# Secure Message Transmission using Dynamic Key Generation

*BASIC TECHNOLOGIES*

In this section different concepts are discussed that are used in the proposed model.

- **Cryptography**- Cryptography is the practice and study of techniques for secure communication in the presence of third parties [3].
- **Encryption-** Encryption is the coding or scrambling of information so that it can only be decoded and read by
  someone who has the correct decoding key.
- **Decryption**-The process of converting encrypted data(cipher) back into its original form (plain text),so that it can be understood. Encryption and decryption should not be confused with encoding and decoding, in which data is converted from one form to another but is not deliberately altered so as to conceal its content.[4]
- **Symmetric key cryptography**-Unlike, asymmetric key cryptography that uses different keys, the algorithm uses the same key for both encryption of plaintext and decryption of ciphertext [5].

## IV. ALGORITHM

The proposed algorithm uses the concept of symmetric key cryptography and sends the message through a communication channel to the receiver that decrypts cipher text to get the original data.

### *A. Working Diagram*

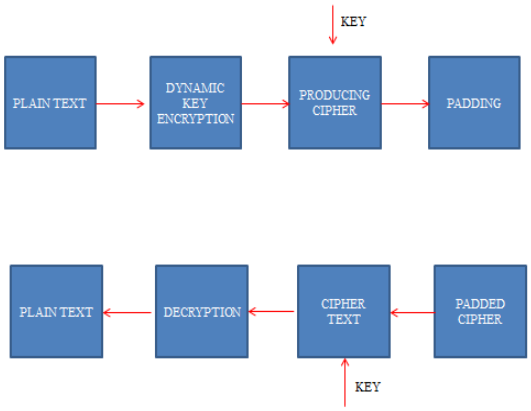


Fig. 2: Model of the cryptography algorithm

### *B. Steps for encryption*

Step 1- Convert plain text into 16 bytes ASCII 4 by 4 matrix.

Step 2-The chief feature of the cryptographic algorithm is **Dynamic Key Generation** which is as follows-

a) A= (Message Length-number of vowels)
   B = (Message Length-number of consonents)
   C = (Message Length-number of digits+ number of spaces)
   D = (Message Length-number of special characters)

b) Generate the 4 byte key matrix –
   Key[0] = A XOR B
   Key[1] = B XOR C
   Key[2] = C XOR D
   Key[3] = D XOR A

Step 3- Perform Circular left shift of second and third rows of the plain text i.e moving each bit to the left.

| | | | |
|---|---|---|---|
| 4 | 2 | 7 | 3 |
| 7 | 5 | 9 | 1 |
| 6 | 2 | 0 | 5 |
| 1 | 0 | 8 | 9 |

Step 4- The obtained shifted matrix is transposed .

| | | | |
|---|---|---|---|
| 4 | 7 | 6 | 1 |
| 2 | 5 | 2 | 0 |
| 7 | 9 | 0 | 8 |
| 3 | 1 | 5 | 9 |

Step 5- Key Encryption – Add the encrypted 4 byte dynamic key to the matrix obtained in step 4.

Step 6- Perform Mono alphabetic substitution i.e for every value that is greater than 26 do – Value=value%26 and then convert to the corresponding character in English alphabets.

Quotient=value/26

Step 7- Now perform padding –

Cipher Text + Key + Quotient.

*C. Steps for decryption*

Step 1- First we will extract the cipher text and the encrypted key from the padded form received from the sender.

Step 2- With the help of quotient, we will generate the original values of the matrix in this way –

Example: if the value received is 10 in the message and the quotient is 2, then 2*26+10=62, So 62 will be the new value in the matrix.

Step 3- Perform Decryption of the symmetric key with the 16 byte matrix obtained in previous step. Step 4: Perform Transpose of the matrix and Circular right shift of the matrix.

Step 5- Convert the resulting ASCII values to the corresponding character in the matrix.

## V. RESULTS AND ANALYSIS

Below are the results obtained after the implementation of the model for 16 bytes data by using 4 bytes key.

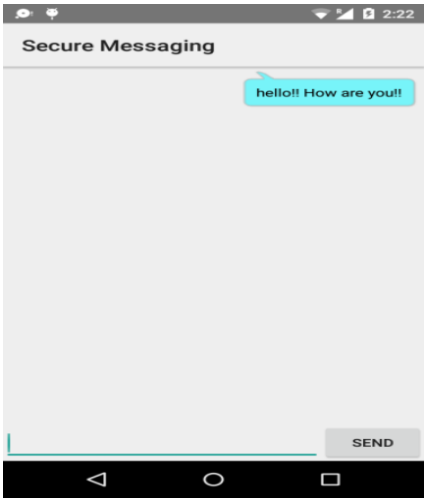


Fig. 3: Sending message through a secure channel

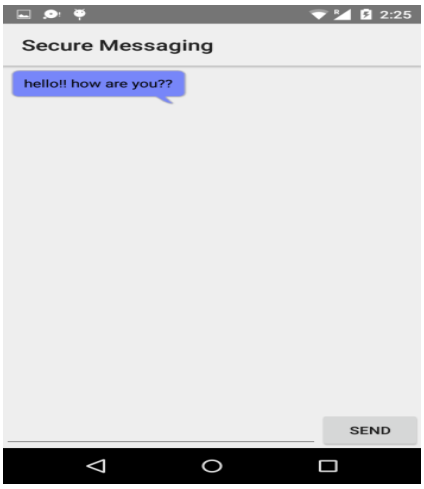


Fig. 4: The receiver decrypts the message and reads the plain text.

TABLE I.

| **Task performed** | **Time taken in milliseconds** |
|---|---|
| Dynamic Key Generation | 0.244479 |
| Circular left shift | 0.1562 |
| Encryption with the key | 0.1198 |
| Decryption | 0.2055 |

Table 1: Time taken in encryption and decryption

## CONCLUSION

Hackers are always curious to look for weaker points so that they can steal the confidential data to directly cripple the user privacy. Keeping all these security problems in mind, the purpose of the model is to provide a secure traffic between the participating users interacting over the internet and also a cost effective technique in terms of execution time for encryption and decryption processes.

It is clear from the analysis that the proposed methodology is technically feasible as it implements stringent policies to make network system simple, fast and secure.

## REFERENCES


[1.] Huang, pu and li, Mengxiang, "analyzing mobile instant messaging user satisfaction and loyalty an integrated perspective", City University of Hong Kong.

[2.] Subir Jhanb, Google Cloud Messaging team, "Powerful new messaging features with GCM" [online], 25th August 2014
Available: http://androiddevelopers.blogspot.in/2014/08/powerful-new-messaging-features-with-gcm.html.

[3.] "Cryptography" ", [online],
Available:
https://en.wikipedia.org/wiki/Cryptography

[4.] Miss Rashmi Shinde, Prof. Sanjay Pawar, "Compartition of different cryptographic algorithms for security of mobile portable devices", International Journal of Engineering Research & Technology, 2012.

[5.] "Data encryption/decryption IC definition", [online],
Available:
http://searchsecurity.techtarget.com/definition/data-encryption-decryption-IC



Ms. **S**arvesh Tanwar
Asst. Professor, CSE Dept.
CET, MUST
s.tanwar1521@gmail.com

Ms. Vinod Maan
Asst. Professor, CSE Dept.
CET, MUST
Vinodmaan.cet@modyuniversity.ac.in