IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 09, Issue 11, November. 2019, Series -I, PP 01-04

Modified Vigenere Cipher Employing Unicode Tamil Characters

Castro B S, J.JohnRaybin Jose
Castro B.S, MPhil, Department of Computer Science, Bishop Heber College.
J.JohnRaybin Jose, HOD &Asst.Professor, Department of IT, Bishop Heber College.
Corresponding Author:Castro B S
Received 22 October 2019; Accepted 05November 2019

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 asthe 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 Mod-ViC(Modified Vigenere Cipher) technique is proposed. It encrypts the plain text (English) to the regional language (Tamil). 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, Substitution, Vigenere Cipher.

I. INTRODUCTION

Mod-ViC is an Encryption Technique or a Tool which is used to encrypt a Plain Text or a Message from English to a Regional Language (Tamil). There are several Encryption methods and techniques created and followed, but all of themmost probably use the international language English such as RSA, DES, etc[4]. From the earlier stage English Language is used all over the Cyber World. Even for the communication purpose and data transfer or transaction process English plays a major role. In the current scenario the internet users are three times higher than the earlier stages. Internet is used in all minor to major organizations and even in private to Public sectors such as E-commerce, Banking, Government Organizations, Military Communications, Social Medias, IT sectors etc. Data is more confidential and privacy is vital even amongst normal users. There are so many techniques and tools to crack all the Encrypted data and even password protected data. But they are encrypted or created with the major Language English. The Plain Text as well as the Cipher Text will be in English. So the Hackers or Intruders can easily Crack the text or data. There are several methods used to crack the Cipher or Encrypted data by using some websites which can decrypt the cipher texts in online, called online cipher crackers. To overcome the problem this Mod - Vic technique is evolved. If the plain text or secret key and the cipher texts are in same language it can be easily cracked by anyone. If there is any change in the secret key or in cipher text's language it can't be easily cracked by anyone. The online cracking tools can't able to decrypt it. So this Cipher technique or the tool will change the language to a South Indian Regional Language (Tamil) of the cipher texts and then it converts the Tamil texts to the Unicode as cipher texts.

II. EXISTING SYSTEM

In Cryptography, there are several Encryption Cipher techniques. They are only based on the English Language.From the beginning of networks the communication occurs in English language. Though the level of security is high there are many hackers and crackers stealing the information and penetrating through the loop holes somehow by various types of attacks. Hackers usually apprehend the key and decode the cipher text by online converters, tools etc. Because English language is known by many and the data are in English.

III. PROPOSED SYSTEM

English language is known by most of the people and the transferring of data will be mostly in English. Using some other regional language among users will make the communication more secure and it will be little complicated to the hackers to apprehend the key as well as to decrypt it when it is caught. So, the Mod-ViCtechnique is proposed.

IV. PROCEDURE

In this proposed system the values of the key will be added. From this tool the user inputs a message or text in English alphabets and keys it will be encrypted to another Indian regional language Tamil and then to Unicode. So, the hackers cannot crack the message easier even with the help of online translators. The values of the keys are not constant and it can be changed as per the sender's logic. The encrypted data or the text will be decrypted only by the receiver who is authorized as well as who knows the key as well as S-Box. Even if the key is captured by hackers it can't be cracked.

A. VIGENERE CIPHER:

Vigenere Cipher is a Substitution technique which is used for Encryption. The main process of this cipher technique is the values of the Plain texts will be added with the values of the keys which are assigned in the S-Box. The S-Box is the Substitution box which is generated by a sender. The values and the method of the keys are also been evolved by the sender.

B.ROLE OF TAMIL CHARACTERS:

In this technique the Encrypted cipher will be assigned by Tamil characters. There are several categories in Tamil characters. 'uir' 'mei' 'uirmei' 'ayutham'. The 'uirezhuthukkal' consists of twelve characters, 'meiezhuthukkal' consists of eighteen characters and the combination of 'uir' and 'mei' ezhuthukkal consists of two hundred and sixteen characters and a single character is presented in 'ayutham'[11]. There are totally two hundred and forty seven characters are presented in Tamil Language. From the total characters in Tamil language only twenty six letters are randomly selected from 'uirmeiezhuthukkal' and used in this technique for the equality of total alphabets in English.

C.MOD-VIC ENCRYPTION**:**

The Plain Text will be processed with multiple operations with the keys and substituted with this Mod-ViCS-Box and encrypted as a cipher text in Unicode which are assigned or substituted in the order of s-box. Each of the character of the plain text will be assigned as per the S-Box and then the values of the keys will be assigned and then those values are added by,

Here,

P is the Plain Text

P_1, P_2, P_3, P_4 are its sequential characters.

K is the Key

K_1. K_2, K_3, K_4, are the sequential characters.

The sequential characters will be added,

$$P1 + K1 + K2 = C1$$

Here, C is the Cipher text.

The Cipher text has a value and it will be assigned by Tamil characters and then by its Unicode values.

This is how the Encryption process occurs.

PROCEDURE :

PLAIN TEXT = ******

KEY VALUE = OKAY (12 1 21 10)

ENCRYPTION :

"HELLO" (PLAIN TEXT)

PLAIN TEXT	ASSIGNED VALUES	KEYS	OUTPUT VALUES	ASSIGNED CHARACTER	ENCRYPTED TEXT
01001000	00110001 00110001	12	00110010 00110100	01001001	11100000 10101110 10110011
01000101	00110001 00110110	1	00110001 00110010	01001111	11100000 10101110 10011001
01001100	00111001	21	00110001 00110100	01010010	11100000 10101110 10101001
01001100	00111001	10	00110101	01001110	11100000 10101110 10110100
01001111	00110001 00110010	12	00110010 00110000	01011001	11100000 10101110 10101000

TABLE 1: MOD-VIC Encrypted Data

D. MOD-VIC DECRYPTION:

The Decryption occurs by the encrypted cipher text, those are in the Unicode of Tamil Characters, this process will be reversed from the encryption. The Unicode will be reforms to Tamil Characters by the use of S-Box and then it will be subtracted

P1 = K1 + k2 – C1

By the same keys which are used to Encrypt and then it will be decrypted to the plain English text.

"ளஙனழய" (ENCRYPTED TEXT)

ENCRYPTED TEXT	ASSIGNED CHARACTER	ASSIGNED VALUES	KEYS	OUTPUT VALUES	DECRYPTED TEXT
11100000 10101110 10110011	01001001	00110010 00110100	12	00110001 00110001	01001000
11100000 10101110 10011001	01001111	00110001 00110010	1	00110001 00110110	01000101
11100000 10101110 10101001	01010010	00110001 00110100	21	00111001	01001100
11100000 10101110 10110100	01001110	00110101	10	00111001	01001100
11100000 10101110 10101000	01011001	00110010 00110000	12	00110001 00110010	01001111

TABLE 4.6.2 MOD-VIC Decrypted Data

E. MOD-VICPURPOSE:

This technique will be highly secured than other techniques. The main advantage of the technique is using a regional language (Tamil) as Cipher text and for encryption. It can be used in all the areas such as Social Media (Chatting), Mails, E- commerce sites to protect the privacy information such as address, name, ids, account details etc. We can use this technique also for encrypt passwords.

A. CONCLUSION

This Mod-ViCtechnique is a Vigenere cipher's modified encryption and decryption process. In this technique, the plain text in international language English, it will be encrypted to a regional language Tamil, and then it converts the resulted data to the Unicode characters of Tamil as cipher text for privacy. The total characters in the Tamil language are two hundred and forty seven and it will be more secured and hard to crack the data or the information if this technique is expanded in future. This Mod-ViCtechnique increases the privacy in transferring the data or message and other communication process. This technique doesn't protect any data from attacks, but the security of thecipher text will be stronger and hard to crack the information by the hackers.

REFERENCE

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

[2]. [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.

[3]. [BLA, 13] Blair, A. (2013, June). Learning the Caesar and Vigenere Cipher by hierarchical evolutionary re-combination.In 2013 IEEE Congress on Evolutionary Computation (pp. 605-612).IEEE.

[4]. [TAM, 15] Encryption Technology For Tamil Language (Tamilan Cipher) P.Thamizhikkavi ,Dr.S.Magesh, International Journal Of Science, Engineering And Technology Research (Ijsetr) Volume 4, Issue 4, April 2015

[5]. [RAJ, 13] English Encryption Technique Using Multilanguage , M.Rajendiran, K.Selvam , N.Ranjith Kumar, T.Venkatesh, International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 3, March - 2013 ISSN: 2278-0181

[6]. [GNA 16] Gnanasekar, J. (2016). Unicode Text Security Using Dynamic and Key-Dependent 16x16 S-Box.

[7]. [DAV, 03] David Bishop, "Introduction to cryptography with java applets", 2003.

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

[9]. [KUM, 10]Kumar, G. P., Murmu, A. K., Parajuli, B., &Choudhury, P. (2010, April). MULET: a multilanguage encryption technique. In 2010 Seventh International Conference on Information Technology: New Generations (pp. 779-782). IEEE.

[10]. [MAN, 12]Manikandan, G., Rajendiran, P., Chakarapani, K., Krishnan, G., &Sundarganesh, G. (2012).A modified crypto scheme for enhancing data security. Journal of Theoretical and applied information Technology, 35(2), 149-154.
[11]. [OJH, 10] Ojha, D. B., Singh, R., Sharma, A., & Mishra, A. (2010). An Innovative Approach to Enhance the Security of Data Encryption Scheme. International Journal of computer Theory and engineering, 2(3), 380.
[12]. [RAN, 10] Ranganathan, V. (2010). Tamil Language in Context: A Comprehensive Approach to Learning Tamil, Department of South Asia Studies, University of Pennsylvania.
[13]. [RIZ, 10] Rizvi, D. S., &Wadhwa, N. Analysis of Substitution and Permutation from Cryptanalysis Perspective. Proceedings of ISCET-2010.
[14]. [SRI, 12] Srivastava, A. K., Sharma, S., &Sahu, S. (2012). Msmet: A Modified & Secure Multilanguage Encryption Technique. International Journal on Computer Science and Engineering, 4(3), 402.
[15]. [SUB, 12] Subramaniam, T., Pal, U., Premaretne, H., &Kodikara, N. (2012).Holistic recognition of handwritten Tamil words.In 2012 Third International Conference on Emerging Applications of Information Technology (pp. 165-169).IEEE.
[16]. [WIL, 05] William Stallings - "Cryptography and Network security", fourth edition, 2005.

IOSR Journal of Engineering (IOSRJEN) is UGC approved Journal with Sl. No. 3240, Journal no. 48995.

Castro B S. "Modified Vigenere Cipher Employing Unicode Tamil Characters." IOSR Journal of Engineering (IOSRJEN), vol. 09, no. 11, 2019, pp. 01-04.