IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 10, Issue 4, April 2020, ||Series -II|| PP 28-29

Modified Alberti' Cipher Employing Special Characters

KaminiIshwarya S, Dr. P. Thangaraju
KaminiIshwarya.S, MPhil, Department of Computer Science, Bishop Heber College.
Dr. P. Thangaraju, Asst.Professor, Department of MCA, Bishop Heber College.

Received 21 April 2020; Accepted 06 May 2020

Abstract: Internet plays a major role in the modern world. Nearly 3.2 Billion of people are using Internet. They use internet for all minor and major purposes like mails, Confidential and privacy text documents, social media, E-commerce, Banking etc. A few security measures like authentication, authorization systems are provided to them. There are several Encryption techniques such as RSA, DES etc. Apparently, somewhere in the world, hackers are cracking the Encrypted data and apprehending the keys and stealing the information as the Encryption and Decryption are only based on the International Language English. They use some online sites and tools to steal the data with ease. To increase the level of security this Alberti's cipher technique is proposed. It encrypts the plain text (English) to the special characters. So the hackers cannot crack it easily even with the help of online crackers or any other tools.

Keywords: Encryption, Decryption, Plain Text, Cipher Text, Alberti Cipher, Special characters.

I. INTRODUCTION

People send information through wired and wireless connection. Sometimes in-order to transfer information we use ad hoc networks. Now a day's data are being exposed to vulnerabilities such as weak passwords, missing data encryption, missing authorization, unrestricted upload of dangerous file type, missing authentication for critical function. People finds these weakness and exploits the weakness in computer systems or networks to gain access which results is the loss of quality of service. In-order to overcome these hacking of information, people started following encryption and decryption techniques. One of the encryption and decryption technique is Alberti's Cipher Method. It has inner disk and outer disk, the inner disc was a mark which could be lined up with a letter on the outer disc as a key, so that if you wanted to encrypt or decrypt a message you only needed to know the correct letter to match the mark to. This method was proposed as an enhancement to Alberti's cipher technology. Instead of alphanumeric characters, the inner circle will consists of Special characters, where it will make difficult for modern computer's to crack it.Not only loss of packets, latency, jitter, data traffic determines the quality of service. Sending and receiving the information safely also determines the Quality of Service.

II.EXISTING SYSTEM

Alberti cipher is an example of Poly alphabetic substitution. It consist of disc namely outer disc and inner disc. The larger one is called Stablilis and the smaller one is called Mobilis. Around the disc, the outer disc are inscribed the uppercase letters in the Latin alphabet, which is the English alphabet less *J, U,* and *W,* and also without *H, K,* or *Y,* since Alberti felt they were superfluous. The outer discalso included the numbers 1 through 4 for use with a codebook containing preselected phrases and words with assigned four-digit values. The inner disc had a randomized uppercase Latin alphabet, which is the English alphabet minus *u, w,* and *j,* and with *et* (probably meaning '&'). Though there is a high level of security, we can improve this method by replacing the inner disc with special characters.

III.PROPOSED SYSTEM

In the proposed system, the inner disc is replaced by special characters such as % ; ^ ! $ etc .,The outer disc will only have Alphabets. English letters from A to Z. In this method the message will be encrypted as special characters, so the hackers will not be able to crack the data/ messages we send. The index value is not constant, it can be changed according to the sender's interest. The encrypted data will be decrypted only by the receiver who is authorized to access the data. In the meantime the receiver should know the key and index value in order to decrypt the data/message. Though if the message is captured by the hackers it will not be cracked by them until they know the index value of the encrypted message.

IV.PROCEDURE

In the proposed system, the user inputs a message or text in English. In-order to encrypt the data/message we need to select any one special character as index. Then we have to choose any word as keyword which should not have any repeated letters. Once we align the keyword to the message, we will rotate the disc according to the index and the keyword to get the cipher text. To decrypt the message the receiver should know the index, keyword. Though if the hackers cracked the keyword and the index, unless they have the knowledge on the Alberti cipher, it is unable to break the cipher text.

The special characters order can be changed according to the sender’s logic. The receiver should also have the same logic and order to decrypt the message.

INDEX	=	=	=	=	=	=	=	=	=	=
KEYWORD	T	U	E	S	D	A	Y	T	U	E
PLAIN TEXT	H	E	L	L	O	W	O	R	L	D
CIPHER TEXT	]	!	&	#	!	,	.	$	-	_
PLAIN TEXT	H	E	L	L	O	W	O	R	L	D

TABLE 1: Encrypted Data using special characters

A.DECRYPTION

The decryption occurs by the encrypted cipher text, those are in special character. This process will be reversed from the encryption. The receiver should use the same Index and the keyword, in-order to decrypt to plain text.

B.PURPOSE

This technique will be highly secure than the other techniques. The main advantage of using this technique is using special characters as Cipher text for encryption. It can be used in all the areas such as, Social media, Mails, E-Commerce sites to protect the privacy information such as address, name, ids, and account details. We can also use this technique for encrypting passwords.

V.CONCLUSION

This technique is a modified encryption and decryption process of Alberti’s cipher. In this technique, the plain text in International language English will be encrypted to a special characters. Also it is a modern Cryptex, where it will have separate disc containing alphabets, index values. This technique increases the privacy in transferring data message or message and other communication process. This technique doesn’t protect any data from attacks, but the security of the cipher text will be stronger and hard to crack the information by the hackers. There by increasing the quality of service in the data perspective.

[1]. REFERRENCE:

[2]. [ATU, 07] AtulKahte, "Cryptography and Network Security”, Tata Mcgraw Hill, 2007.

[3]. [BHA, 14] Bhadada, R., & Sharma, A. (2014, December). Montgomery implantation of ECC over RSA on FPGA for public key cryptography application. In 2014 2nd International Conference on Emerging Technology Trends in Electronics, Communication and Networking (pp. 1-5). IEEE.

[4]. [KAT, 14] Katz, J., &Lindell, Y. (2014).Introduction to modern cryptography. Chapman and Hall/CRC.

[5]. [WIL, 05] William Stallings - “Cryptography and Network security”, fourth edition, 2005.

[6]. David Kahn, "On the Origin of Polyalphabetic Substitution," Isis 71, no. 1 (Mar., 1980): 122-127.

[7]. [Online available]: http://www.cs.trincoll.edu/~crypto/historical/alberti.html

[8]. [Online available]: https://en.wikipedia.org/wiki/Alberti_cipher_disk

[9]. [Online available] https://sites.wcsu.edu/mbxml/html/section_alberti.html

[10]. Mohammed Abutaha, MousaFarajallah, RadwanTahboub& Mohammad Odeh, “Survey Paper: Cryptography Is The Science Of Information Security”, International Journal of Computer Science and Security (IJCSS), Volume (5) : Issue (3) : 2011

[11]. PedramRadmand “Impact of Encryption on Qos in Voip, IEEE, 11570078, 10.1109/SocialCom.2010.112, 978-0-7695-4211-9

[12]. Vinod B Durdi ; P T Kulkarni ; K L Sudha, Analysis of QOS retention for transfer of multimedia data in wireless sensor networks, IEEE, **INSPEC Accession Number:** 15701534, **DOI:** 10.1109/APWiMob.2015.7374974, **CD:** 978-1-4799-8289-9

KaminiIshwarya S. "Modified Alberti’ Cipher Employing Special Characters." *IOSR Journal of Engineering (IOSRJEN)*, 10(4), 2020, pp. 28-29.