A Novel Approach of Symmetric Key Cryptography

Sanjeev Kumar
Department of Computer Applications
G L Bajaj Institute of Technology & Management
Greater Noida, India
Sanjeevnmc83@gmail.com

Madhu Sharma Gaur
Department of Computer Applications
G L Bajaj Institute of Technology & Management
Greater Noida, India
madhu14nov@gmail.com

Prem Sagar Sharma
Department of Computer Applications
G L Bajaj Institute of Technology & Management
Greater Noida, India
Premsagar1987@rediffmail.com

Deepkiran Munjal
Department of Computer Applications
G L Bajaj Institute of Technology & Management
Greater Noida, India
Deepa.munjal@gmail.com

2021 2nd International Conference on Intelligent Engineering and Management (ICIEM) | 978-1-6654-1450-0/20/$31.00 ©2021 IEEE | DOI: 10.1109/ICIEM51511.2021.9445343

***Abstract*- Cryptography plays an important role in secured data communication over the network using unknown, untrusted mediums. In the fast digital transformation, traffic on network increasing rapidly where users are always connected, being online, anytime anywhere. As part of data, extortions like altering, spoofing and snooping of are quite common over the network by unauthorized access. Cryptography is well known mechanism where asymmetric or symmetric algorithms using public or private keys provide secure data communication. There are many more cryptography algorithms existing but with emerging technologies and diverse application domains seeking consistent enhancement and better performance with resource restriction. In this paper, we present a novel symmetric cryptography technique based on Caesar cipher symmetric cryptography technique to transform the original text/message into secret text/message. In this technique, the sender transmits hash code instead of symmetric key and Hash code provides the symmetric key to the receiver to decrypt the message of a sender. Proposed method works for all 256 characters having ASCII value from 0 to 255.**

Keyword- Cryptography, Encryption, Decryption, Symmetric Key, Network Security

I. INTRODUCTION

Cryptography is a term made from two Greek words “kryptos” means hide and “graphein” means write, it is an art and science of hiding the data from unauthorized users during the time of storing and transmission[1]. In every field, security of confidential data is the biggest concern, especially in online banking and reservation system, so that nobody can change and access the data for illegal use. To prevent such circumstance, preferred technique is cryptography that converts the data into an indescribable code form (cipher) at sender side, and decode into readable form at receiver side. The main objective of cryptography technique is to convert the data into non-readable form so that only authorized user can access the data, and in any situation the attacker should not have any chance to access the database server or secrete data [2][3].

Cryptography carried out into two different phases' encryption and decryption. Encryptions as well as decryption both are important aspects of security. In encryption process[4], plain text or secret message converted into a weird message or scrambled one known as cipher text with the help of secret key and, in the decryption process, cipher text is converted back to plain text with the help of same secret key used in encryption process.

Caesar cipher is one of the oldest and commonly used encryption decryption methods in Cryptography. Firstly, Julius Caesar used this method at the time of Gallic Wars to communicate with army officers that is why commonly known as Caesar cipher. It said that *Caesar* was the first person to applied encryption method in order to provide security of confidential data. Caesar decided to make a simplest encryption code to secure the message because his soldiers were not more educated to understand the complicated coding method[5][6].

In cryptography, transposition and substitution methods are widely used for data conversion into non-readable form. But Caesar cipher is based on substitution cipher method in which each character in the plaintext is replaced by a fixed character that depends upon the shiftingposition of the initial character[7][8].

The encryption and decryption process in this method mostly performed by modular arithmetic[9].

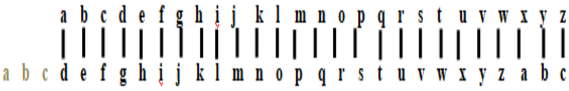

a b c d e f g h i j k l m n o p q r s t u v w x y z
a b c d e f g h i j k l m n o p q r s t u v w x y z a b c

Fig. 1. Caesar cipher working

Caesar developed character shifting (shown in fig-1) based encryption method, where each character shifting three place down to its current position in the message, and after that a lot of improvement has been done in the original Caesar cipher character shifting method using 26 arithmetic modulo method to generate encryption key given as

$$CT = (PT + N)\ mod\ 26 \qquad (1)$$

Where PT, CT and N, are the plaintext, cipher text, and the number of shift respectively. One of the main drawback of this cipher method is that, it is very simple to encrypt and decrypt, and can be decrypted without having encryption key. It is easy to crack because the decryption process is the reverse process of encryption process as given below [8]

$$PT = (CT - N)\ mod\ 26 \qquad (2)$$

One more problem with this cipher method is that, if someone already knows that how one alphabet is

978-1-6654-1450-0/21/$31.00 ©2021 IEEE

deciphered, and then it will be very easy to identify the number of shift, and decrypt the whole message.

II. Related Work

Caesar cipher encryption method is one of the simplest traditional method firstly used by Julius Caesar at the time of Gallic Wars, since the time various Caesar cipher method based on symmetric key have been developed by different techniques as discussed in [5]and in the literature.

Sourabh Chandra et al[1], used mathematical models to develop a Caesar Cipher symmetric key encryption technique that convert the original data into secure information. In this method plaintext can contains case sensitive characters, numbers and special symbols. The proposed model have used Caesar Cipher key concept to normalize the encryption method. The generated cipher text contains a lot of special symbols and numbers, which is very hard to understand for the unauthorized person.

In [10], the author developed a text based symmetric key algorithm that used secure key to transmit the data through the network. The focus of the model is to generate secure key using circular bit shift operation and folding method with binary addition operation. The limitation of the proposed model is that it can work with string and 8-bit data only.

Benni Purnama et al [2],altered (Monoalphabetic Substitution) the Caesar Cipher techniques to produce the cipher text in readable form. In this method all 26 alphabets are divided into two parts i.e. vowels and consonants, and the alphabet replacement method has been used that replaced vowels by alphabet vowels too, and consonants replaced by alphabet consonants. However, some consonant alphabets not replaced due to the Indonesian text. The only replace position of alphabet. In this method the plaintext has encrypted at each level with same and different key.

Atish Jain et al [14], proposed a modified and expanded mathematical model for Caesar cipher encryption by combining three method namely affine ciphers, transposition ciphers and randomized substitution in order to create strong cipher text that is hard to decode. In this method a key is generated by randomized substitution which is partitioned into two different keys and combined with double column transposition[15]ciphers to create secure cipher text. The experimental results shows that it is impossible to decode the cipher by the brute force method even the cryptanalysis have used 256 distinct combinations of keys. In [14], the author have developed a multilevel algorithm for Caesar cipher using substitution and Rail fence transposition method to obtain ciphertext that is difficult to crack. Priyadarshini Patil et al [16], gave a detailed study of implementation and performance analysis of various cryptography algorithm like AES, DES, RSA, blowfish and 3DES in terms of time and memory used for encryption and encryption. Sourabh Chandra et al [1]gave a detailed survey of symmetric key cryptography and its use with different encryption methods.

Pankaj Kumar Keserwani et al in [17], a hybrid symmetric cryptography have been developed by combining Affine cipher and Hill cipher technique to provide more security. In this method, a matrix of 473 property of the hill cipher used to make the system more robust. This system uses multiple shared symmetric keys and can be in any field for encryption and decryption like chat in order to show the performance of the model.

A number of Caesar cipher encryption techniques have been proposed so far with different method as discussed in[18], the author proposed ASCII value based shifting and transposition of plaintext alphabets in the form of matrix. In [19] a modified Caesar cipher method was proposed to generate secure cipher with the help of digits, symbols, lower and upper case alphabets to enhance the performance of the model. The obtained cipher text is hard to crack because the size of key is 82, so brute force cryptanalyst has to try 82(factorial) key combinations. S. N. Gowda[20], combined Diffie-Hellman key swapping method and simple mathematics to provide quick encryption and more security. D. Ginting et al [21] proposed a multilevel encryption technique by combined three traditional algorithm namely affine chipper and Caesar chipper and transposition chipper to enhance the level of security. In the first phase affine chipper and Caesar chipper are combined to make the cipher dynamic that display in binary digit form and then implement transposition to represent the cipher in rice cultivation groove pattern obtained cipher text read, at that point the cryptanalyst not suspicious of the received message.

KashishGoyal et al [11], proposed substitution Caesar Cipher encryption and decryption method using integer value. The author modified the traditional cryptography (Caesar Cipher) in its own way by using alphabet index value. In this technique when a key has generated, the index value of the alphabet is checked, if the index value is even then increase the index value by one else decrease by one. The limitation of this model was that it requires more memory, and needs some enhancement in the model. Greetta Pinheiro et al [12], developed a multilevel encryption technique for secure Caesar cipher using face values and place values of the respective alphabet as the key.

A Caesar Cipher encryption and decryption techniques have discussed in [13], where the author have used substitution and multilevel row transposition method for encryption and decryption process, which provides more strong ciphertext. Substitution method has been used for alphabet replacement with any other alphabet and multilevel row transposition Ciphers used to represents the plaintext in the form of matrix.

III. Proposed Symmetric Key Cryptography Method

The proposed symmetric key cryptography (shown in fig-2) provides a highly secure environment over the existing Caesar cipher cryptography and A Modified Symmetric Key Cryptography Method [10]. It can accepts all alphabets (a-z, A-Z), digits (0-9) and Special characters in the plaintext. It is double secure symmetric key data encryption technique. In this technique sender transmit hash code instead of symmetric key and Hash code provide same key (symmetric key) to receiver to decrypt message of a sender.

Proposed method work for all256 characters having ASCII value from 0 to 255.Fig 3 represents the working flow of proposed symmetric cryptography.

A. *Components of Proposed Technique*

a. *Plain Text*-it is a basic term used in cryptography which refer original message before encryption.

b. *Symmetric Key*- it is a code which used to encrypt a message at sender end and same code used to decrypt a message at receiver end in symmetric key cryptography.

c. *Hash Code Generator* – it is process which used to generate hash code corresponding symmetric key.

d. *Hash Code*- It is an integer value which associated with symmetric key. <Hash code, symmetric key length> transmit over the secure or unsecure channel. Key generator process at receiver end used to generates symmetric key corresponding hash code.

e. *Encryption Algorithm*-it is a mathematical process to translate original message (plain text) into encrypted message (cipher text) using a key before transmitting secure data over network.

f. *Cipher Text*-A meaningless code/text which generated by encryption algorithm. Cipher text is transmits over network.

g. *Secured Channel*- it is a confidential way to transferring secure data (cipher text).

B. *Decryption Algorithm*-It is also a mathematical process used to retrieve original message (Plain Text) from Encrypted message (Cipher Text) using a secure key. *Encryption Algorithm*

- Read first character (V) from a given plain text
- Generate ASCII Value for (V) for a character of a given plain text
- Generate Symmetric Key:
  - B= binayNumber (V)
  - Key= (Append (B, Revese_bits (B)))$_{10}$
  - hash_key=generate_hash_Code(Key, Key_length);
- Generate Cipher Text for give Plain Text:
- 1 for all character ch_i of plain text
  Cipher$_i$=(ch_i+Key)%256
- Transmit <Cipher ,hash_key, key_length> to receiver over the network.
- End

For Example: Data Encryption Process

Enter Plain Text=> “President of India”
Proposed Encryption technique get first character V= ‘P’ to generate symmetric key by using step-3 of encryption algorithm.
B=Binary(V) => $(1010000)_2$
Key= (Append (B, Reverse_bits(B))) =>
(1010000 00000101) // Reverse bit convert into 8 bits by appending zeros in left side.
Key= 20485
// it is the decimal value of $(1010000\ 00000101)_2$
Hash Code=generate_hash_Code(20485, 5);
// define this function into procedure-1
Hash Code => 1851139
Generate cipher text using step-4 defined in above encryption algorithm
Cipher Text =>Uwjxnijsy%tk%Nsinf

C. *Decryption Algorithm*

- Receiver receive <hash_key,key_length, Cipher Text> from Sender
- Retrieve Symmetric Key:
  - Key= find_symmetric_key(hash_code, Key_length);
- Generate Plain Text:
  - for each character cipher$_i$ for received cipher text:
  - plain$_i$= (cipher$_i$- Key)%256
- End

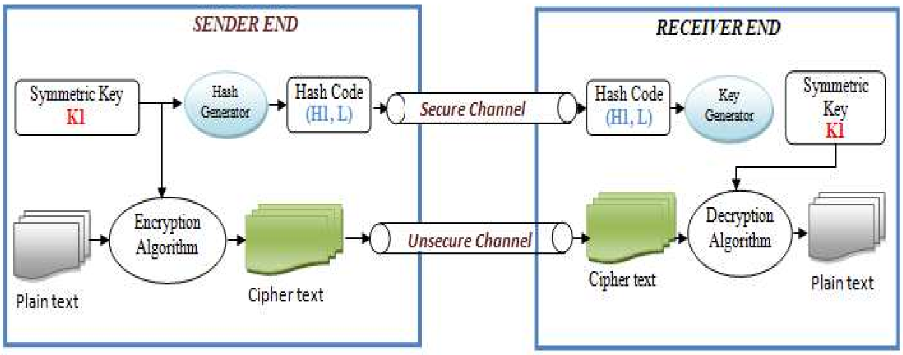


Fig. 2. Proposed Symmetric Encryption and Decryption Technique

For Example: Data Decryption Process

Cipher Text =>Uwjxnijsy%tk%Nsinf

Step-2 is used to retrieve the symmetric key from <hash code , key length>

Key= find_symmetric_key (hash_code, Key_length); // this function is defined in implementation part
Key=find_symmetric_key(1851139,5);
Key => 20485
Step -3 is used to generate plain text from cipher text
plain$_i$= (cipher$_i$- Key)%256

Palin Text =>Uwjxnijsy%tk%Nsinf

IV. Implementation And Results

All the procedures which are used in Encryption & Decryption Algorithms are defined below. Driver functions for both algorithms are also defined:

PROCEDURE-1: Generate Hash Code for Symmetric Key at Sender End

```
unsigned long intgenerate_hash_Code (unsigned long int
key, unsigned long intkey_len)
{
unsigned long inthash_value = 0,i;
for (i = 0; i<key_len ; i++) {
        hash_value = hash_value + (pow(31,i) * (key %
10));
        key=key/10;
   }
returnhash_value;
}
```

PROCEDURE-2: Reverser binary code of first character of plain text

```
unsignedintreverse_input_eight_bits_text(unsigned int
number)
{
        unsignedintreverse_bits = 0;
        while (number> 0)
        {
        reverse_bits<<= 1;
                if (number& 1 == 1)
                        reverse_bits^= 1;
                number>>= 1;
        }
        returnreverse_bits;
}
```

PROCEDURE-3: Generate Symmetric Key at Sender End

```
unsignedintgenerate_Symmetric_Key(unsigned
intbinary_first_char, unsigned intreverse_bits)
{
        return ( (binary_first_char& 0x00ff)<<8 |
(reverse_bits& 0x00ff));
}
```

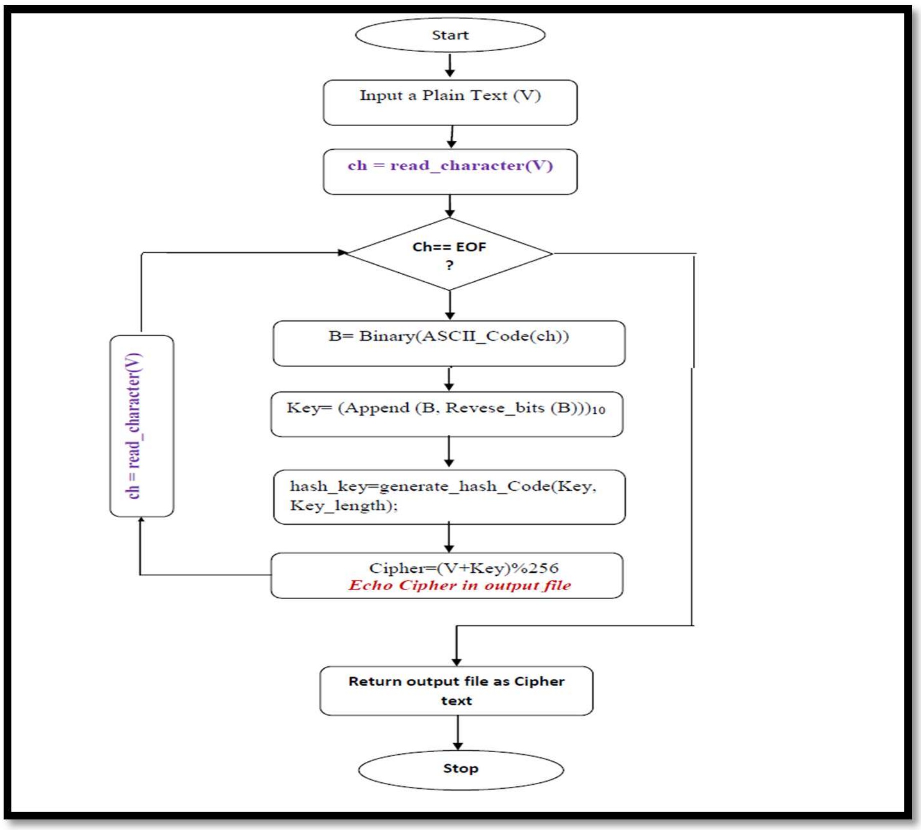

Start
Input a Plain Text (V)
ch = read_character(V)
Ch== EOF
?
B= Binary(ASCII_Code(ch))
Key= (Append (B, Revese_bits (B)))10
hash_key=generate_hash_Code(Key,
Key_length);
Cipher=(V+Key)%256
Echo Cipher in output file
ch = read_character(V)
Return output file as Cipher
text
Stop

Fig. 3. Flow char of proposed Symmetric Encryption and Decryption Technique

PROCEDURE-4: Generate Symmetric Key from hash Code at Receiver End

```
unsigned long
intgenerate_symmetric_key_decoderEnd(unsigned long
inthash_code, unsigned long intkey_len)
{
unsigned long int key = 0, quotient ;
inti;
for (i = key_len-1; i>=0 ; i--) {
quotient = hash_code/(pow(31,i);
            key=10*key + quotient;
            hash_code=hash_code % (pow(31,i);
            }
return key;
}
```

PROCEDURE-5: Find number of digits in symmetric key at Sender End

```
intfind_key_len(int key)
{
int count=0;
while(key>0)
    {
            key=key/10;
            count=count+1;
    }
return count;
}
```

Driver Code-1: Encryption Algorithm

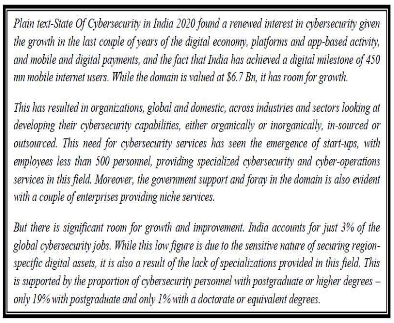
```
FILE *fp,*fw;
char plain[2000];
fp= fopen("author_plain_at_sender.txt", "r");
fread(plain,2000,1,fp);
n=strlen(plain);
x=reverse_input_eight_bits_text((int)plain[0]);
key=concatinate_num_rev_num((int)plain[0],x);
key_len=find_key_len(key);
hash_code=generate_hash_Code(key,key_len);
                        for(i=0;i<n;i++)
                        {
                        cipher[i]=(key+(int)plain[i])%256;
                        }
            printf("\nPlain Text  => %s",plain);
            printf("\nKey         => %ld",key);
            printf("\nHash Code   => %ld",hash_code);
            printf("\nCipher Text => %s",cipher);
fw=fopen("auther_cipher.txt", "wb");
fwrite(cipher,2000,1,fw);
fclose(fp);
fclose(fw);
```

Driver Code-2: Decryption Algorithm

```
charplain_d[2000],cipher[2000];
fp=fopen("auther_cipher.txt", "r");
fread(cipher,2000,1,fp);
key_d=generate_symmetric_key_decoderEnd(hash_code,key_len);
printf("\nCipher Text => %s",cipher);
printf("\nKey at Receiver END        => %ld",key_d);
printf("\nPalin Text at Receiver END =>");
n=strlen(cipher);
for(i=0;i<n;i++)
plain_d[i]=(((int)cipher[i])-key_d)%256;
fw=fopen("author_plain_at_receiver.txt", "wb");
fwrite(plain_d,2000,1,fw);
            fclose(fp);
fclose(fw);
```

V. RESULTS

User uploads "author_plain_at_sender.txt" file an input to encrypt data using proposed encryption algorithm before transmitting over network:

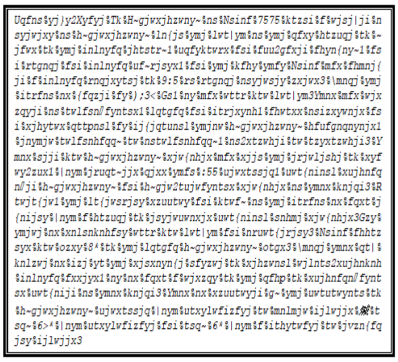


Plain text-State Of Cybersecurity in India 2020 found a renewed interest in cybersecurity given the growth in the last couple of years of the digital economy, platforms and app-based activity, and mobile and digital payments, and the fact that India has achieved a digital milestone of 450 mn mobile internet users. While the domain is valued at $6.7 Bn, it has room for growth.

This has resulted in organizations, global and domestic, across industries and sectors looking at developing their cybersecurity capabilities, either organically or inorganically, in-sourced or outsourced. This need for cybersecurity services has seen the emergence of start-ups, with employees less than 500 personnel, providing specialized cybersecurity and cyber-operations services in this field. Moreover, the government support and foray in the domain is also evident with a couple of enterprises providing niche services.

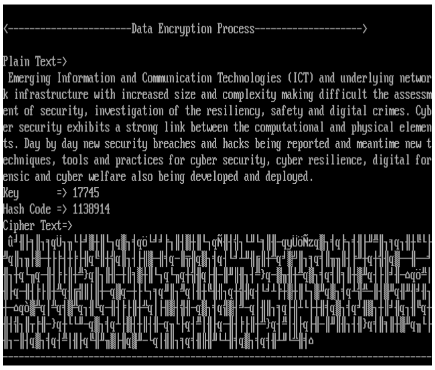
But there is significant room for growth and improvement. India accounts for just 3% of the global cybersecurity jobs. While this low figure is due to the sensitive nature of securing region-specific digital assets, it is also a result of the lack of specializations provided in this field. This is supported by the proportion of cybersecurity personnel with postgraduate or higher degrees – only 19% with postgraduate and only 1% with a doctorate or equivalent degrees.

Proposed encryption algorithm generate "author_cipher.txt" file as a cipher text.



```
Uqfns%yj}y2Xyfyj%Tk%H~gjwxjhzwny~%ns%Nsinf%7575%ktzsi%f%wjsj|ji%n
syjwjxy%ns%h~gjwxjhzwny~%ln{js%ymj%lwt|ym%ns%ymj%qfxy%htzuqj%tk%~
jfwx%tk%ymj%inlnyfq%jhtstr~1%uqfyktwrx%fsi%fuu2gfxji%fhyn{ny~1%fs
i%rtgnqj%fsi%inlnyfq%uf~rjsyx1%fsi%ymj%kfhy%ymfy%Nsinf%mfx%fhmnj{
ji%f%inlnyfq%rnqjxytsj%tk%9:5%rs%rtgnqj%nsyjwsjy%zxjwx3%\mnqj%ymj
%itrfns%nx%{fqzji%fy%);3<%Gs1%ny%mfx%wttr%ktw%lwt|ym3Ymnx%mfx%wjx
zqyji%ns%twlfsn∥fyntsx1%lqtgfq%fsi%itrjxynh1%fhwtxx%nsizxywnjx%fs
i%xjhytwx%qttpnsl%fy%ij{jqtunsl%ymjnw%h~gjwxjhzwny~%hfufgnqnynjx1
%jnymjw%twlfsnhfqq~%tw%nstwlfsnhfqq~1%ns2xtzwhji%tw%tzyxtzwhji3%Y
mnx%sjji%ktw%h~gjwxjhzwny~%xjw{nhjx%mfx%xjjs%ymj%jrjwljshj%tk%xyf
wy2zux1%|nym%jruqt~jjx%qjxx%ymfs%:55%ujwxtssjq1%uwt{ninsl%xujhnfq
n∥ji%h~gjwxjhzwny~%fsi%h~gjw2tujwfyntsx%xjw{nhjx%ns%ymnx%knjqi3%R
twjt{jw1%ymj%lt{jwsrjsy%xzuutwy%fsi%ktwf~%ns%ymj%itrfns%nx%fqxt%j
{nijsy%|nym%f%htzuqj%tk%jsyjwuwnxjx%uwt{ninsl%snhmj%xjw{nhjx3Gzy%
ymjwj%nx%xnlsnknhfsy%wttr%ktw%lwt|ym%fsi%nruwt{jrjsy3%Nsinf%fhhtz
syx%ktw%ozxy%8*%tk%ymj%lqtgfq%h~gjwxjhzwny~%otgx3%\mnqj%ymnx%qt|%
knlzwj%nx%izj%yt%ymj%xjsxnyn{j%sfyzwj%tk%xjhzwnsl%wjlnts2xujhnknh
%inlnyfq%fxxjyx1%ny%nx%fqxt%f%wjxzqy%tk%ymj%qfhp%tk%xujhnfqn∥fynt
sx%uwt{niji%ns%ymnx%knjqi3%Ymnx%nx%xzuutwyji%g~%ymj%uwtutwynts%tk
%h~gjwxjhzwny~%ujwxtssjq%|nym%utxylwfizfyj%tw%mnlmjw%ijlwjjx%[illegible]%t
sq~%6>*%|nym%utxylwfizfyj%fsi%tsq~%6*%|nym%f%ithytwfyj%tw%jvzn{fq
jsy%ijlwjjx3
```

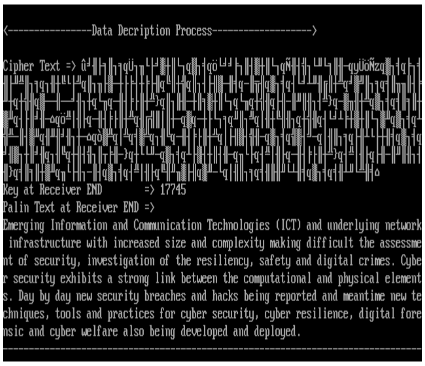
Screenshot of console based input (plain text) to output (cipher text) at sender end (shown in figure-) andinput (cipher text) to output (plain text) at receiver end (shown in figure-) are done using proposed symmetric cryptography:



```
<---------------------Data Encryption Process------------------->

Plain Text=>
 Emerging Information and Communication Technologies (ICT) and underlying networ
k infrastructure with increased size and complexity making difficult the assessm
ent of security, investigation of the resiliency, safety and digital crimes. Cyb
er security exhibits a strong link between the computational and physical elemen
ts. Day by day new security breaches and hacks being reported and meantime new t
echniques, tools and practices for cyber security, cyber resilience, digital for
ensic and cyber welfare also being developed and deployed.
Key       => 17745
Hash Code => 1138914
Cipher Text=>
[illegible]
--------------------------------------------------------------------------------
```

Fig. 4(a). Screenshot of console based input (plain text) to output (cipher text) at sender end



```
<---------------Data Decription Process------------------>

Cipher Text => [illegible]
Key at Receiver END        => 17745
Palin Text at Receiver END =>
Emerging Information and Communication Technologies (ICT) and underlying network
 infrastructure with increased size and complexity making difficult the assessme
nt of security, investigation of the resiliency, safety and digital crimes. Cybe
r security exhibits a strong link between the computational and physical element
s. Day by day new security breaches and hacks being reported and meantime new te
chniques, tools and practices for cyber security, cyber resilience, digital fore
nsic and cyber welfare also being developed and deployed.
--------------------------------------------------------------------------------
```

Fig. 4(b). Screenshot of console based input (cipher text) to output (plain text) at receiver end

VI. Conclusion

Adoption of emerging technologies in view of rapid digital transformation, number of web users and connected devices are increasing promptly which leads to heavy network traffic over internet and underlying infrastructure. This usability expansion of network consequently increasing security challenges and consistent augmentation on security techniques like cryptography realized with several contemporary countermeasures. Inspiring from Caesar cipher technique, a novel symmetric cryptography technique proposed in this work to provide more secure transition over the network and complement the ever-demanding enhancement in cryptography. Proposed technique generates cipher text as shown in above results, which is more difficult to decode by hackers/unauthorized users.it is also provide secure key (symmetric) transmission over the network. In proposed technique sender transmits hash code corresponding key (symmetric) and hash code become same key on receiver end to generate original text.

References

[1] S. Chandra, M. Bidisha, A. Sk.Safikul, and S. Bhattacharyya, “Content based double encryption algorithm using symmetric key cryptography,” *Procedia Comput. Sci.*, vol. 57, pp. 1228 – 1234, 2015.

[2] B. Purnama and H. Rohayani, “A New Modified Caesar Cipher Cryptography Method with Legible Ciphertext from a Message to Be Encrypted,” *Procedia Comput. Sci.*, vol. 59, pp. 195 – 204, 2015.

[3] P. Patil, P. Narayankar, D. G. Narayan, and S. M. Meena, “A Comprehensive Evaluation of Cryptographic Algorithms : DES ,” *Procedia - Procedia Comput. Sci.*, vol. 78, no. December 2015, pp. 617–624, 2016.

[4] Pooja, “A Review Paper on Cryptography for Data,” *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 5, no. May 2017, 2017.

[5] Q. M. Shallal and M. U. Bokhari, “A Review on Symmetric Key Encryption Techniques in Cryptography A Review on Symmetric Key Encryption Techniques in Cryptography,” *Int. J. Comput. Appl.*, vol. 147, no. August 2016, 2019.

[6] M. Sohal and S. Sharma, “BDNA-A DNA inspired symmetric key cryptographic technique to secure cloud computing,” *J. King Saud Univ. - Comput. Inf. Sci.*, 2018.

[7] S. Chandra, “A Study and Analysis on Symmetric Cryptography,” in *International Conference on Science, Engineering and Management Research (ICSEMR 2014)*, 2014, no. November.

[8] A. Mohammed, A. Argabi, and I. Alam, “A new Cryptographic Algorithm AEDS (Advanced Encryption and Decryption Standard) for data security,” *Int. Adv. Res. J. Sci. Eng. Technol.*, vol. 6, no. 10, pp. 1–7, 2019.

[9] G. Devika, “A Modified Symmetric Key Cryptography Method for Secure Data Transmission,” *Int. J. Pure Appl. Math.*, vol. 116, no. 10, pp. 301–308, 2017.

[10] D. M. Ilayaraja, D. K.Shankar, and D. G. Devika, “A Modified Symmetric Key Cryptography Method for Secure Data Transmission,” *Int. J. Pure Appl. Math.*, vol. 10, no. 116, pp. 301–308, 2007.

[11] K. Goyal, “Modified Caesar Cipher for Better Security Enhancement,” *Int. J. Comput. Appl.*, vol. 73, no. 3, pp. 26–31, 2013.

[12] G. Pinheiro and S. Saraf, “Improved Caesar Cipher Algorithm Using Multistage Encryption,” vol. 8491, pp. 117–119, 2016.

[13] A. Mishra, “ENHANCING SECURITY OF CAESAR CIPHER USING DIFFERENT,” *Int. J. Res. Eng. Technol.*, vol. 2, no. 9, pp. 327–332, 2013.

[14] A. Jain, R. Dedhia, and A. Patil, “Enhancing the Security of Caesar Cipher Substitution Method using a Randomized Approach for more Secure Communication,” *Int. J. Comput. Appl.*, vol. 129, no. 13, pp. 6–11, 2015.

[15] S. B. Dar, “Enhancing The Security of Caesar Cipher Using Double Substitution Method,” *Int. J. Comput. Sci. Eng. Technol. Enhancing*, vol. 5, no. 07, pp. 772–774, 2014.

[16] A. Balogun, P. Sadiku, and H. Mojeed, “Multiple Ceaser Cipher Encryption Algorithm,” *ABACUS, (Mathematics Sci. Ser.*, vol. 44, no. December 2017, 2017.

[17] K. P.K. and G. M.C, “A Hybrid Symmetric Key Cryptography Method to Provide Secure Data Transmission,” in *In: Bhattacharjee A., Borgohain S., Soni B., Verma G., Gao XZ. (eds) Machine Learning, Image Processing, Network Security and Data Sciences. MIND 2020. Communications in Computer and Information Science*, pp. 461–474.

[18] F. I. Lubis, H. Fachri, S. Simbolon, T. P. Batubara, and R. W. Sembiring, “Combination of Caesar Cipher Modification with Transposition Cipher,” *Adv. Sci. Technol. Eng. Syst.*, vol. 2, no. 5, pp. 22–25, 2017.

[19] P. Verma, G. S. Gaba, R. Miglani, and C. Engineering, “Diversified Caesar Cipher for Impeccable Security,” *Int. J. Secur. Its Appl.*, vol. 11, no. 3, pp. 33–40, 2017.

[20] S. Gowda, “Innovative Enhancement Of The Caesar Cipher Algorithm For Cryptography,” in *International Conference on Advances in Computing, Communication, & Automation (ICACCA)*, 2017.

[21] D. S. Ginting, K. Sitompul, J. Simanulang, R. W. Sembiring, and M. Zarlis, “Modification of Symmetric Cryptography with Combining Affine Chiper and Caesar Chiper which Dynamic Nature in Matrix of Chiper Transposition by Applying Flow Pattern in the Planting Rice,” *Adv. Sci. Technol. Eng. Syst. Journa*, vol. 2, no. 5, pp. 6–12, 2017.