (26 in English), they can each be tested in turn in a brute force attack. One way to do this is to write out a snippet of the cipher text in a table of all possible shifts a technique sometimes known as "completing the plain component". The example given is for the cipher text "EXXEGOEXSRGI"; the plaintext is instantly recognizable by eye at a shift of four. Another way of viewing this method is that, under each letter of the cipher text, the entire alphabet is written out in reverse starting at that letter. This attack can be accelerated using a set of strips prepared with the alphabet written down them in reverse order. The strips are then aligned to form the cipher text along one row, and the plaintext should appear in one of the other rows.

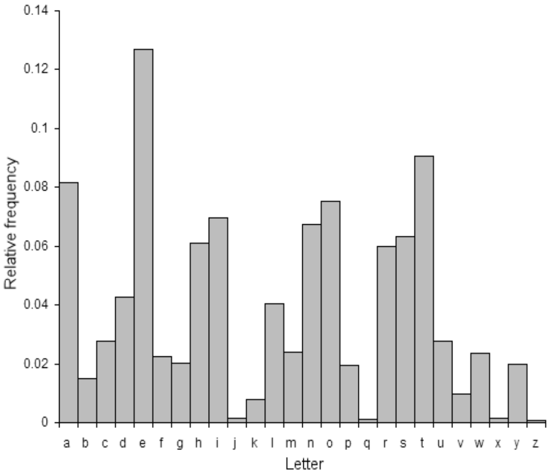
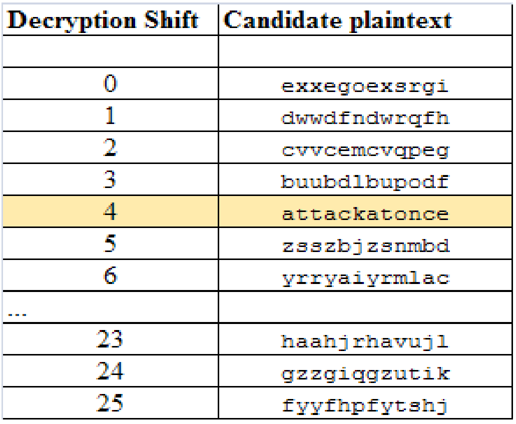


Fig 4: A Caesar shift "rotates" this distribution, and it is possible to determine the shift by examining the resultant frequency graph.

Another brute force approach is to match up the frequency distribution of the letters. By graphing the frequencies of letters in the cipher text, and by knowing the expected distribution of those letters in the original language of the plaintext, a human can easily spot the value of the shift by looking at the displacement of particular features of the graph. This is known as frequency analysis. For example in the English language the plaintext frequencies of the letters E, T, (usually most frequent), and Q, Z (typically least frequent) are particularly distinctive. Computers can also do this by measuring how well the actual frequency distribution matches up with the expected distribution; for example, the chi-squared statistic can be used.



Decryption Shift	Candidate plaintext
0	exxegoexsrgi
1	dwwdfndwrqfh
2	cvvcemcvqpeg
3	buubdlbupodf
4	attackatonce
5	zsszbjzsnmbd
6	yrryaiyrmlac
...	
23	haahjrhavujl
24	gzzgiqgzutik
25	fyyfhpfytshj

5. Conclusion

Security has become a very critical aspect of modern computing systems. The use of internet and network is growing rapidly. So requirement to secure the data is necessary. To provide security to network and data different encryption methods can be used. The result from this paper is a data which is encrypted and be decrypted to its readable form. As a conclusion, Caesar cipher algorithm can be implemented in advanced encryption to make data secure and better to achieve the fortification, spaces in between words were ignored and encrypted characters were scrambled. Caesar cipher algorithm can produce a flow of characters continuously it is far better used encryption technique.

References:

[1] Dulaney E., CompTIA Security+ Study Guide, Fourth Edition, Wiley Publishing Inc., Indianapolis, Indiana, 2009.

[2].http://www.cs.trincoll.edu/~crypto/historical/caesar.html (Savarese, C and Hart, B, The Caesar Cipher, Last updated: 04/26/2010 03:46:57).

[3]. http://en.wikipedia. org/wiki/Caesar_cipher, Caesar Cipher (Last accessed: April 20, 2012).

[4].http://www.simonsingh.net/The_Black_Chamber/caesar.html (Last accessed: April 23, 2012).

[5]. Luciano D. and Prichett G., "Cryptology: From Caeser Ciphers to Public-Key Cryptosystem", The College Mathematics Journal, vol 18, no 1, pp. 2 -17, 1987.

[6]. Murphy C., "Data Masking with Classical Ciphers", SAS Global Forum 2010, Paper 108-2010, 2010.

[7]. Sahami, M, CS106A: Strings and Ciphers, Handout #26, October 22, 2007 (Assessed March 25, 2011).

[8]. Sinkov A., Elementary Cryptoanalysis – A mathematical Approach, Mathematical Association of America, 1966.

[9] David Kahn, The Codebreakers — The Story of Secret Writing, Revised ed.1996. ISBN0-684-83130-9.

[10]F.L. Bauer, Decrypted Secrets, 2nd edition, 2000, Springer. ISBN 3-540-66871-3.

[11]Chris Savarese and Brian Hart, The Caesar Cipher, 1999.

[12] Kester, Quist Aphetsi., & Danquah, Paul. (2012). A novel crypto graphic key technique. In adaptiveScience & Technology (ICAST), 2012 IEEE 4th In- ternational Conference on (pp. 70-73).

[13]Nicolas Courtois, Josef Pieprzyk, "Cryptanalysis of Block Ciphers with Overdefined Systems of Equations". pp267.

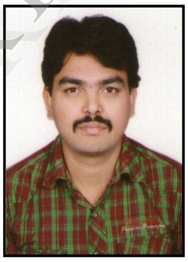
[13] Bruen, Aiden A. & Forcinito, Mario A. (2011). Cryp-tography, Information Theory, and Error-Correction: A Handbook for the 21st Century. John Wiley & Sons. p. 21. ISBN 978-1-118-03138-4.

[14] Martin, Keith M. (2012). Everyday Cryptography. Oxford University Press. p. 142. ISBN 978-0-19-1625886.http://books.google.com/books?id=1NHli2uztEC&p g=PT142.

[15] Kester, Q.-A. "A public-key exchange cryptographic technique using matrix," Adaptive Science & Technology (ICAST),2012 IEEE 4th International Conference on , vol., no., pp.78-81, 25-27 Oct. 2012.

[16] L.Thulasimani , M.Madheswaran, "Design And Implementation of Reconfigurable Rijndael Encryption Algorithms For Reconfigurable Mobile Terminals", International Journal on Computer Science and Engineering (IJCSE), Vol. 02, No. 04, pp. 1003-1011, 2010.

[17] 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.



M.CHALAPATHI RAO, Currently working as a Associate Professor in Vaageswari College of Engineering (VGSE), Karimnagar. He completed his M.Tech degree in J.N.T.U. Hyderabad. He received B.Tech Degree from J.N.T.U. Hyderabad. He had 8 years of Teaching Experience. Interested domain is Network Security.