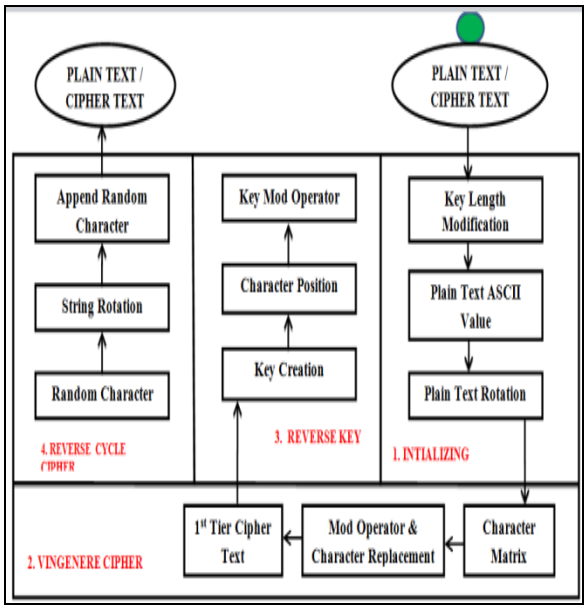

Figure 5: System architecture

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

$$Pt = f^{-1}(Ct, k(0 + len(k)) \quad (2)$$

From equation (2) we get equation (3)

$$Rcp = \sum_{i=0}^{n} \sum_{i=0}^{R} Pt \quad (3)$$

Where,

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

5. Experimental Results

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

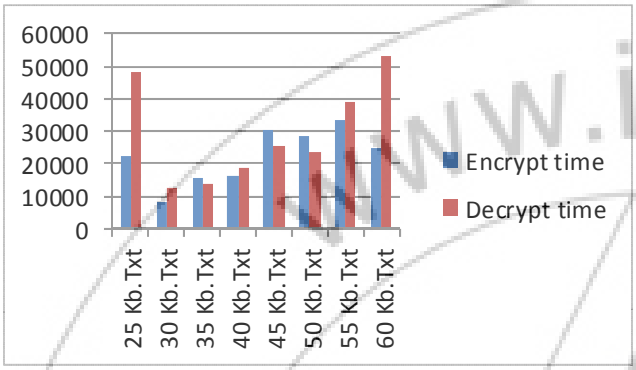

Figure 8: Comparison with data and encryption decryption time

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