Volume 4, Issue 3, March 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Enforcing Reverse Circle Cipher for Network Security Using Multirotational Technique

Sajjade Zeba S.
Dept. of Computer Engineering,
Jayawantrao Sawant College of Engineering,
University of Pune, India

Gupta Aruna K.
Dept. of Information Technology,
Jayawantrao Sawant College of Engineering,
University of Pune, 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. Problem of normal encryption why people unable to choose to encrypt their data is because of complications in encryption, cost and problem to organize the data which has to be encoded. 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.

Keywords: Buffer Size, Cipher text, Decryption, Encryption, Network Security, Plain text.

I. 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].

The rest of the paper is organized as follows, Section II literature review for the reverse circle cipher. The design and implementation details with their merits and demerits are provided at section III. In section IV a discussion on conclusion and future scope is provided.

II. 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.

A: 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].

B: Frequency Distribution of Character:

It is the number of occurrence of each character used in a message of plain text. Through mapping substitution makes the brute-force cryptanalysis easier to start with substituting the character with highest frequency. The main goal of encryption is to dissolve the character distribution frequency to range of character so that an average cryptanalyst not know where to start decryption. In reverse circle cipher the cipher text slope continues to slowly increase at a greater rate than the plain text slope [10].

C. 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.

III. SYSTEM OVERVIEW

- *Existing System Architecture:*

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.

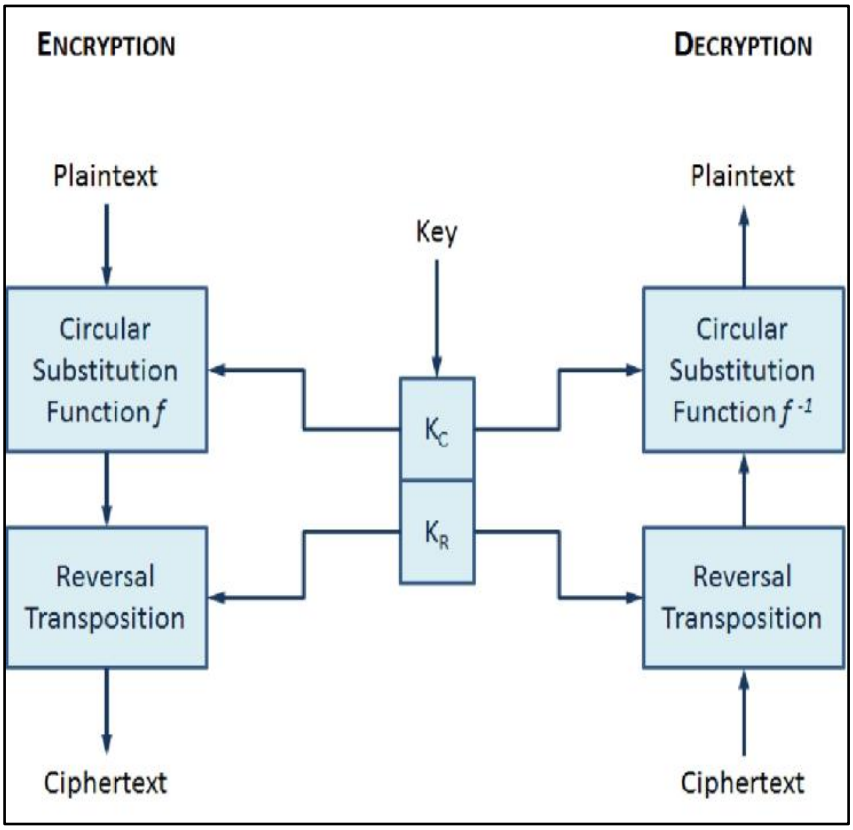

Fig. 1, System architecture of the reverse circle cipher

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.

$$\mathrm{Ci} = f(\mathrm{Pi}, \mathrm{k}(0 + \mathrm{len}(\mathrm{k})\mathrm{i}) \qquad (1)$$

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

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

- *Design modification:*

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 4.

Use-Case Diagrams:

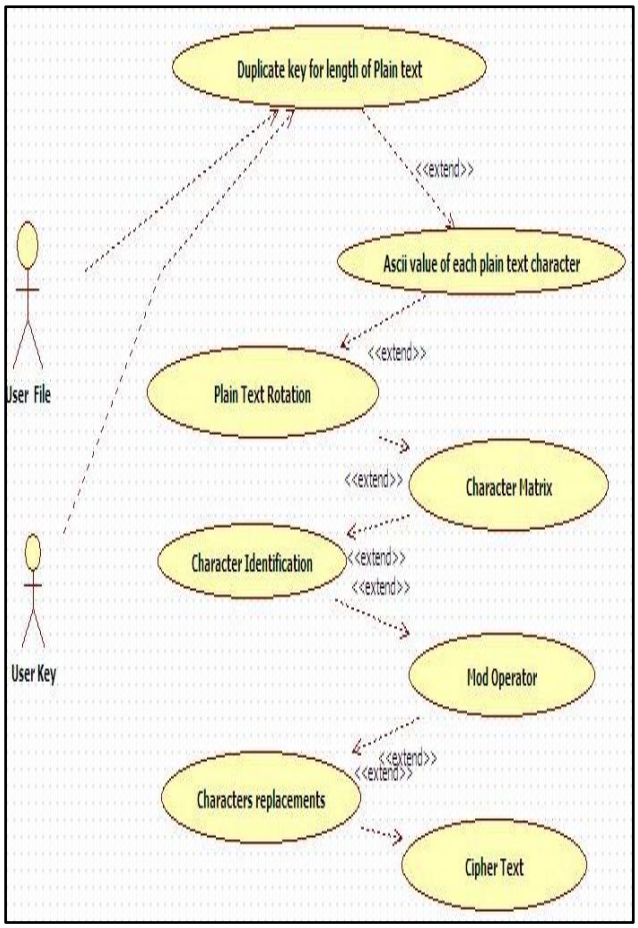

Fig. 2, First tier security using vigenere cipher

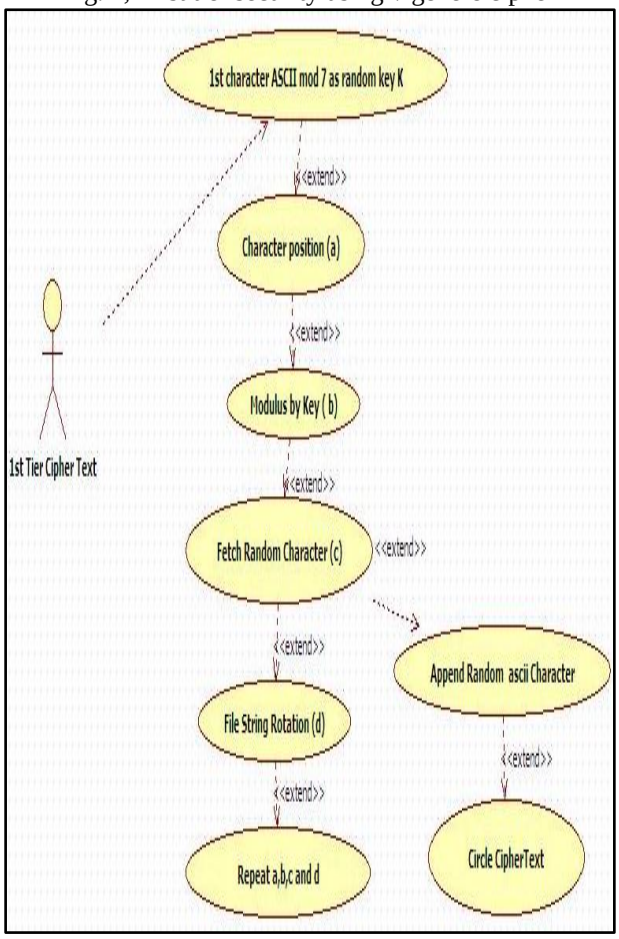

Fig. 3, Multirotational circle cryptography

Block diagram:

Following are the steps for system flow from plaintext to cipher text and vice versa.

1. *Initializing*

Step 1: take user Plain text/cipher text file.
Step 2: take user key length for plaint text.
Step 3: take ASCII value of each plain text character.
Step 4: plain text rotation for each rotation of Multirotational technique.

2. *Vigenere cipher*

Step 5: rotate multiple characters and arrange through character matrix.
Step 6: identify the character ASCII value.
Step 7:Apply Mod operator and replace the character from result of MOD operator.
Step 8: first tier cipher text of vigenere cipher achieved.

3. *Reverse key*

Step 9: take first tier vigenere cipher encrypted file.
Step 10: get the first character ASCII value and find key by applying MOD to ASCII value.
Step 11: set the character position.
Step 12: apply MOD operator for the character position.

4. *Reverse circle cipher*

Step13: Fetch a random character position for the index of step 12.
Step 14: Append Random Character
Step 15: Rotate the String by one character for each Random Character.
Step 16: Repeat steps from 13 to 15
Step 17: Write all the Random character String in a file.
Step 18: Store the encrypted file.
Same procedure for plaintext see figure4.
Following are the proposed system diagram.

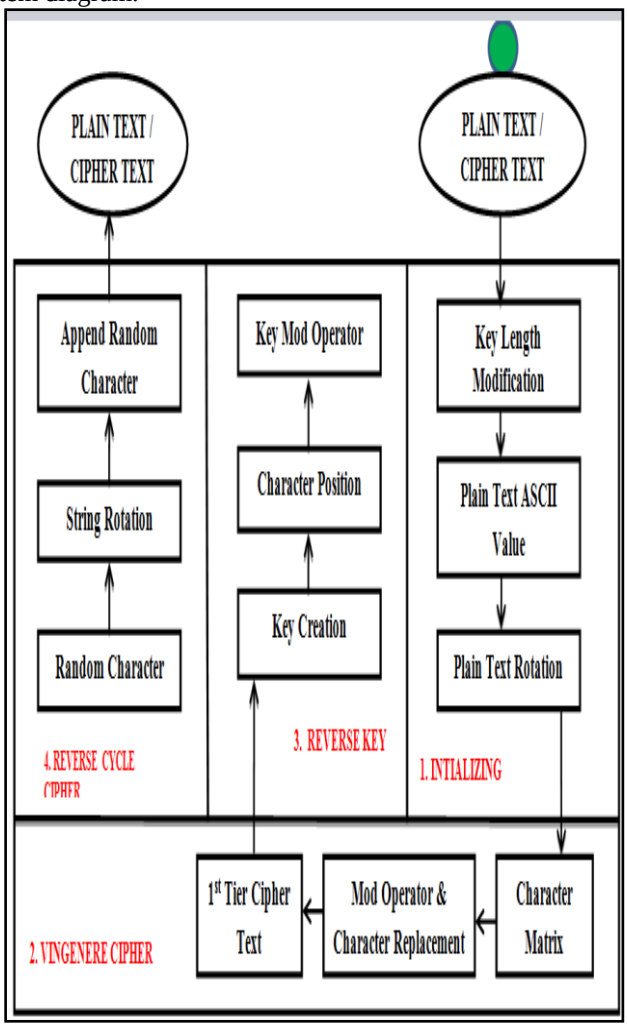

Fig.4, Data flow architecture

- *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 5where,

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: for j=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

Fig.5, Algorithm multirotational technique in encryption and decryption

Mathematical equation:

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

From equation (2) we get equation (3)

$$\mathrm{R_{cp}} = \sum_{i=0}^{R} \sum_{j=0}^{B} Pi \qquad (3)$$

Where,
$\mathrm{R_{cp}}$= multi rotational cipher for plain text and cipher text.
R= reverse circle cipher.
B= buffer size.

User of the system should have operating systems like Windows XP, Vista and Windows7. The system is implemented using JAVA. We required Minimum of Dual Core of 2.2 GHZ, 2GB RAM.

IV. CONCLUSION AND FUTURE SCOPE

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.

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

ACKNOWLEDGEMENT

Zeba S.Sajjade received her B.E. degree in Computer Science and Engineering from Aditiya College of Engineering Beed, BAMU University, in 2007.Currently she is teaching 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 by using multirotational technique.

Prof. Gupta Aruna K. Ph.D. (Pursuing), M. E. She is Working as an Asst. Professor in Information Technology Department of J.S.P.M.S Jayawantrao Sawant College of Engineering, Hadapsar Pune-28,

REFERENCES

[1] BruceSchneier*,"AppliedCryptographyProtocols,Algorithms,and Source Code inC",* JohnWiley andSonsInc.SecondEdition.pp.12-30.

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

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

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

[5] FUNDAMENTALS OF CRYPTOLOGY by Henk C.A. van Tilborgby*Eindhoven University of Technology The Netherlands.*

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

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

[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] 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.

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

