International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Enforcing Reverse Circle Cipher for Network Security Using Multirotational Technique

Sajjade Zeba-Shazesh[1], **Aruna K. Gupta**[2]

[1]Research Scholar, JSCOE, PUNE, Pune, Maharashtra, India

[2]Professor, JSCOE IT, Pune, Maharashtra, India

Abstract: ***Encryption is the process where data or information is turned into cipher text then we coded it, so that it cannot be understood to unauthorized access. Once the message has been encrypted it is not possible for a person to read it though he or she possesses knowledge to decrypt the data by using key. The main objective is to use multirotational technique instead of linear rotational technique by using 'circular substitution' and 'reversal transposition' is to exploited the benefit of both confusion and diffusion, also we study coding and decoding of algorithm to implement successful crypto system by using symmetric poly alphabetic cipher for image cryptography and data compression technique using key length modification. User's authentication procedures will be design for data storage and retrieval. The user text file will be secured using Hybrid Cryptosystem before storing in network and building secure communication channel for text based files transmission and improve performance between client and server by reducing communication time. For this, we propose a method for secure text based files storage and secure text based files retrieval in network by using the Hybrid Cryptosystem. It provides two tier security using Vigenere cipher and reverse circle cipher with symmetric key multi rotational technique.***

Keywords: Buffer Size, Cipher text, Data Encryption, Data Decryption, Network Security

1. Introduction

To make reverse circle cipher we use confusion and diffusion principle by using ASCII (American standard code for information interchange) or UTF (Unicode transformation format) code [1] based on arithmetic coding for algorithm. We use circular substitution to reduce both time and space complexity to provide security for both personal and network security domains [2]. The complexity of algorithm is always based on size of encryption key. If the key is large, more complex is encryption program. In reverse circular cipher classical crypto technique is use whose algorithm weakness lies in the user selection key to run cryptanalysis. The weakness of reverse circular cipher algorithm is that, when encryption is over if any change in cipher text whole system data destroys. Used of simple block cipher scheme is to reduce time and space availability. Brute-force attacker tries each and every possible key on cipher text till plain text is obtained [3]-[4]. In this paper we are going to discuss two tier security approaches for cloud data storage and secure communication channel and the time complexity in cloud. The main feature of the this proposed system is that all cryptographic operations are performed on the client side, which provides the users more control on the security of their data, and thus the data are not dependent on the security solutions provided by the servers. In this proposed system, user data will be secured using Hybrid Cryptosystem before storing in cloud server. This system also helps to solve main security issues like malicious intruders, hacking, etc of cloud storage. Reverse circle cipher with symmetric key multi rotational technique is used for secured communication between the users and the servers. The proposed two tier Security approach in this paper is based on conventional crypto techniques that uses less time requirements and still maintain a adequate level of security.

2. Literature survey

The DES (Data encryption standard) is the most commonly used algorithm to work cryptography. It is use in public and private key encryption cipher such as RSA (Rivest Shamir, Adleman) uses in internet with PGP (Pretty Good Privacy) encryption. Another cipher AES (Advanced Encryption Standard) is used in security but it is not commonly accepted. All above mention cipher uses bit or byte level manipulation to convert plain text into cipher text. Vernam invented first poly alphabetic substitution automated cipher by using electrical impulses which had period equal to the length of key where each 5- bit key value determine one of 32 fixed mono alphabetic substitution.

2.1 Existing Reverse Circle Cipher

In this symmetric poly alphabetic cipher use of concept called circular substitution and reversal transposition, also it combines simple character level displacement principle of Caeser cipher, distribution principle of Vernam poly alphabetic cipher and the diffusion principle of Transposition cipher [6].This cipher provides security even with white box and grey box model in addition to black box models of attacks [8]-[9].

2.1 Existing Reverse Circle Cipher

In this symmetric poly alphabetic cipher use of concept called circular substitution and reversal transposition, also it combines simple character level displacement principle of Caeser cipher, distribution principle of Vernam poly alphabetic cipher and the diffusion principle of Transposition cipher [6].This cipher provides security even with white box and grey box model in addition to black box models of attacks [8]-[9].

2.2 Pros and Cons

No space is required for plain text and cipher text buffer for algorithm.

Advantages:

- Key length is a variable, not a fixed set of bits used in DES or AES.
- Speed of algorithm is independent of key size.
- Additional level of security is added with confusion and diffusion by circular substitution and reversal transposition.
- It requires less cost.

Disadvantages:

- This algorithm deals with text based files and even by knowing the algorithm it is difficult to decode.
- If any modification is done in the cipher text, whole file can become incorrect.

2.3 Future Scope

- System can create more confused cipher by introducing compression technique.
- The algorithm can enriched to use in any type of file.
- Variable size of bit size can be used

3. System Overview

Take input circular character key is KC and reversal length key KR. When encryption performs, the circular substitution takes place with plaintext as circular key input. The output is in the form of reversal transposition with the reverse length of key. In decryption only difference is, circular substitution function is the reversal of arithmetic function used in encryption as shown in figure1 [10]. Following are the equations used for cryptanalysis.

$$Ci = f(Pi, k(0 + len(k)i) \quad (1)$$

$$Pi = f^{-1}(Ci, k(0 + len(k)i) \quad (2)$$

Where,

+len (k) is the modular addition; i corresponds to position under operation.
Ci, Pi, (k)i corresponds to ith binary digit of cipher text, plain text and key respectively and (+) is XOR operation

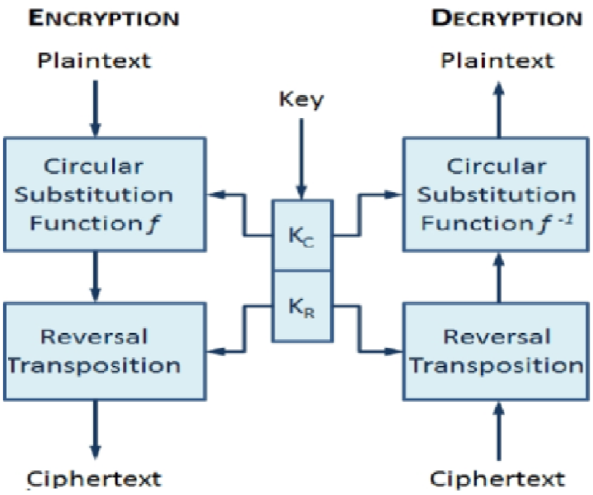


Figure 1: System architecture of the Reverse Circle Cipher

- ***Design modification:***

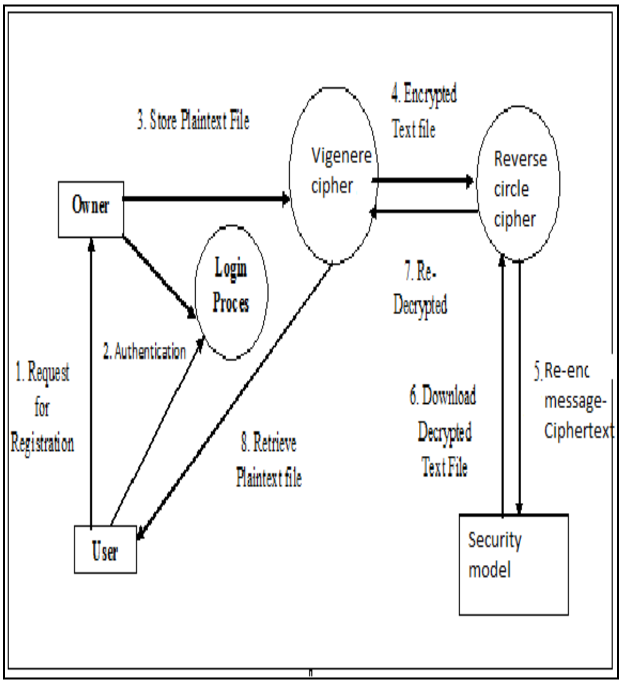


Figure 2: Encryption using Multi rotational technique

Hybrid cryptosystem is based on the combination of the poly alphabetic cipher Vigenere and the Reverse circle cipher with symmetric key multi rotational technique to give a new and more secure two tier security model. User who wants to go for cloud storage service must be an authorized user and register themselves as a client. The proposed system ensures that unauthorized users are not permitted to login. The authorized client can apply first tier security in text file using Vigenere cipher then Vigenere encrypted text file output will be given to second tier encryption i.e. Reverse circle cipher with symmetric key multi rotational technique as input. Finally output of reverse circle cipher with symmetric key multi rotational generate encrypted file that file upload into cloud. Fig.1. Shows the Outline of proposed hybrid cryptosystem. It provides processes for secure data storage and retrieval in cloud is as follows:

1. Registration Process.
2. Authentication Process.
3. First tier encryption. (Vigenere cipher)

4. Second tier encryption (Reverse circle cipher with symmetric key multi rotational technique).
5. Generated Encrypted & metadata file and Upload.
6. File Download and twice Decryption Process.

3.1 System Operation

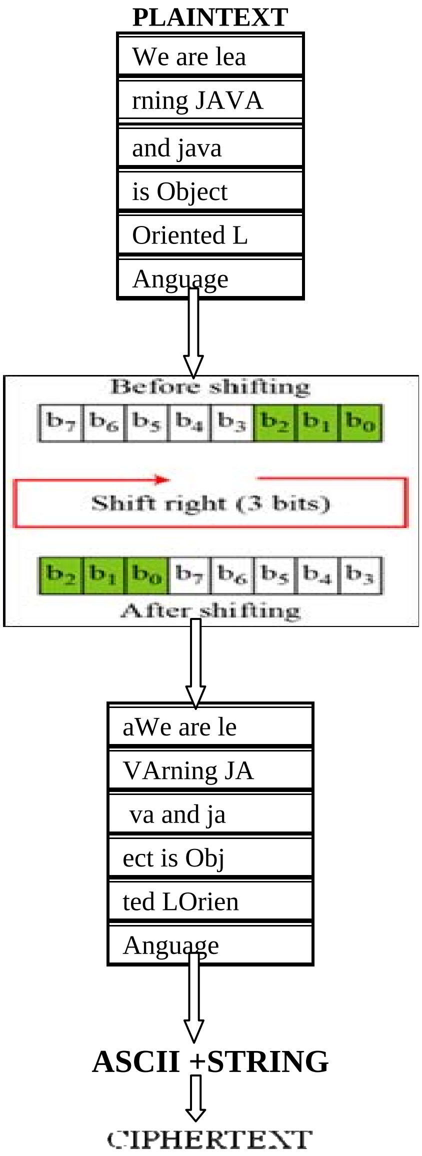


Figure 4: Operation Encryption and decryption using Multi rotational technique

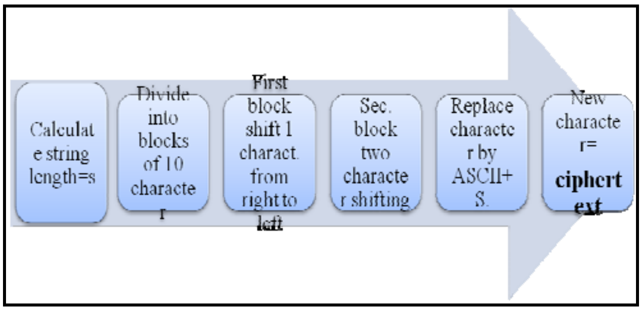

Calculat e string length=s
Divide into blocks of 10 characte r
First block shift 1 charact from right to left
Sec. block two characte r shifting
Replace characte r by ASCII+ S.
New characte r=
ciphert ext

Figure 3: System operation

1. String is converted array of character.
2. Divide the array in each block of 10 characters.
3. Rotate each block based on index position of vector+1.
4. Modify the ASCII of the characters to result a special character
5. Replace with special character.
6. Append all blocks to give a encrypted file.
7. Reverse step followed for decryption.

4. Two Tier Security Approach

The Proposed system consists of two tiers Security approach mainly works with the following security algorithms:

1. Vigenere cipher algorithm.
2. Reverse circle cipher algorithm with symmetric key multi rotational technique.

1. Vigenere Cipher Algorithm

Vigenere cipher is a simple poly alphabetic version of shift cipher, in which the cipher text is obtained by modular addition of a (repeating) key phrase and an open text (both of the same length). In Vigenere cipher, generate Pseudo key using Pseudo key generation algorithm using input file.

Same procedure for plaintext sees figure 2

Following are the proposed system diagram.

To achieve confusion principle, use of symmetric key multirotational technique is used instead of linear rotation which produces further confusion using ASCII code characters shown in figure 5.

2. Reverse Circle Cipher Algorithm

The Reverse Circle Cipher algorithm uses a concept called circular substitution with reversal transposition. It is a symmetric poly alphabetic block cipher [4].To make reverse circle cipher we use confusion and diffusion principle by using ASCII (American standard code for information interchange) or UTF (Unicode transformation format) based on arithmetic coding for algorithm. We use circular substitution to reduce both time and space complexity to provide security for both personal and network security domains. The complexity of algorithm is always based on size of encryption key.

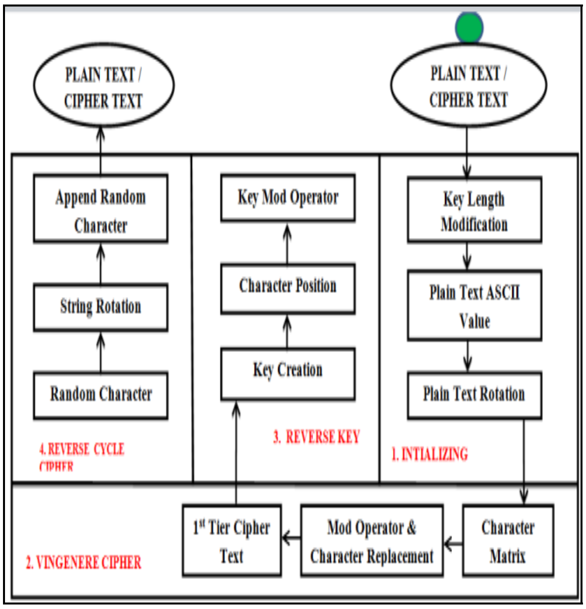


Figure 5: System architecture

If the key is large, more complex is encryption program. In reverse circular cipher classical crypto technique is use whose algorithm weakness lies in the user selection key to run cryptanalysis using the weakness of reverse circular cipher algorithm is that after encryption if we change in cipher text which cause error in whole system and destroy data. This simple block cipher scheme reduces both time and space complexity. Brute-force attacker tries every possible key on cipher text till plain text is obtained.

Algorithm design and platform:

Let us see the algorithm used for reversal circle cipher and modification what we introduce in between is use of multirotational substitution instead of linear substitution in step 11.Same thing is reverse for decryption. In algorithm see figure 6where,

P: Plaintext buffer,
C: Cipher text buffer, R: Reversal length hence buffer size.
Pi: Character at position i of plaintext buffer,
Ci: Character at position i of cipher text buffer, Ki: Character at position of i of the key.
+len(k): Modular addition with respect to key length taken as number of character.

Encryption:

```
Step 0: Start
Step 1: Get Input String S
Step 2: Initialize a String ENC as empty
Step 3: Divide the string S in N blocks of size 10 characters
Step 4: for I =1 to N
    Step 5: Let String BS =10 character of each block
    Step 6: rotate block with I characters in clock wise
    Step 7: for j=1 to 10
        Step 8: substitute each character
        Step 9: Replace character
    Step 10: End of inner for
    Step 11: ENC=ENC+BS
Step 12: End of Outer for
Step 13: Stop
```

Decryption:

```
Step 0: Start
Step 1: Get Input String S
Step 2 : Initialize a String DCR as empty
Step 3: Divide the string S in N blocks of size 10 characters
Step 4: for I =1 to N
    Step 5: Let String BS =10 character of each block
    Step 6: rotate block with I characters in anti clock wise
    Step 7: forj=1 to 10
        Step 8: substitute each character
        Step 9: Replace character
    Step 10: End of inner for
    Step 11: DCR=DCR+BS
Step 12: End of Outer for
Step 13: Stop
```

Figure 6: Algorithm multirotational technique in encryption and decryption

Mathematical Equation

$$Pi = f^{-1}(Ci, k(i) + len(k)) \quad (2)$$

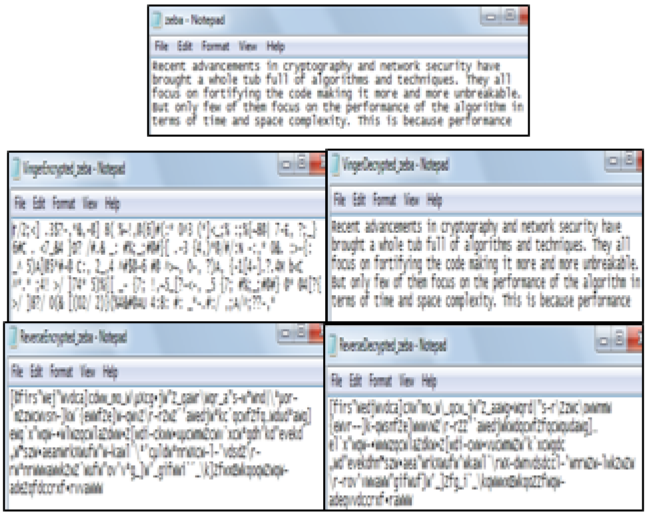
From equation (2) we get equation (3)

$$Rcp = \sum_{i=0}^{R} \sum_{j=0}^{R} Pi \quad (3)$$

Where,

R_{cp}= multi rotational cipher for plain text and cipher text, R= reverse circle

5. Experimental Results


zeba - Notepad
File Edit Format View Help
VingeEncrypted_zeba - Notepad
File Edit Format View Help
VingeDecrypted_zeba - Notepad
File Edit Format View Help
ReverseEncrypted_zeba - Notepad
File Edit Format View Help
ReverseDecrypted_zeba - Notepad
File Edit Format View Help

```
Recent advancements in cryptography and network security have
brought a whole tub full of algorithms and techniques. They all
focus on fortifying the code making it more and more unbreakable.
But only few of them focus on the performance of the algorithm in
terms of time and space complexity. This is because performance
```

[illegible]

```
Recent advancements in cryptography and network security have
brought a whole tub full of algorithms and techniques. They all
focus on fortifying the code making it more and more unbreakable.
But only few of them focus on the performance of the algorithm in
terms of time and space complexity. This is because performance
```

[illegible]

[illegible]

Figure 7: Cipher text Encrypted by Vigenere cipher, Cipher text Decrypted by the Reverse Circle Cipher symmetric key Multirotational technique

Table 1: Plaintext Size and Encryption and Decryption Time

Plaintext Size	*Encrypt time*	*Decrypt time*
25 Kb.Txt	22375	48250
30 Kb.Txt	8486	12797
35 Kb.Txt	15468	13625
40 Kb.Txt	15953	18735
45 Kb.Txt	30188	25688
50 Kb.Txt	28453	23576
55 Kb.Txt	33469	38891
60 Kb.Txt	24703	52859

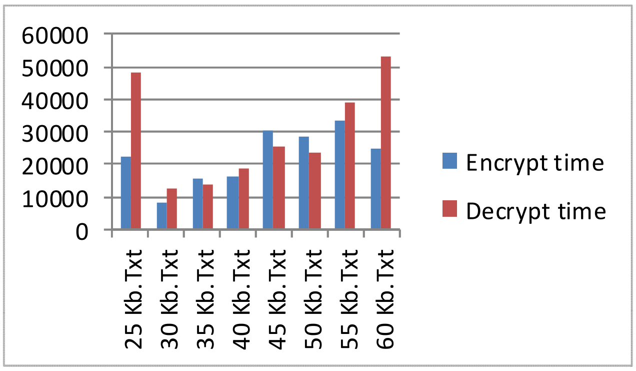


Figure 8: Comparison with data and encryption decryption time

In figure 8 shows the comparison of time and data means how much time required for encryption and decryption the data.

6. Conclusions

We are doing enhancement for reverse circle cipher for network security using multi rotational technique to provide satisfactory level of security for image cryptography and data compression technique using key length modification. The main aim is to securely store and manage the text based files using Vigenere cipher and the reverse circle cipher with symmetric key multi rotational technique so that only authorized users can have access stored files. The main advantage of this system is every time unique key is generated. This proposed system ensures strong authentication is implemented in performance with encrypted transmission. When the size of text file is increased then its computation time is increased, but we proposed one can decrease computation time by using appropriate approach and only space required for the plaintext and cipher text buffers, there is no additional space required for the computational part of the algorithm.

1. We use in complete Application Programming Interface.
2. This technique use in E-mail system and messaging.

References

[1] Linear cryptanalysis was presented by Mitsuru Matsui in 1993.

[2] [NICH99]Nichols, R. ed. ICSA Guide to Cryptography. New York: McGraw-Hill, 1999.

[3] [GARR01]Garrett P., "Making, Breaking Codes: An Introduction to Cryptology", Upper Saddle River, NJ: Prentice Hall, 2001.

[4] AamerNadeem et al, "A Performance Comparison of Data Encryption Algorithms", IEEE 2005.

[5] Yee Wei Law, JeroenDoumen, and Pieter Hartel, "Survey and Benchmark of Block Ciphers for Wireless Sensor Networks",Transactions on Sensor Networks (TOSN), ACM February 2006.

[6] BruceSchneier,"AppliedCryptographyProtocols,Algorithms,andSourceCodeinC",\JohnWileyandSonsInc.SecondEdition.pp.12-30.

[7] FUNDAMENTALS OF CRYPTOLOGY by Henk C.A. van TilborgbyEindhoven University of Technology The Netherlands.2007

[8] Sun Tzu, "The Art of War", translated by Lionel Giles, first published as part of the Project Gutenberg. URL: http://www.kimsoft.com/polwar3.htm IN 1910.

[9] Handbook of Applied Cryptography by A. Menezes, P. van Oorschot and S. Vanstone.

[10] AviKak, "Classical Encryption Techniques" (kak@purdue.edu), February 26, 2013.

[11] Ebenezer R.H.P. Isaac, Joseph H.R. Isaac and J. Visumathi, "Reverse Circle Cipher for Personal and Network Security".ebeisaac@gmail.com-2013

Author Profile

Sajjade Zeba-Shazesh received the B.E. degree in Computer Science and Engineering from Aditiya College of Engineering Beed, BAMU University, in 2007. Presently working as Senior lecturer with Department of Computer Engineering at JSPM's Group of Institutes, Pune since June 2008. In her post graduate course she is doing research work in enforcing reverse circle cipher for network security using multirotational technique.

Prof. Gupta Aruna K. M. E. She is working as an Associate Professor in Information Technology Department of J.S.P.M.S Jayawantrao Sawant College of Engineering, Hadapsar Pune-28, India