IOSR Journal of Computer Engineering (IOSRJCE)
ISSN: 2278-0661 Volume 4, Issue 2 (Sep.-Oct. 2012), PP 35-38
www.iosrjournals.org

Modification of Vigenère Cipher by Random Numbers, Punctuations & Mathematical Symbols

C. R. S. Bhardwaj

Abstract: *This dissertation discusses modification of Vigenère cipher which works by adding a key repeatedly into the plaintext using the convention that A = 0, B = 1, . . . , Z = 25; and addition is carried out modulo 26—that is, if the result is greater than 25, we subtract as many multiples of 26 as are needed to bring us into the range [0, . . . , 25], that is, [A, . . . , Z]. Mathematicians write this as: C = P + K mod 26 .For modification of Vigenère cipher, numbers, punctuations, mathematical symbols may be used for key in place of characters. Random generated numbers may be used to spread the encrypted message.*

Keywords: *Vigenère cipher, numbers, punctuations, mathematical symbols security, pseudorandom generator.*

I. Introduction

The success of E-commerce and m-commerce transactions depends on how transactions are carried out in the most secured manner. The prime requirements for any e-commerce and m-commerce transactions are Privacy, Authentication, Integrity maintenance and Non-Repudiation. Cryptography helps us in achieving these prime requirements. Today, various cryptographic algorithms have been developed. These are broadly classified as symmetric key (DES, TDES, Blowfish, CAST, IDEA, RC4, RC6, AES) and asymmetric key (RSA, ECC) algorithms. This dissertation discusses modification of Vigenère cipher which works by adding a key repeatedly into the plaintext using the convention that A = 0, B = 1, .. . , Z = 25; and addition is carried out modulo 26—that is, if the result is greater than 25, we subtract as many multiples of 26 as are needed to bring us into the range [0, . . . , 25], that is, [A, . . . , Z]. Mathematicians write this as: C = P + K mod 26 .For modification of Vigenère cipher, numbers, punctuations, mathematical symbols may be used for key in place of characters. Random generated numbers may be used to spread the encrypted message. both encryption and decryption process are carried out using a single key. These algorithms are efficient, are secure, execute at high speeds, and consume less computer resources of memory and processor time.

II. Literature Review

1. *Symmetric-Key Encryption Techniques*

In any symmetric-key encryption technique, both encryption and decryption process are carried out using a single key. These algorithms are efficient, are secure, execute at high speeds, and consume less computer resources of memory and processor time. However, symmetric key cryptographic techniques suffer from the disadvantages of Key distribution problem, Key management problem and inability to digitally sign a message. (Schneier [6], Stallings [7]).

Despite these drawbacks, numerous secure symmetric key encryption algorithms such as DES, TDES, Blowfish, CAST, IDEA, RC4, and RC6 have been developed. In recent times, National Institute of Standards (NIST) selected Rijndael algorithm as the Advanced Encryption

2. *Asymmetric Key Encryption Techniques*

The problems associated with symmetric-key cryptographic techniques were solved when asymmetric encryption mechanism was implemented. Here, instead of a single key, every person has a pair of keys. One key, called the public key is known to everyone and the other one, the private key is known only to the owner. There is a mathematical relationship between both these keys. Thus, if any message ‘m’ is encrypted using any of the key, it can be decrypted by the other portion. Various asymmetric encryption algorithms (RSA, Elgamal) have been implemented. Details on the working of asymmetric encryption techniques can be had from Schneier [6], Stallings [7]. Asymmetric encryption algorithms are broadly divided into three families:
1. Algorithms based on the integer factorization Problem (e.g. RSA)
2. Algorithms based on the discrete logarithm problem

III. Materials, Method & Procedure

Modification of Vigenère Cipher

The Vigenère cipher is a method of encrypting alphabetic text by using a series of different Caesar ciphers based on the letters of a keyword. It is a simple form of polyalphabetic substitution.

In a Caesar cipher, each letter of the alphabet is shifted along some number of places; for example, in a Caesar cipher of shift 3, A would become D, B would become E, Y would become B and so on. The Vigenère cipher consists of several Caesar ciphers in sequence with different shift values.

To encrypt, a table of alphabets can be used, termed a tabula recta, Vigenère square, or Vigenère table. It consists of the alphabet written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar ciphers. At different points in the encryption process, the cipher uses a different alphabet from one of the rows. The alphabet used at each point depends on a repeating keyword. For example, suppose that the plaintext to be encrypted is:

ATTACKATDAWN

The person sending the message chooses a keyword and repeats it until it matches the length of the plaintext, for example, the keyword "LEMON":

LEMONLEMONLE

Each row starts with a key letter. The remainder of the row holds the letters A to Z (in shifted order). Although there are 26 key rows shown, you will only use as many keys (different alphabets) as there are unique letters in the key string, here just 5 keys, {L, E, M, O, N}. For successive letters of the message, we are going to take successive letters of the key string, and encipher each message letter using its corresponding key row. Choose the next letter of the key, go along that row to find the column heading that matches the message character; the letter at the intersection of [key-row, msg-col] is the enciphered letter.

For example, the first letter of the plaintext, A, is paired with L, the first letter of the key. So use row L and column A of the Vigenère square, namely L. Similarly, for the second letter of the plaintext, the second letter of the key is used; the letter at row E and column T is X. The rest of the plaintext is enciphered in a similar fashion:

Plaintext:	ATTACKATDAWN
Key:	LEMONLEMONLE
Ciphertext:	LXFOPVEFRNHR

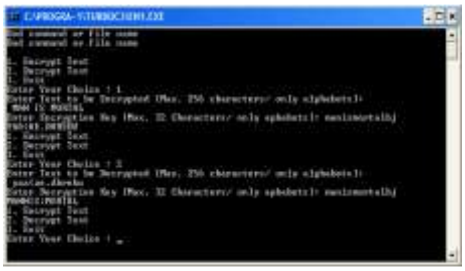
Decryption is performed by going to the row in the table corresponding to the key, finding the position of the ciphertext letter in this row, and then using the column's label as the plaintext. For example, in row L (from LEMON), the ciphertext L appears in column A, which is the first plaintext letter. Next we go to row E (from LEMON), locate the ciphertext X which is found in column T, thus T is the second plaintext letter.

Vigenère can also be viewed algebraically. If the letters A–Z are taken to be the numbers 0–25, and addition is performed modulo 26, then Vigenère encryption using the key can be written, and decryption using the key .This dissertation discusses modification of Vigenère cipher which works by adding a key repeatedly into the plaintext using the convention that A = 0, B = 1, . . . , Z = 25; and addition is carried out modulo 26—that is, if the result is greater than 25, we subtract as many multiples of 26 as are needed to bring us into the range [0,., 25], that is, [A, . . . Z]. Mathematicians write this as: C = P + K mod 26.

.For modification of Vigenère cipher, numbers, punctuations, mathematical symbols may be used for key in place of characters to make it more difficult for brute force attack. If random numbers are used for key and to spread the spectrum then only trained persons can identify the message. Comparision of both (Vigenère cipher and modification of Vigenère cipher) is given in the following diagram. I proposed two modifications in Vigenère cipher.

1. Random generated numbers may be used in place of alphabets for encryption key.
2. Random generated numbers may be used to spread the encrypted message.
3. Both encryption and decryption process are carried out using a single key. These algorithms are efficient, are secure, execute at high speeds, and consume less computer resources of memory and processor time.

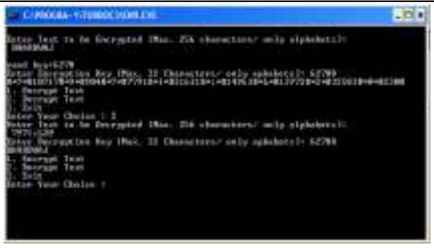
Face diagrams for both encryption and decryptions are shown which clearly indicates that modified encrypted program is very difficult to any kind of brute force attack.



```
Bad command or file name
Bad command or file name

1. Encrypt Text
2. Decrypt Text
3. Exit
Enter Your Choice : 1
Enter Text to be Encrypted (Max. 256 characters/ only alphabets):
 [illegible]
Enter Encryption Key (Max. 32 Characters/ only aphabets): manismortalhj
[illegible]
1. Encrypt Text
2. Decrypt Text
3. Exit
Enter Your Choice : 2
Enter Text to be Decrypted (Max. 256 characters/ only alphabets):
 [illegible]
Enter Decryption Key (Max. 32 Characters/ only aphabets): manismortalhj
[illegible]
1. Encrypt Text
2. Decrypt Text
3. Exit
Enter Your Choice : _
```

Figure: - Face diagram of Vigenère cipher algorithm

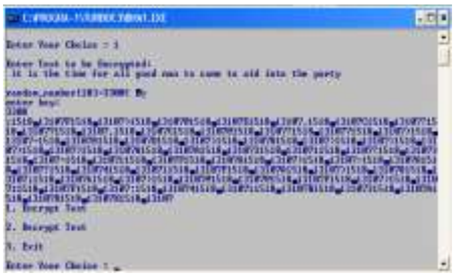


```
Enter Text to be Encrypted (Max. 256 characters/ only alphabets):
 [illegible]

rand key=[illegible]
Enter Encryption Key (Max. 32 Characters/ only alphabets): [illegible]
[illegible]
1. Encrypt Text
2. Decrypt Text
3. Exit
Enter Your Choice : 2
Enter Text to be Decrypted (Max. 256 characters/ only alphabets):
 [illegible]
Enter Decryption Key (Max. 32 Characters/ only alphabets): [illegible]
[illegible]
1. Encrypt Text
2. Decrypt Text
3. Exit
Enter Your Choice :
```

Figure: - face diagram of modification of Vigenère cipher algorithm

Implementation
#include <stdio.h>
#define SHR_LENGTH 4
#define COMPUTATION 1



```
Enter Your Choice : 1

Enter Text to be Encrypted:
 it is the time for all good men to come to aid into the party

random_number(1000-3000): [illegible]
enter key:
[illegible]
[illegible]
1. Encrypt Text

2. Decrypt Text

3. Exit

Enter Your Choice :
```

Implementation means install the software to the destination and make it to work there. Implementation is an ongoing process and can be achieved by one of the following methods:

1. The implementation of this paper is carried out in language “c” because of the following advantages.
2. C is a building block for many other currently known languages.
3. C is a compiled language versus an interpreted language.
4. A lot of libraries are written in C.
5. The main advantages of C language are that there is not much vocabulary to learn, and that the programmer can arrange for the program is very fast.
6. C has features that allow the programmer to organize programs in a clear, easy, logical way.
7. C is a portable language.

IV. Result and Discussion

1. Asymmetric Encryption is 100-1000 times slower than symmetric algorithms (RSA v. DES). Message can be transmitted faster than asymmetric Key.
2. Symmetric keys are subject to a brute force attack where all keys in the key space are tried systematically to break the encryption. As we are using Customized PN Generator Hybrid cryptography, there is no chance to pick up the actual signals during the transmission by the intruders.
3. Customized PN Generator Hybrid Cryptography is the better solution which ensures secrecy at terminal ends and during the transmission of the text.
4. Customized PN Generator Hybrid Cryptography is very important during the wars where each message has its own value. It is also important in business transactions.
5. Customized PN Generator Hybrid Cryptography ensures user authentication, bandwidth sharing, and security from eavesdropping and immunity to interference, and difficulty in detection, data encryption and key management.

Limitations

1. Using Customized PN Generator hybrid Cryptography can be a complex process and its concept is often difficult for some people to grasp.
2. Both parties must be able to use Customized PN Generator Hybrid Cryptography. It is impossible to use it unless people at both ends of the connection are capable of using this.

V. Conclusion

This dissertation discusses modification of Vigenère cipher which works by adding a key repeatedly into the plaintext using the convention that A = 0, B = 1, . . . , Z = 25; and addition is carried out modulo 26—that is, if the result is greater than 25, we subtract as many multiples of 26 as are needed to bring us into the range [0, . . . , 25], that is, [A, . . . , Z]. Mathematicians write this as: $C = P + K \bmod 26$ .For modification of Vigenère cipher, numbers, punctuations, mathematical symbols may be used for key in place of characters.

Modification of Vigenère cipher is more immune to any type of outsider attack. Random generated number increase the difficulty to decipher the message. Both encryption and decryption process are carried out using a single key. These algorithms are efficient, are secure, execute at high speeds, and consume less computer resources of memory and processor time.

VI. Acknowledgement

I would like to thank **Prof. R.K Pandey** for his guidance and help. His constant inspiration and timely suggestions helped me in collection all the information I needed for my thesis without much difficulty. Finally, I am highly obliged to all my family members for their support and blessings.

References

[1] Overview of Cryptography by Alfred J. Menezes

[2] M. Blaze, J. Feigenbaum, J. Ioannidis, A. Keromytis. Cryptography—G. Julius Caesar

[3] M. Abdalla, M. Bellare, and P. Rogaway.

[4] S. S. Al-Riyami and K. G. Paterson.

[5] Schneier, Bruce (1995-10- 9). Applied Cryptography. New York: 11.

[6] Schneier B.Applied Cryptography. John Wiley & Sons Inc., New York, New York, USA, 2nd edition, 1996.

[7] Stallings W. Cryptography and Network Security. Prentice Hall, Upper Saddle