Cryptographic Technique: Base Change Method

Prabhas Tiwari
Deptt. of Computer Science
Jamia Hamdard University,
Hamdard Nagar, New Delhi

Nishtha Madaan
Deptt. of Computer Science
Jamia Hamdard University,
Hamdard Nagar, New Delhi

Md.Tabrez Nafis
Deptt. of Computer Science
Jamia Hamdard University,
Hamdard Nagar, New Delhi

ABSTRACT
Cryptography is the study of cryptographic algorithms that include encryption and decryption both. The importance of cryptography is discussed.

The problem statement here is, to form a cryptographic algorithm that uses randomization. Usage of high amount of randomization makes it tougher for one to crack the cipher text.

In our algorithm, we have made use of two concepts, usage of the alphabets' table from Caesar's Cipher and XOR decoding method using Vignere Cipher. Additional knowledge of Number Systems in Computers is used.

The algorithm is highly flexible. Since usage of number system theory has been made, the encoder may make use of any of the following system during encoding: BINARY, OCTAL, HEXA DECIMAL.

Further, any of these systems can be used in sub parts of the plain text, if the pre-process knowledge stored in K_1 can be varied to change the base and XOR operation results.

General Terms
Plain Text, Cipher Text, Cryptography, Encrypt, Decrypt, Key, Preprocessing Knowledge, Base Change, Randomization

Keywords
Cryptography, Encrypt, Decrypt, Cipher Text, Plain Text, Data Security

1. INTRODUCTION
Cryptography is the study of encryption and decryption techniques and algorithms. It is believed that more the randomization of the cipher text there is, the tougher it is to break the cipher text and retrieve the original plain text.

In today's times, data is the biggest weapon. It is often said that in modern times, war is not won by weapons, but by information. Data protection, therefore takes utmost priority in today's era.

After being recognized by the Queen of England, Queen Elizabeth II, and given Royal pardon, Alan Turing's great contribution to the defeat of Germany during the World War II saw the light of the day. Noting the computing scientist and mathematician's contributions to the war effort, British Prime Minister David Cameron used the occasion of the queen's pardon to laud Turing as "a remarkable man who played a key role in saving this country in World War II by cracking the German enigma code." [1]

Another essential aspect of data and network security is the CIA triad, where C is Confidentiality, I in for Integrity and A is for Availability. According to the Imperial College of London, in its article "CIA Principles" [2].

A model known as the **CIA triad** was designed to guide policies for information security within organizations. It has the following characteristics.

Confidentiality, an important part of security used to hide information from unauthorized people and the one most often attacked. It is achieved through access control lists, user ID's, passwords and policy based security.

Integrity is the property which assures that information can be trusted and the data remains in its original form. One type of security attack is to intercept some important data and make changes to it before sending it to the intended receiver.

Availability means that the information concerned can be readily accessed by an authorized viewer at any point of time. Network optimizations, upgrading the software and hardware maintenance ensure availability. Some types of security attack attempt to deny access to the appropriate user, for example, by breaking the web site for a particular search engine.

2. PROBLEM STATEMENT
With the onset of newer technologies and better understanding of cryptography, cracking a cipher has become comparatively easier. The DES algorithm that was once considered to be unbreakable is today absolutely breakable. However in 1976, the EFF DES cracker cracked the DES encrypted text in 22 hours 15 minutes [3]

In DES Algorithm we see that there has been plenty of randomization of the input text, which made it harder to crack it, at that era.

Since today, it is much easier to crack cipher texts that use older techniques, newer techniques of encryption need to be more random so as to make it tougher to decrypt.

3. SOLUTION

The solution to the problems statement is to add as much randomization as possible.

The idea behind the Base Change Method, as we call it, is derived from two different cryptographic techniques i.e. Caesar's Cipher and Vignere Cipher; and using the concept of number system.

The sender is treated as Encoder and the receiver is treated as Decoder in this paper. We are using 'K_1' as preprocess knowledge and 'K_2' as the shared secret key. 'C' is the Cipher text and 'P' is the Plain Text.

K_1 is the value to which the base needs to be changed in the number system theory. K_2 is a shared private bit key, generated using a random key generator of a length equal to the value of K_1. It means length (K_2) = value (K_1). K_2 used can be binary.

4. ALGORITHM

4.1 Encryption Method [E (P,K_1)]

1. P is the plain text; K_1 is the value to which the base of P will be converted to in number system.
2. Plain text P is divided into sub-parts. Pairs of 2 alphabets is taken and these groupings are hence forward considered for the encryption process. Padding with a dummy text can be used if the number of alphabets is not even.
3. P, which was alphabetic originally, is converted to its Decimal Equivalent using the table of Alphabets and their respective number representations as seen in Caesar's Cipher. However, since two alphabets are being used at a time, we concatenate the decimal representation. Example : PL = 1511
4. BaseChange(P,K_1). In this function, the plain text that is in decimal format is changed to the base value provided in K_1. After the conversion of base, the length of each sub part must be equal using bit expansion method.
5. K_2 key is formed. This key is the shared secret key in binary format. The value of this key is generated randomly and of length equal to the face value of K_1.
6. Once the plain text's base is shifted, with perform the XOR operation using the randomly formed K_2 key, to obtain the final cipher text C.

4.2 Decryption Method [D(C, K2)]

1. Now at the receiver's end, that is the decoder end, only 2 entities are available i.e. C (cipher text) and K_2 the randomly generated binary key that was shared.
2. For decryption, first step is to consider subparts of C one at a time only.
3. Next, perform XOR operation on the Cipher Text using the K_2 key.
4. Preprocess knowledge is retrieved by finding the length of K_2. Length (K_2) = Value(K_1).
5. On finding the value of K_1 we use it to change the base back to decimal number system.
6. On getting the decimal equivalent, we refer to the Caesar's cipher table to retrieve the Plain Text.

Table 1. Caesar's Cipher Table of Alphabet

Alphabet	Number	Alphabet	Number
A	0	**N**	13
B	1	**O**	14
C	2	**P**	15
D	3	**Q**	16
E	4	**R**	17
F	5	**S**	18
G	6	**T**	19
H	7	**U**	20
I	8	**V**	21
J	9	**W**	22
K	10	**X**	23
L	11	**Y**	24
M	12	**Z**	25

4.3 Dry Run & Results of Algorithm

Suppose our input is 'plaintext', it is divided into pairs then the value of each pair is calculated using the cipher table. Taking the value of key as 16,the text is converted to hexadecimal.

4.4 Encryption Method

Step 1. P = PLAIN TEXTS

P	L	A	I	N	T	E	X	T	S

P1 = PL
P2 = AI
P3 = NT
P4 = EX
P5 = TS

Step 2. Using the table from Caesar's Cipher

PL = 1511 AI = 0008 NT = 1319
EX = 0423 TS = 1918

Step 3. K_1 for instance is 16. And the randomly generated 16-bit shared private key, K_2 = 1011101000101110

PL = 05E7 AI =0008 NT=0527 EX=01A7 TS=077E

Step 4. Using the XOR operation on these sub parts to get the cipher text

C1= BFC9
C2= BA26
C3= BF09
C4= BB89
C5= BD50

Step 5.

Final Cipher Text = BFC9 BA26 BF09 BB89 BD50

4.5 Decryption Method

Step1. Given is:

K_2 = 1011101000101110
C1= BFC9
C2= BA26
C3= BF09
C4= BB89
C5= BD50

Step 2. Performing XOR

C1 = 05E7 C2 =0008 C3=0527 C4=01A7 C5=077E

Step3. Using the length of K_2 we can find out the value of the preprocess knowledge. Length(K_2) = 16 = Value(K_1)

Step 4. Since value of K_1 is 16, thus we know the hexadecimal conversion was made. Convert the values to base 10 i.e. decimal conversion

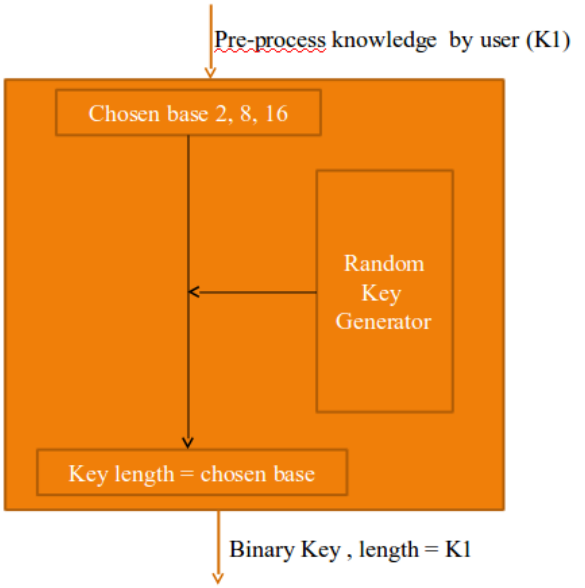

Fig 1: block diagram for key generation

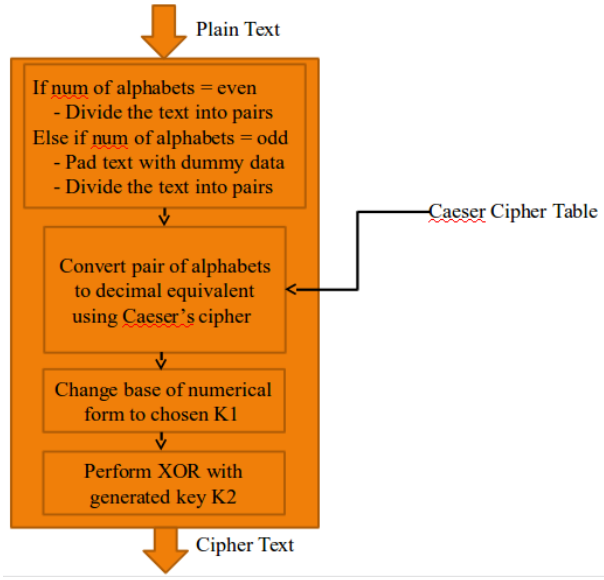

Fig 3: block diagram for decryption

P1 = 1511 P2 = 0008 P3 = 1319
P4 = 0423 P5 = 1918

Step 5. Comparing the decimal values to the Caesar's table of alphabets and the numerical values

P1 = PL P4 = EX
P2 = AI P5 = TS
P3 = NT

Thus, entire Plain Text = PL AI NT EX TS

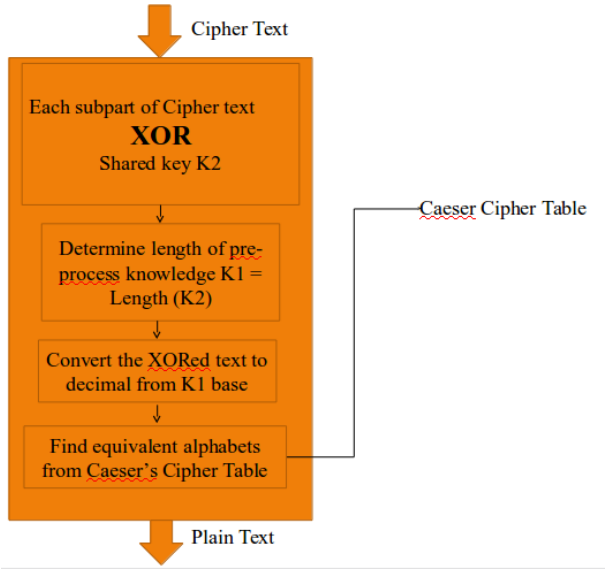

Fig 2: block diagram for encryption

5. ADVANTAGES

a. The resultant cipher text is Alpha-Numeric, which makes it tougher to guess the method of cracking the cipher.

b. Since we are using the concept of Number Systems, we have a bigger advantage of using multiple base change options i.e. Binary, Octal, or Hexadecimal.

c. Usage of XOR operation makes it easier to encode the text with a long binary key.

d. The K_1-lengthed key which is used for XOR can also be changed to Binary, Octal or Hexadecimal system.

6. DISADVANTAGES

a. Lower the base, longer the length of the cipher text is being formed.

b. Identifying the sub-parts of equal lengths

7. FUTURE SCOPE

a. Modification can always be made to any algorithm

b. We can extend the table for Caesar's Cipher of Alphabets and Numerical representation to include lower case and upper case separately.

c. Another extension that can be made is of symbols like punctuation marks.

8. ACKNOWLEDGMENTS
We would like to thank Ms. Richa Gupta, Assistant Professor at Jamia Hamdard University for her constant guidance during the development of the proposed algorithm. We would also like to acknowledge Sandeep Singh, for helping us with the implementation of the algorithm and in verification of the obtained results.

9. CONCLUSION
It is an alphanumeric technique for encryption using ciphers and number system. The proposed algorithm can be used in transmitting health care data during inter-organizational collaboration.Patient data can be encoded into alphabetical codes that cannot be cracked. Its advantage is that the codes look similar to medical codes (International Codes for Diseases, ICD) but actually are encrypted text. So it's a secure way of transmission of sensitive patient-data.

10. REFERENCES
[1] Web Source : http://www.advocate.com/world/2014/08/22/queens-decree-alan-turing-now-officially-pardoned

[2] Imperial College of London, Web Source: http://www.doc.ic.ac.uk/~ajs300/security/CIA.htm

[3] Electronic Frontier Foundation (1998). Cracking DES - Secrets of Encryption Research, Wiretap Politics & Chip Design. Oreilly & Associates Inc. (ISBN 1-56592-520-3)

[4] William Stallings (2003), Cryptography and Network Security, 3 rd edition, Pearson Education

[5] Plain Text Basesd Trasposition Method, Prof. S. D. Padiya* Prof. D. N. Dakhane, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, July 2012 ISSN: 2277 128X

[6] Atul Kahate (2009), Cryptography and Network Security, 2 nd edition, McGraw-Hill.