A Cipher Design using the Combined Effect of Arithmetic and Logic Operations with Substitutions and Transposition Techniques

S.G.Srikantaswamy
Research Scholar
National Institute of Engineering, Mysore

Prof. H. D. Phaneendra
Research Guide & Professor, Department of CS
National Institute of Engineering, Mysore

ABSTRACT
Communication is a basic process of exchanging information**.** Information security is a very important aspect now a day. The introduction of internet and distributed system made the information security issue more challenging and complex. Cryptography plays a crucial role in providing security to data transmitted over the internetwork. Encryption is the most widely used technique used to scramble the data that is being transmitted over the network from sender to a receiver. The encryption algorithms are available practically and provide the security for user data and information. This paper presents an advanced encryption technique which combines the features of substitution and transposition. Five different key values being used in this algorithms and each key value is used to substitute the corresponding plaintext characters in association with addition operation. Each key value is twice as that of the previous one. The basic key value is a fixed one defined by the user. The transposition technique is employed by left shifting each bit of the data. The shifted data is complemented to alter the each bit of the cipher text that is being generated. The effort of the algorithm is to make the cryptanalysis difficult and to make the algorithm stronger.

Keywords
Information Security, Plaintext, Ciphertext, Key, Cipher, Substitution, Transposition.

1. INTRODUCTION
A Cryptosystem for a specified task is secure if no adversary of a specified power can achieve a specified break.[6].All cryptosystems are based on two general principles: Substitution, in which each element in the plaintext is mapped in to another element and , Transposition, in which characters in the plaintext are rearranged.[4] .Many encryption and decryption algorithms are widely available and being used for encrypting and decrypting the data [4, 5, 6]. Many encryption algorithm incorporates both substitution and transposition techniques [1, 2, 3]. Substitution cipher involves the replacing one or more characters in a message with one or more other entities may be other characters, symbols and numbers. There are several types of substitution ciphers available in the field of network security [4].Monoalphabetic substitution involves replacing each character or letter in the given message with another character of the alphabet. Polyalphabetic substitution involves the following features:A set of related monoalphabetic substitution rules is used.

- A key determines which particular rule is chosen for a given transformation.

In this paper, an encryption algorithm which incorporates the features of both substitution and transposition technique is proposed. To encrypt a message, a key value K is assumed. The first character of the message is added with the key value. The resultant value is then left shifted once. The left shifted value is then complemented using the logical NOT operation. The resultant complemented value is the final ciphertext value for the corresponding plaintext character. The second character is encrypted in the same manner but with a key value 2*K. The third character is complemented using the key value 3*K. The fourth character by 4*K and fifth by 5*K. The sixth character by K, Seventh character by 2*K and so on, with the value of K_j, where $1 \leq j \leq$ mod 6. The organization of the paper is gives as follows: Section 2 provides the complete encryption process details. Section 3 gives encryption algorithm details. Section 4 gives encryption and decryption results. Section 5 provides the features of the proposed scheme and Section 6 provides conclusions drawn from the analysis carried out on the above desired encryption and decryption algorithm. Section 7 gives references.

2. ENCRYPTION PROCESS
Consider a plaintext message say "NETWORK". Let the key be K. Now the five different versions of key values are derived based on first key value. Consider the first character of the plaintext message P_i. Let the key value used to substitute the first character of the plaintext be K_j, where $K_j = K$ and $1 \leq i \leq n$ and $1 \leq j \leq$ mod 6. The resultant substituted value of the plaintext is left shifted by one position. The shifted value of the plaintext is complemented to obtain the final ciphertext value for corresponding value of the plaintext (P_i). Now for the plaintext character P_2, the key value is used is K_2 where K_2 = 2*K. The above procedure is repeated to obtain C_2. Similarly to obtain C_3 from P_3, the key value used will be K_3 = 3*K, for C_4, key K_4 = 4*4, and finally for C_5, key K_5 = 5*K. Now for sixth character of the given message key value used will be K_1, for seventh character K_2 and so on. The value of i and j are such that $1 \leq i \leq n$, $j \leq 1 \leq$ mod 6.

3. ENCRYPTION ALGORITHM

Step 1: Start
Step 2: Input the plaintext message P_i, $1 \leq i \leq n$.
Step 3: Declare the key value K.
Step 4: Generate 5 different key values K_j, $1 \leq j \leq$ mod 6, $K_1 = K$, $K_2 = 2*K$, $K_3 = 3*K$, K4 = 4*K, K5 = 5*K;
Step 5: $C_i = P_i + K_j$;
Step 6: Repeat for i = 1 to n
j = 1 to mod 6
$C_i = P_i + K_j$;
C^1_i = Left shift (C_i);
$[C_i]_{final}$ = One's Complement of $[C^1_i]$;
Output $[C_i]_{final}$
Step 7: Stop

4. ENCRYPTION AND DECRYPTION RESULT

Example 1: Consider the plaintext message "NETWORK".
The Encryption and Decryption results produced by the Algorithm are as follows

Table 1: Encryption

Plaintext Character	ASCII Value	Binary Equivalent	Add key Value Let K=25 $C_i = P_i + K_j$ $1 \leq i \leq n$ $j \leq 1 \leq$ mod 6	Left Shift $C_i = C^1_i$	Complement $C^1_i = C_{i\ final}$	ASCII Equivalent value of Ciphertext
N	46	01000111	71	10001110	01110001	113
E	37	01010111	87	10101110	01010001	81
T	52	01111111	127	11111110	00000001	01
W	55	10011011	155	00110111	11001000	200
O	47	10101100	172	01011001	10100110	166
R	50	01001011	75	10010110	01101001	105
K	43	01011101	93	10111010	01000101	69

Table 2: Decryption

ASCII Equivalent value of Ciphertext	Binary Equivalent Of C_i	Complement C_i	Right Shift C_i once	ASCII Equivalent Of C_i	Subtract Key value K_j from C_i	Resultant Plaintext Character P_i
113	01110001	10001110	01000111	71	46	N
81	01010001	10101110	01010111	87	37	E
01	00000001	11111110	01111111	127	52	T
200	11001000	00110111	10011011	155	55	W
166	10100110	01011001	10101100	172	47	O
105	01101001	10010110	01001011	75	50	R
69	01000101	10111010	01011101	93	43	K

Example 2: Consider the plaintext message "CIPHER".
The Encryption and Decryption results produced by the Algorithm are as follows:

Table 3: Encryption

Plaintext Character	ASCII Value	Binary Equivalent	Add key Value Let K=25 $C_i = P_i + K_j$ $1 \leq i \leq n$ $j \leq l \leq \text{mod } 6$	Left Shift $C_i = C^1{}_i$	Complement $C^1{}_i = C_{i\ final}$	ASCII Equivalent value of Ciphertext
C	67	01000011	92	10111000	01000111	71
I	73	01001001	123	11110110	00001001	09
P	80	01010000	155	00110111	11001000	200
H	72	01001000	172	01011001	10100110	166
E	69	01000101	194	10000101	01111010	122
R	82	01010010	107	11010110	00101001	41

Table 4: Decryption

ASCII Equivalent value of Ciphertext	Binary Equivalent Of C_i	Complement C_i	Right Shift C_i once	ASCII Equivalent Of C_i	Subtract Key value K_j from C_i	Resultant Plaintext Character P_i
71	01000111	10111000	01011100	92	67	C
09	00001001	11110110	01111011	123	73	I
200	11001000	00110111	10011011	155	80	P
166	10100110	01011001	10101100	172	72	H
122	01111010	10000101	11000010	194	69	E
41	00101001	11010110	01101011	107	82	R

5. FEATURES OF THE SCHEME

- Involve simple coding
- Low processing delay
- Simple to analyze
- Incorporates both substitution and transposition
- Fast response.

6. CONCLUSION

The security aspect is a more important in data communications over internet-works. Active attacks involve both modification and fabrication of messages. The goal of the encryption algorithm designing is to frustrate the hackers and makes the cryptanalysis difficult. The key value play more important role in encryption process. The processing speed,coding factors also plays a very important role. Using different key values for encrypting consecutive characters of plaintext hides the relationship between the ciphertext and plaintext. Altering each value of the ciphertext generated to get the final ciphertext make the cryptanalysis still more complex.The algorithm provides appreciable data security and requires minimum coding .The algorithm can be applied to message of any length.

7. REFERENCE

[1] Information Security**:** Text Encryption and Decryption with Poly Substitution method and combining features of cryptography.-R.Venkateswaram, Dr.V.Sundaram , June 2010.

[2] A modified Hill cipher Involving Interweaving and Iteration.- V. Umakanta Sastry, N. Ravi Shankar and S. Durga Bhavani , July 2010.

[3] A block cipher having a key on one side of plaintext Matrix and its Inverse on the other side. Dr. V. U. K. Sastry, Prof. D. S. R. Murthy, Dr. S. Durga Bhavani .

[4] Cryptography and Network Security Principles and Practices, Third Edition – William Stallings

[5] Applied Cryptography Protocols, Algorithms and Source Coding BRUE SCHNEIER, Second Edition, John Wiley & Sons, Inc.

[6] Introduction to Modern Cryptography, Jonathan Katz, Yehuda Lindell Chapman & Hall / CRC Taylor R Francis Group.