Advances in Computational Sciences and Technology
ISSN 0973-6107 Volume 10, Number 5 (2017) pp. 977-983

http://www.ripublication.com

Addendum of Playfair Cipher in Hindi

Saman[1] , Md.Tabrez Nafis[2] , Mohammad Sadiq Nisar Siddiqui [3], Siddhartha Sankar Biswas [4]

Dept of Computer Science and Engineering, Jamia Hamdard University, New Delhi – 110062, India.

Abstract

With the rapid growth and development of technology in today's world security and privacy have become a major concern. We need to protect our data from antagonists. The digitalization of world is not circumscribed to just English language rather it is unbounded to any language. Hindi is the national language of India whose population is around 1.2 billion and it is one of the major factions in Information technology industry. In this paper an idea is presented in accord to encryption and decryption of data in Hindi language. The idea proposed is to modify original 5*5 playfair cipher to 6*10 matrix cipher to accommodate all the characters of Hindi language, numerical digit and a special character to overcome the limitation of original playfair cipher.

Keywords- cryptography,Playfair, plaintext, ciphertext,

1. INTRODUCTION

India is a country with 1.2 billion population and hindi as its official language. Hindi is the fourth most spoken language in the world, after Standard Mandarin, Chinese, Spanish and English[1].

Cryptography-the word derived from Greek language. It is basically the method of maintaining the data security from the intruder or the adversaries. It is a covert conversation which involves two parties communicating with each other. The three main triads of cryptography which is assured in secure communication are CIA.CIA is confidentiality, integrity and availability as shown in Fig 1. Confidentialityrefers to

the preservation of data from illegitimate disclosure. Integrity refers to the affirmation that data received is as sent by a legitimate entity. Availability ensures that the legitimate parties are capable to access the information when needed.

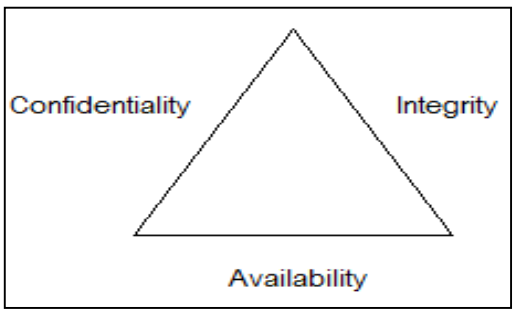

Fig 1. CIA Triad

Cryptography is the study of building and using encryption and decryption techniques. The term plaintext is used for the original message which is going to be encrypted and after applying encryption algorithm, the plaintext is converted to cipher text at the sender's side and is send to the receiver in a secure mode. While reaching the receiver's side the cipher text is converted into plaintext using the decryption algorithm. The whole process is shown in Fig 2. Encryption algorithm converts plaintext to cipher text while decryption algorithm converts cipher text to plaintext. Decryption algorithm is the reverse process of encryption algorithm[2]. A symmetric key is used by the encryption/decryption algorithm to encrypt/decrypt message.

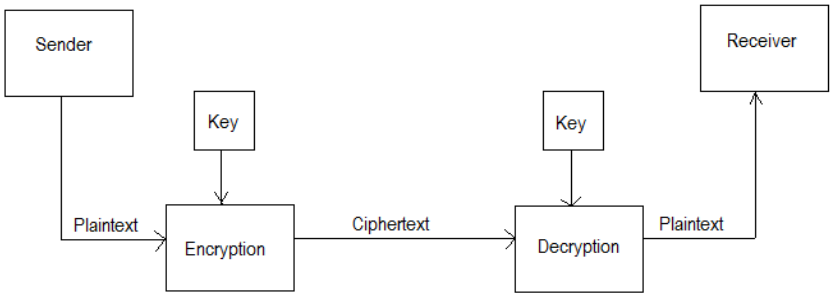

Fig 2. Cryptography process

Cryptography is of two types, Symmetric Key Cryptography and Asymmetric Key Cryptography [3]. In symmetric key cryptography, key used for encryption/decryption process is same. Thesender uses the key and the encryption algorithm to encrypt the data and the receiver uses the same key and decryption algorithm to decrypt the data.

In Asymmetric Key Cryptography each user is assigned a pair of keys, public key and private key[4].The public key is declared to the public while private key is kept secret.

2. LITERATURE SURVEY

The conventional Playfair cipher makes use of 25 uppercase alphabets with I=J or Q neglected[5]. A key-word is selectedand is used to create a key matrix which is used for both encryption/decryption process which is shown in Table 1.The key matrix is generated by filling the matrix with the characters of the keyword without any repetition in the order of their appearance in the keyword, the remaining matrix is filled by the remaining alphabets.Plaintext is encrypted two letters at a time. Any repeating plaintext letters that are in the same pair are separated with a filler letter such as X[6]. Also for any standalone letter at the end would be paired by using some filler letter such as X.

Table 1. 5*5 Playfair Cipher

H	A	M	D	R
B	C	E	F	G
I/J	K	L	N	O
P	Q	S	T	U
V	W	X	Y	Z

Keyword: Hamdard

Plaintext: BALLOONS

Diagraphs: BA LX LO ON SX

Ciphertext: CH SM NI IO XM

2.1. How the algorithm works?

a)Encryption

i) Eachplaintext letters are supplanted by the letter to the right when it lies within the similar row of the matrix and the primary element of the row circularly follows the last.

ii) Each plain text letters are each supplanted by the letter beneath when it lies within the similar column of the matrix and the top element of the row circularly follows in the last.

iii) Each plaintext letter is supplanted by the letter that falls in its own row and the column occupied by the other plaintext letter.

b)Decryption

In the event of decryption the inverse is finished with the cipher text and we get returned the apparent plain text.

i) Each ciphertext letters are supplanted by the letter to the left when it lies within the similar row of the matrix and the last element of the row circularly follows the last primary.

ii) Each ciphertext letters are each supplanted by the letter above when it lies within the similar column of the matrix and the last element of the row circularly follows in the top.

iii) Each ciphertext letter is supplanted by the letter that falls in its own row and the column occupied by the other ciphertext letter.

2.2 Drawbacks of existing playfair cipher

- I and J are considered as an individual character or Q is neglected.
- It doesn’t make use of numbers.
- When the plaintext wordcomprises of odd number of characteran extra letter X is included and during the process of decryption X is left out.
- X is a legitimate character and makes disarray since it could be a unit of plaintext, so in decryption process we just can't evacuate X.

3. PROPOSED 6*10PLAYFAIR CIPHER

Hindi is the most talked dialect in the world after Standard Mandarin,Chinese, Spanish and English respectively. The hindilanguage consists of 49 characters which are further described as vowels and consonants. Out of the 49 characters, 13 are vowels and the remaining 36 are consonants. In addition to this numerical digits are added and also * is added to be used as filler character as described in Table 2. Vowels are defined at the top of matrix followed by consonants, numerical digits and * respectively.So, for the process of encrypting/decrypting messages in hindi, a 6*10 matrix would be required.

Table 2. 6*10 Playfair Cipher

अ	आ	इ	ई	उ	ऊ
ऋ	ए	ऐ	ओ	औ	अं
अः	क	ख	ग	घ	ङ
च	छ	ज	झ	ञ	ट
ठ	ड	ढ	ण	त	थ
द	ध	न	प	फ	ब
भ	म	य	र	ल	व
श	ष	स	ह	क्ष	त्र
ज्ञ	०	१	२	३	४
५	६	७	८	९	*

The proposed 6*10 playfair cipher overcomes the limitation of conventional 5*5 playfair cipher. Unlike 5*5 playfair cipher, while creating diagraphs the filler character is a special symbol rather than the letter of the specified language.

3.1 How the algorithm works?

A key-word is selected and is used to create a key matrix which is used for both encryption/decryption processes as shown in Table 3. The key matrix is generated by filling the matrix with the characters of the keyword without any repetition in the order of their appearance in the keyword, the remaining matrix is filled by the remaining alphabets followed by numerical digit and special symbol "*" .

Keyword: बरगद

Plaintext:हमसब१साथहैं

Diagraphs:हमसब१सआथहऐअं*

Ciphertext:सयशग७१गपशअंं८क

Table 3. 6*10 Playfair Cipher

ब	र	ग	द	अ	आ
इ	ई	उ	ऊ	ऋ	ए
ऐ	ओ	औ	अं	अः	क
ख	घ	ङ	च	छ	ज
झ	ञ	ट	ठ	ड	ढ
ण	त	थ	ध	न	प
फ	भ	म	य	ल	व
श	ष	स	ह	क्ष	त्र
ज्ञ	०	१	२	३	४
५	६	७	८	९	*

a) Encryption

i) Each plaintext letters are supplanted by the letter to the right when it lies within the similar row of the matrix and the primary element of the row circularly follows the last.

ii) Each plain text letters are each supplanted by the letter beneath when it lies within the similar column of the matrix and the top element of the row circularly follows in the last.

iii) Each plaintext letter is supplanted by the letter that falls in its own row and the column occupied by the other plaintext letter.

b) Decryption

In the event of decryption the inverse is finished with the cipher text and we get returned the apparent plain text.

i) Each ciphertext letters are supplanted by the letter to the left when it lies within the similar row of the matrix and the last element of the row circularly follows the last primary.

ii) Each ciphertext letters are each supplanted by the letter above when it lies within the similar column of the matrix and the last element of the row circularly follows in the top.

iii) Each ciphertext letter is supplanted by the letter that falls in its own row and the column occupied by the other ciphertext letter.

4. CONCLUSION

This paper endeavored to utilize the traditional 5*5 playfair cipher and propose an improved 6*10 playfair cipher for hindi language which overcomes limitation of the original 5*5 playfair cipher while providing a cryptographic algorithm in hindi language. It accommodates all letters of the hindi language and numerical digits in hindi. In the proposed 6*10 playfair cipher, a special character * is used as a filler character when needed which was not available in original playfair cipher.

REFRENCES

[1] Mikael Parkvall, "Världens 100 störstaspråk 2007" (The World's 100 Largest Languages in 2007), in Nationa lencyklopedin.

[2] A. Forouzan and G. Hill, Data Communications and Networking, 4th Edition by Behrouz, Feb 9, 2006.

[3] Muhammad Salam, Nasir Rashid, Shah Khalid, Muhammad Raees Khan, "A NXM Version of 5X5 Playfair Cipher for any Natural Language (Urdu as Special Case)". World Academy of Science, Engineering and Technology 73 2011.

[4] A. AftabAlam, B. Shah Khalid, and C. Muhammad Salam ,"A Modified Version of Playfair Cipher Using 7×4 Matrix", International Journal of Computer Theory and Engineering, Vol. 5, No. 4, August 2013

[5] Sanjay Basu and Utpal Kumar Ray, "Modified Playfair Cipher using Rectangular Matrix", International Journal of Computer Applications (0975 – 8887) Volume 46– No.9, May 2012

[6] Subhajit Bhattacharyya, Nisarga Chand and SubhamChakraborty"A Modified Encryotion Technique using Playfair Cipher 10 by 9 Matrix with Six Iteration Steps", International Journal of Advanced Research in Computer Engineering & T echnology (IJARCET) Volume 3, Issue 2, February 2014