International Journal of Education and Information Technology
Vol. 3, No. 4, 2018, pp. 107-111
http://www.aiscience.org/journal/ijeit
ISSN: 2381-7410 (Print); ISSN: 2381-7429 (Online)

Encryption of Hindi Plaintext Using Modified Affine Cipher Technique

Piyali Sharma[1], Pramay Bhatpahri[2], Ravi Shrivastava[3, *]

[1]Department of Computer Science and Engineering, ICFAI (Institute of Chartered Financial Analysts of India) University, Raipur (Chhattisgarh), India
[2]Department of Mechanical Engineering, ICFAI (Institute of Chartered Financial Analysts of India University), Raipur (Chhattisgarh), India
[3]Department of Physics, ICFAI (Institute of Chartered Financial Analysts of India University), Raipur (Chhattisgarh), India

Abstract

In this paper, the encryption of Hindi plaintext using the modified affine cipher technique is reported. The numerical equivalents of the characters of Hindi were retrieved in Matlab 2016. Using Hindi characters for encryption, increases the level of security of the substitution cipher because of the availability of more characters for encryption in comparison to English. According to a cryptanalyst, any substitution cipher can be broken easily specially using the frequency analysis therefore it is proposed to divide the plaintext in small groups and then assigned different keys to different section of the text. In current work the plain text is divided into the number of groups of four characters and each group is assigned with a pair of co-prime numbers. Hence, total 8 keys will be required to encrypt a plain text of length 16 characters. By doing this, a specific plaintext character can be encrypted in different characters therefore the possibility of decrypting the message by frequency is very less. Here symmetric key cryptography is used hence only the sender and receiver know the security key i.e. they share the same key. It can be predicted that, if we encrypt Hindi plaintext message using above mentioned process, then it is impossible to decrypt the encrypted message without knowing security keys.

Keywords

Affine Cipher, Text Encryption, Hindi Encryption

Received: June 30, 2018 / Accepted: September 7, 2018 / Published online: October 9, 2018

1. Introduction

Today, we are living in the era of technology and internet. The Internet is the method to connect various computers for sharing information and data. Security of these data and information is the most important point to consider. Numbers of security issues are increasing with increasing use of internet technologies also. The user of cloud computing face this issue and become the victim of the security issues. Even cloud providers are also suffered from the same. Text cryptography plays an important role in securing the messages sent from one end to the other. In text cryptography, the original text is encrypted using a specific algorithm. This encryption is done using some confidential security keys, which is known to sender and receiver only. Without the security keys, it's a very difficult task for anyone to decrypt the messages [1-4]. Most of the text ciphers have already been reported by the different researchers. Some of them are Simple Substitution cipher [5], Caesar Shift Cipher [6], Vigenère cipher [7], Hill cipher [8], Affine cipher [3, 9, 10] etc. While choosing the method of text encryption, one needs to think about the possibilities of these encryptions to be broken using cryptanalysis. Ciphertext-only, Known-plaintext, Chosen-plaintext, Chosen-ciphertext and related-key models are commonly used by the cryptanalyst. One has

* Corresponding author
E-mail address: ravishrivastava@iuraipur.edu.in (R. Shrivastava)

to think from the point of view of a cryptanalyst to prevent encrypted data from hacking. Encryption for Hindi plaintext has not been extensively studied because an inbuilt Hindi typing facility was not there, earlier in our operating systems (OS). Nowadays Hindi fonts and typing features are available in the Windows (OS) itself.

In this article, a modified Affine ciphering technique has been used to encrypt a text given in the Hindi language. For this the manually retrieved the number associated with each character of Hindi language in Matlab 2016 have been used. Total 76 different numbers associated to various Hindi characters were found Matlab 2016.

2. Encryption and Decryption Process

Function used for encryption

E(x) = (ax + b) mode m, where m is the size of the alphabet and a & b are the key of the cipher. 'a' must be chosen in such a way that m and a are co-prime [5, 6].

Function used for decryption [5, 6].

D (E(x)) = a^{-1} (E(x) – b) mod m

= a^{-1} (((ax + b) mod m) – b) mod m

= a^{-1} (ax + b – b) mod m

= a^{-1} (ax) mod m

= x mod m

Where m = 76 (as 76 characters are used).

a^{-1}= inverse modulo of a.

Example encryption

Let a=3, b=5

Plaintext: - **स** ,Number mapping (x): - 54 (Table 1)

For encryption: - E(x) = (ax + b) mode m

= (3*54+5) = 167

= mod (167, 76) = 15

Ciphertext: - **ऑ**

For decryption:-

D (E(x)) = a^{-1} (E(x) – b) mod m

= 51 (167 – 5) = 8262

= mod (8262, 76)

= 54

Decrypted Text: - **स**

3. Complexity Analysis

Affine cipher is very old and popular method to encrypt a text message. Using this method anyone use to encrypt English alphabets by assigning a number value of 0-25 to A-Z respectively and then applying the specific algorithm to encrypt. As per researchers towards this field is concerned, it has been applied to English alphabets only but not on Hindi devnagri alphabets till now. Using Hindi alphabet in affine cipher technique of encryption has a major advantage over using same in English alphabets that approximately 76 different alphabets are available in Hindi including 'matras'. Having more number of characters helps in increasing the complexity of encryption. As total 76 characters can be used, we have used modular of 76 instead of 26 as one of the modification in traditional affine cipher techniques. Affine cipher is a substitution cipher; therefore, cryptanalysts may opt for frequency analysis for the decryption of hidden messages. Mathematical expressions used in affine cipher suggest that a cryptanalyst require 2 letters from the plain text for doing back calculation to get the decrypted text. Considering this point, have one key to a set of 4 letters is given. As a result of that the number of keys required to encrypt the text is increased and hence the complexity level of the security also increased.

4. Security Analysis

Affine cipher is the strongest possible substitution cipher. In general, the substitution ciphers are decrypted using the frequency analysis. Usually, the concept of frequency analysis is to identify the commonly used letters in the ciphertext and try to replace them by the generally used letters in the used language. The cryptanalysts, go for the checking the number of possibilities and make the substitution in the ciphertext. They study the possible appearing words and based on that make more substitution. For example, if a word "z" is coming frequently in the ciphertext, they try to replace the same with the vowels like 'a', 'e', 'i', 'o', 'u' because these are mostly used in any phrase.

Total 76 characters of Hindi language rather than using 26 alphabets of English are used. These number of characters used makes it difficult for a cryptanalyst to decrypt the cipher text.

Apart from that, we retain the liberty to set different keys each time whenever going for encryption. Having this property, this cipher system is may be free from ciphertext-only attack.

During the ciphertext-only attack, the attacker has access only to a number of encrypted messages. He has no idea what

the plaintext data or the secret key may be. The goal is to recover as much plaintext message as possible to guess the secret key. After discovering the encryption key, it will be possible to break all the other messages which have been encrypted by this key.

In all, providing the different key set for the different ciphers, make the above-mentioned process, difficult for the cryptanalysts and our message will become secure.

The Affine cipher technique used for Hindi encryption has more security as far as other attacks like chosen key attack, Chosen – ciphertext attack, Brute Force attack, frequency attack etc.

Table 1. Hindi alphabets and their numeric equivalent.

Alphabet	Equivalent numeric value	Number mapping	Alphabet	Equivalent numeric value	Number mapping	Alphabet	Equivalent numeric value	Number mapping
ं	2306	0	ज	2332	26	श	2358	52
ः	2307	1	झ	2333	27	ष	2359	53
अॅ	2308	2	ञ	2334	28	स	2360	54
अ	2309	3	ट	2335	29	ह	2361	55
आ	2310	4	ठ	2336	30		2362	56
इ	2311	5	ड	2337	31		2363	57
ई	2312	6	ढ	2338	32	़	2364	58
उ	2313	7	ण	2339	33	ऽ	2365	59
ऊ	2314	8	त	2340	34	ा	2366	60
ऋ	2315	9	थ	2341	35	ि	2367	61
ऌ	2316	10	द	2342	36	ी	2368	62
ऍ	2317	11	ध	2343	37	ु	2369	63
ऎ	2318	12	न	2344	38	ू	2370	64
ए	2319	13	ऩ	2345	39	ृ	2371	65
ऐ	2320	14	प	2346	40	ॄ	2372	66
ऑ	2321	15	फ	2347	41	ॅ	2373	67
ओ	2322	16	ब	2348	42	ॆ	2374	68
ओ	2323	17	भ	2349	43	े	2375	69
औ	2324	18	म	2350	44	ै	2376	70
क	2325	19	य	2351	45	ॉ	2377	71
ख	2326	20	र	2352	46	ॊ	2378	72
ग	2327	21	ऱ	2353	47	ो	2379	73
घ	2328	22	ल	2354	48	ौ	2380	74
ङ	2329	23	ळ	2355	49	्	2381	75
च	2330	24	ऴ	2356	50			
छ	2331	25	व	2357	51			

Table 2 expressed the step wise encryption using affine cipher technique for Hindi plaintext. It can be observed from the table that we have the liberty of using 2 different keys in various section of the plaintext, which make ciphertext more complex and hard to crack. In present example, total number of keys used is 12. The plaintext used in this paper is "हिन्दी हमारी मातृभाषा" which contains total 21 characters including space and matras. Encryption started with first four characters. Keys chosen for first four characters i.e. "हिन्" were 1 & 3 and "ंूफअॅ" cipher text was retrieved. Similarly, remaining parts of the plaintext were encrypted and finally achieve "ंूफअॅधऩ औ्अऋए ऑवगमठृूध" as ciphertext.

Table 2. Section wise encryption using affine cipher technique.

Keys used	Characters 1- 4	Characters 5 - 8	Characters 9 – 12
a	1	3	5
b	3	5	7
Plaintext	हिन्	हिन्दी ह	हिन्दी हमारी
Ciphertext	ंूफअॅ	ंूफअॅधऩ औ	ंूफअॅधऩ औ्अऋए
Keys used	Characters 13 - 16	Characters 16 - 20	20+
a	7	11	13
b	11	13	17
Plaintext	हिन्दी हमारी मात	हिन्दी हमारी मातृभाष	हिन्दी हमारी मातृभाषा
Ciphertext	ंूफअॅधऩ औ्अऋए ऑवग	ंूफअॅधऩ औ्अऋए ऑवगमठृू	ंूफअॅधऩ औ्अऋए ऑवगमठृूध

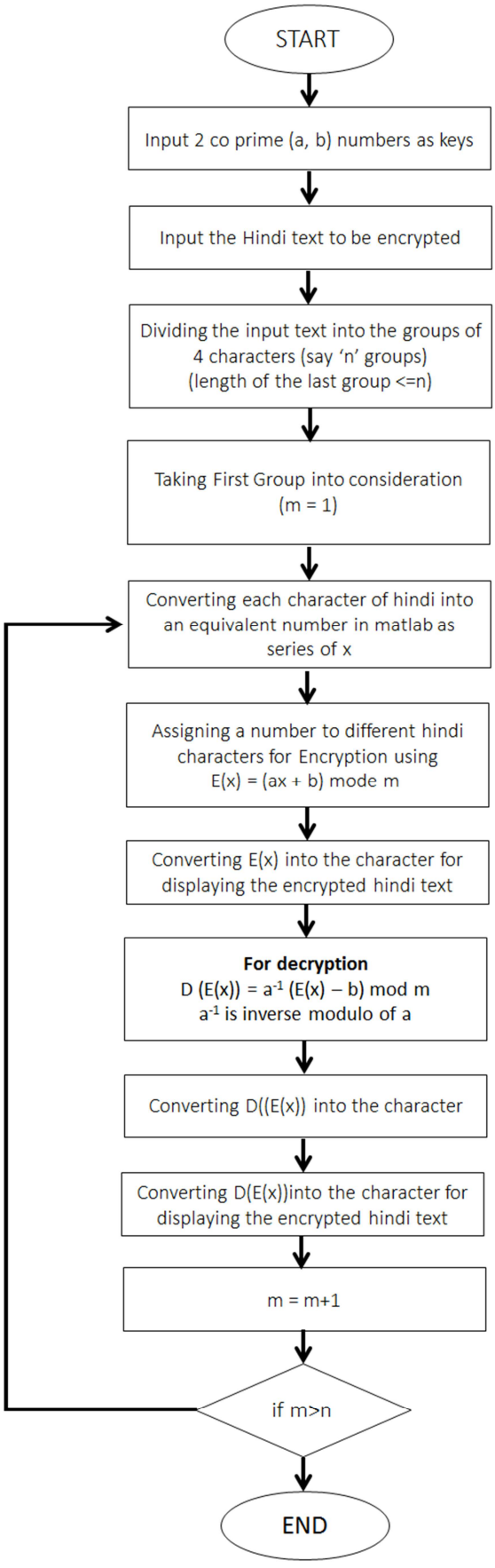

Figure 1. Flow chart explaining the algorithm used.

5. Conclusion

Most of the researchers are concentrating on ciphertext using the English language. Because of the aforesaid reasons cryptanalysts are also studying hard to crack the English Ciphertext. There are numbers of regional languages which can also be used for encryption. Hindi language is used as encryption language because Hindi is our national language. There are numbers of advantages of using Hindi in place of English for encrypting plaintext. First of all, Total 76 different characters are available in Hindi, which are almost thrice, what is there in English. Having, the greater number of characters increases the complexity of the ciphertext. Affine's technique is applied for encryption of Hindi text. Since the affine's technique is somehow a substitution technique, it can be cracked using frequency analysis, hence entire plain text is broken into a group of 4 characters. Affine cipher technique is applied to these groups separately by giving different keys to various groups. This again enhanced the complexity of the ciphertext. In near future, we may apply the similar technique for text cryptography for different regional language available.

References

[1] P. Sharma, P. Bhatpahri and R. Shrivastava, "Scrambling of an image using Block based circular shift technique for enhancing the security level of information", International Journal of Advanced in Management, Technology and Engineering Sciences, 8 (3), 1768-1774 (2018).

[2] P. Sharma, R. Shrivastava, V. K. Sarthi and P. Bhatpahri, "Security Analysis of XOR Based Ciphered Image", Asian Journal of Computer Science and Technology, 7 (1), 55-60 (2018).

[3] P. Sharma, P. Bhatpahri, R. K. Patnaik and R. Shrivastava, "Visual Encryption Using Multilevel Scrambling Followed by Affine Encryption Technique", Asian Journal of Computer Science and Technology, 7 (1), 40-45 (2018).

[4] P. Sharma, D. Mishra, V. K. Sarthi, P. Bhatpahri and R. Shrivastava, "Visual Encryption Using Bit Shift Technique", International Journal of Scientific Research in Computer Sciences and Engineering, 5 (3), 58-62 (2017).

[5] https://en.wikipedia.org/wiki/Substitution_cipher (Access Date: - October 26, 2017).

[6] G. P. Arya, A. Nautiyal, A. Pant, S. Singh and T. Handa, "A Cipher Design with Automatic Key Generation using the Combination of Substitution and Transposition Techniques and Basic Arithmetic and Logic Operations", The SIJ Transactions on Computer Science Engineering & its Applications (CSEA), 1 (1), 21-24 (2013).

[7] A. A. Soofi, I. Riaz and U. Rasheed, "An Enhanced Vigenere Cipher For Data Security", International Journal Of Scientific & Technology Research, 5 (3), 141-145 (2016).

[8] S. Chandrasekhar, H. P. Akash, K. Adarsh and S. Sasi, "A Secure Encryption Technique based on Advanced Hill Cipher for a Public Key Cryptosystem", IOSR Journal of Computer Engineering (IOSR-JCE), 11 (2), 10-14 (2013).

[9] Toru Sasaki, Hiroyuki Togo, Jun Tanida, and Yoshiki Ichioka, "Stream cipher based on pseudorandom number generation with optical affine transformation", Applied Optics, 39 (14), 2340-2346 (2000).

[10] http://practicalcryptography.com/ciphers/affine-cipher/ (Access Date:- October 26, 2017).