



**IJIRCCCE**

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 4, April 2024

**ISSN** INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA

**Impact Factor: 8.379**



9940 572 462



6381 907 438



ijircce@gmail.com



www.ijircce.com

# Hybrid Encryption Using Cyclic Bit Shift and RC4

Mrs. Nagaraj Meghasree, B. Sai Meghana, G. H. Deepika, D. Bharathi, K. Hemanth Kumar

Assistant Professor, Dept. of CSE., JNTUA University, Kuppam Engineering College, Andhra Pradesh, India

B. Tech Students, Dept. of CSE., JNTUA University, Kuppam Engineering College, Andhra Pradesh, India

**ABSTRACT:** Encryption and decryption are critical security measures that are designed to ensure that communication is received and processed correctly. In computer networks, digital information such as text, audio and video have been broadly exchanging over the communication system. Encryption is the process by which a readable message is converted to an unreadable form to prevent unauthorized parties from reading it. Decryption is the process of converting an encrypted message back to its original (readable) format. The original message is called the plaintext message. The encrypted message is called the cipher text message. The security of the communication system in the present day imperative conception because the information ingredient of the human life. There are many Techniques to encrypt and decrypt the information; in this work we proposed combination of two techniques into a hybrid technique to get stronger encryption. The proposed permutation technique is cyclic bit shift, while the proposed stream technique is RC4. The results of the combination of two methods are then performed performancetests using the avalanche effect (AE), bit error ratio (BER), the time required for decryption encryption and character error rate (CER). The Hybrid Encryption Technique using Cyclic Bit Shift and RC4 comes under the category of Symmetric key algorithms. Based on the results of testing the proposed method is superior compared to the method that has been previously proposed.

**KEYWORDS** Data security, Decryption, Encryption, Cyclic bit shift, RC4, StreamCipher, Permutation Technique

## I. INTRODUCTION

Data security becomes an important aspect along with more data is sent via the internet. Many types of data such as text, images, videos, or files in certain formats can be hacked and utilized by irresponsible parties. Especially, if the data will be sent is sensitive, confidential and valuable data. To maintain data security during data transmission cryptographic techniques are needed. The cryptography technique is an encoding technique to keep data secret so it cannot be read directly.

The data to be encoded is called a plaintext, where the plaintext is converted to ciphertext using a specific key then be sent to the recipient. After reaching the recipient, the ciphertext will be restored to the plaintext using the key so that it can be read. Cryptography is classified into three types based on the key, they are symmetric keys, asymmetric keys, and hash functions. Symmetric keys only use one key for the encryption and decryption process. While asymmetric keys use different keys when encryption and decryption process, for example, RSA. For hash function does not use a key and directly convert text to random characters, for example, is SHA 256. The symmetric key is divided into block ciphers and stream ciphers. The examples of block ciphers are many from classical cryptography such as substitution techniques, permutation techniques, and some modern cryptography.

RC4 is one of the most popular stream cipher algorithms today. The techniques on symmetric keys have the advantage which is the time needed for encryption and decryption is fast due to a relatively simpler algorithm. Because of the simple algorithm, symmetric-key cryptography has weaknesses. RC4 algorithm has weaknesses in the S-Box table, where this table allows us to do key repetition to full fill 256 bytes so that it will produce the same table. So the message can be easily guessed if several characters in the input are known. Keys on RC4 can be easily identified from the output of the keystream and can be exploited using WEP and WPA. Therefore a hybrid method is proposed by combining the block cipher using the cyclic bit shift algorithm and the stream cipher, RC4 algorithm. Both algorithms are symmetric keys so they only need one key for the encryption and decryption process. The cyclic bit shift will rotate the position of the bit in a single byte length. The RC4 algorithm will change the ciphertext resulting from the cyclic bit shift to the final ciphertext. In the RC4 algorithm process, the ciphertext results from the cyclic bit shift cipher will be encrypted using XOR using the keystream. Key streams are generated from the KSA (Key Scheduling Algorithm) and PRGA (Pseudo Random Generation Algorithm) processes. The initial process in the proposed method is that each character in the plaintext will be converted into an ASCII number. Then the ASCII numbers on each plaintext character

are converted to binary. Plaintext that has been converted into binary then will be encrypted using the cyclic bit shift algorithm.

The first ciphertext then encrypted again using XOR function with keystream in the RC4 algorithm. The keystream is obtained from the permutation process in key with the initial vector with a range of 1-256. This process is called Key Scheduling Algorithm (KSA). Then the results from KSA are processed using Pseudorandom Generation Algorithm (PGRA). To test the method performance, parameters such as Avalanche Effect (AE), Bit Rate Error (BER) and time required in the encryption/decryption process are needed. In addition, the AE value of the proposed method is compared with other techniques in previous studies. The CER value is to determine whether the algorithm can be decrypted completely or not

## **II. RELATED WORK**

Research specifically focusing on hybrid encryption schemes that combine cyclic bit shift (CBS) and RC4 encryption techniques may be limited, as these methods are not commonly used together due to their respective vulnerabilities and weaknesses. However, it's possible to find related work in the broader context of hybrid encryption, symmetric encryption algorithms (including RC4), and data obfuscation techniques (such as cyclic bit shift).

Here are some directions where you might find related work:

1. **Hybrid Encryption Research:**
  - Look for studies and papers that explore the design, analysis, and implementation of hybrid encryption schemes. While they may not specifically mention CBS and RC4 together, they can provide insights into the general principles and best practices of combining symmetric and asymmetric encryption techniques.
2. **Symmetric Encryption Algorithms:**
  - Research focusing on symmetric encryption algorithms, including RC4, may discuss their strengths, weaknesses, and usage scenarios. While RC4 has vulnerabilities that limit its security in many contexts, research on its optimization or combination with other techniques could be relevant.
3. **Data Obfuscation Techniques:**
  - Studies investigating various data obfuscation techniques, such as cyclic bit shift, might offer insights into how such methods can be integrated into encryption schemes to enhance security. While CBS is not commonly used in encryption independently, its principles could inspire novel approaches when combined with encryption algorithms like RC4.
4. **Security and Cryptanalysis:**
  - Explore research that discusses the security analysis and cryptanalysis of encryption algorithms and techniques. Understanding the vulnerabilities and attack vectors associated with CBS, RC4, and hybrid encryption can inform the design of more robust encryption schemes.
5. **Practical Implementations:**
  - Look for practical implementations or case studies where hybrid encryption or variants of it have been deployed in real-world scenarios. These implementations may not explicitly mention CBS and RC4, but they could provide valuable insights into the challenges and considerations involved in building secure encryption systems.

Keywords like "hybrid encryption," "cyclic bit shift," "RC4," and "symmetric encryption" can help narrow down your search and identify relevant literature. Additionally, reviewing conference proceedings, journals, and research papers in the field of cryptography and information security can provide valuable insights into current trends and advancements.

## **III. PROPOSED ALGORITHM**

In this work we proposed combination of two techniques into a hybrid technique to get stronger encryption. The proposed permutation technique is cyclic bit shift, while the proposed stream technique is RC4. The results of the combination of two methods are then performed performance tests using the avalanche effect (AE) and character error rate (CER). The Hybrid Encryption Technique using Cyclic Bit Shift and RC4 comes under the category of Symmetric key algorithms. Based on the results of testing the proposed method is superior compared to the method that has been previously proposed.

### **Advantages**

→ More secure. → Stream ciphers are simple to use and implement. → RC4 has an advantage on entropy value and should not require a very long key. → RC4 stream ciphers do not require more memory. Encryption is the process of converting normal message (plaintext) into meaningless message (Ciphertext). Whereas

Decryption is the process of converting meaningless message (Ciphertext) into its original form (Plaintext). The major distinction between secret writing associated secret writing is that the conversion of a message into an unintelligible kind that's undecipherable unless decrypted, whereas secret writing is that the recovery of the first message from the encrypted information.

Shared Key and Public Key Encryption:

SKIP uses a combination of shared key cryptography and public key cryptography to protect messages sent between hosts. SKIP hosts use shared traffic keys that change frequently to encrypt data sent from one host to another. To protect these shared traffic keys, SKIP hosts use the public key to calculate an implicit shared secret, which they use to encrypt the shared traffic keys, keeping network communication secure.

#### IV. METHODOLOGY & ALGORITHMS

RC4 bit encryption algorithm:

RC4 means Rivest Cipher 4 invented by Ron Rivest in 1987 for RSA Security. It is a Stream Ciphers. Stream Ciphers operate on a stream of data byte by byte. RC4 stream cipher is one of the most widely used stream ciphers because of its simplicity and speed of operation. It is a variable key-size stream cipher with byte-oriented operations. It uses either 64 bit or 128-bit key sizes. It is generally used in applications such as Secure Socket Layer (SSL), Transport Layer Security (TLS), and also used in IEEE 802.11 wireless LAN std. Unauthorized data access can be prevented by encryption. If we perform encryption then third parties can not have access to data which we share or receive. The encryption is done by using a secret key, or we can say that by using a public key and private key. Both sender and receiver are having their public key and private key through which encryption of plain text and decryption of ciphertext is performed. RC4 is used in various applications such as WEP from 1997 and WPA from 2003. We also find applications of RC4 in SSL from 1995 and it is a successor of TLS from 1999. RC4 is used in varied applications because of its simplicity, speed, and simplified implementation in both software and hardware. The algorithm operates on a user-selected variable-length key(K) of 1 to 256 bytes (8 to 2048 bits), typically between 5 and 16 bytes. To generate a 256-byte state vector S, the master key used. The first step is the array initialization. It is a character array of size 256 i.e. S[256]. After that, for every element of the array, we initialize S[i] to i.

Advantages: → RC4 stream ciphers are simple to use. → The speed of operation in RC4 is fast as compared to other ciphers. → RC4 stream ciphers are strong in coding and easy to implement. → RC4 stream ciphers do not require more memory. → RC4 stream ciphers are implemented on large streams of data.

#### V. CYCLIC BIT SHIFT ALGORITHM

The new mechanism of cyclic shift delay means to delay the space-time streams with different time reference. This technique can prevent from unintentional beam forming when the same signal is sent through different space-time streams. In [IEEE P802.11n], the cyclic shift duration is defined in Table n61 for the non-HT portion of packet, including L-STF, LLTF, L-SIG and HT-SIG, and in Table n62 for the HT portion of packet, including HT-STF, HT-LTF and HT data. The cyclic shift can be viewed as an optimization of the MIMO communication channel and this processing is transparent to the receiver. It is worthy to notice that in case of non-HT portion, the cyclic shift is applied directly to each transmit chain while in case of HT portion the cyclic shift is applied to each space-time stream. This implies the cyclic shift processing should be taken in frequency domain for the HT portion, in general with the spatial mapping processing. An exception is when the spatial mapping is in mode direct mapping that the cyclic shift can be done in the time domain.



Fig. Architecture diagram of proposed method

Encryption Procedure → The user inputs a plain text and a secret key. → The plain text is converted to ASCII code and bit shift procedure is performed → The resultant is then encrypted using RC4 Algorithm → The encrypted text is displayed to the user.

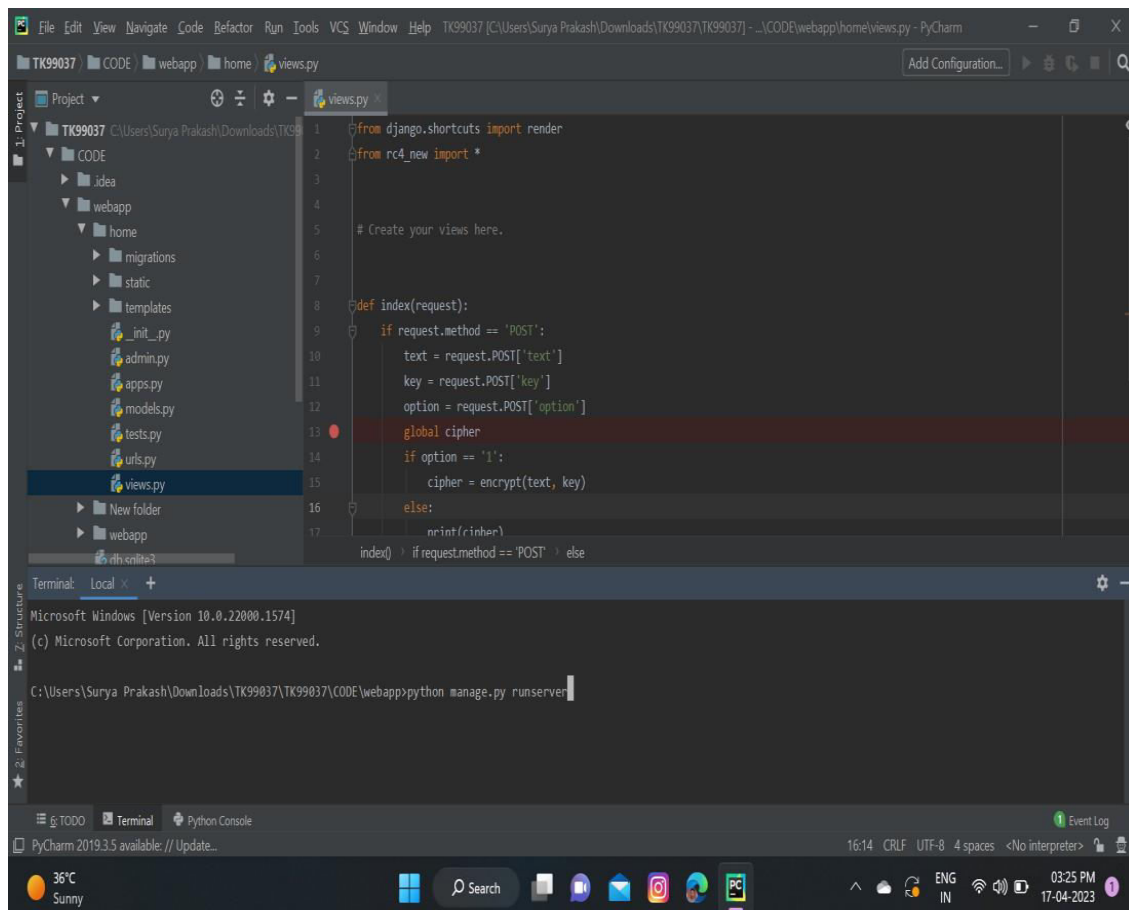
Decryption Procedure → The user inputs a cipher text and the secret key. → The cipher text is converted to binary code and RC4 procedure is performed. → The resultant is then decrypted using Bit Shift Algorithm and then converted from ASCII code to characters. → The decrypted text is displayed to the user.

## VI. SIMULATION RESULTS

### Step 1:- Execution

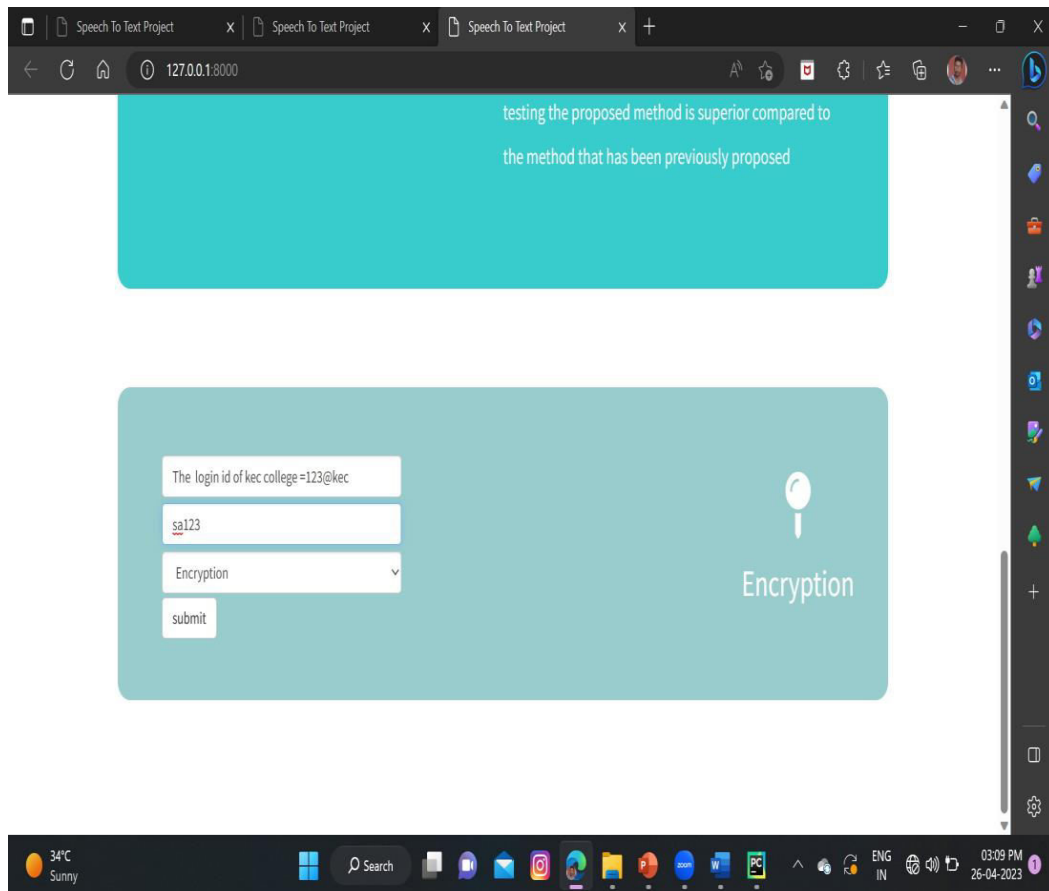
To run the code:

>>>Python manage.py runserver

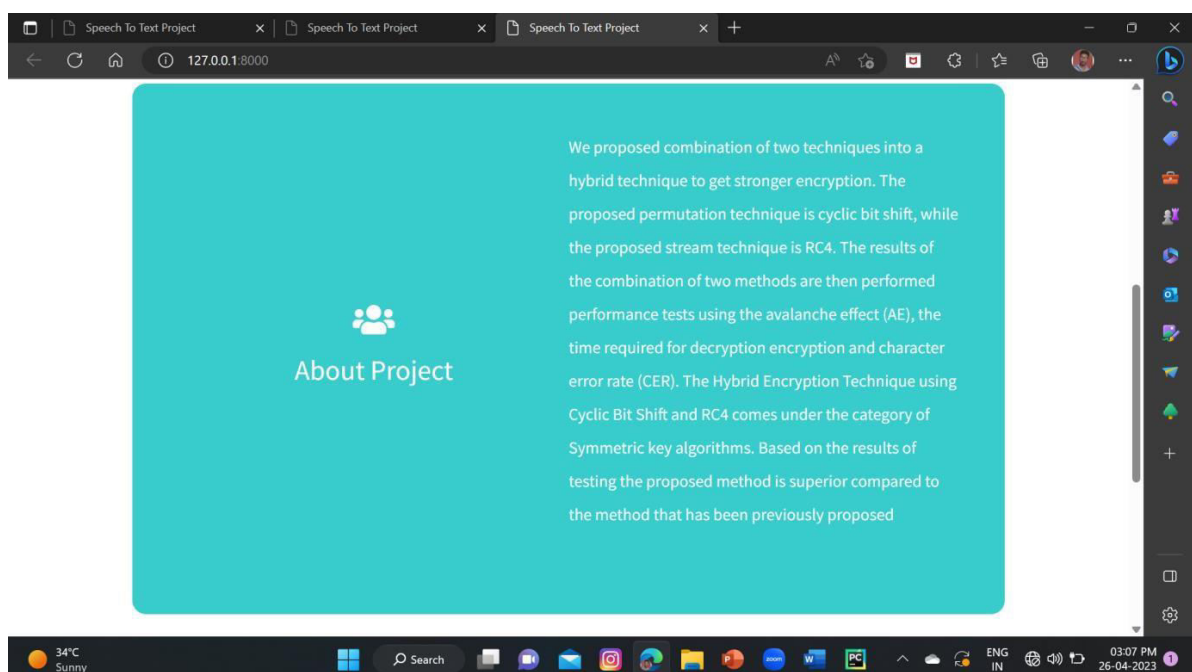


The screenshot shows the PyCharm IDE interface. The main editor displays the contents of the `views.py` file, which includes imports for `render` and `rc4_new`, and a function `index` that handles POST requests by encrypting text using the RC4 algorithm. The terminal window at the bottom shows the command `C:\Users\Surya.Prakash\Downloads\TK99037\TK99037\CODE\webapp>python manage.py runserver` being executed. The system tray at the bottom indicates a temperature of 36°C and the date 17-04-2023.

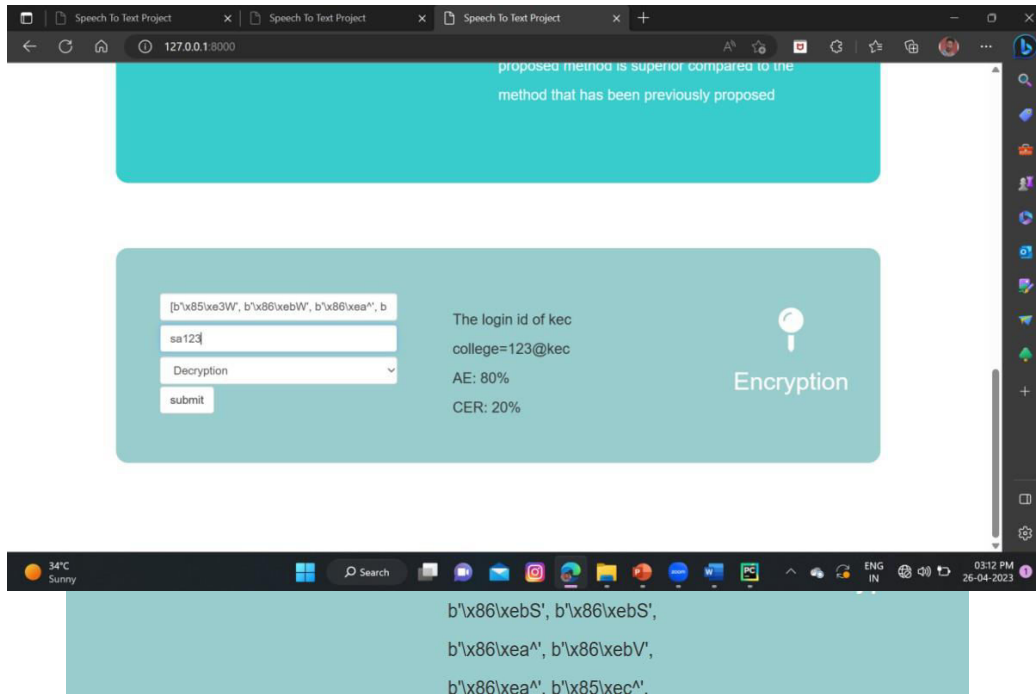
Step 2:- Home page



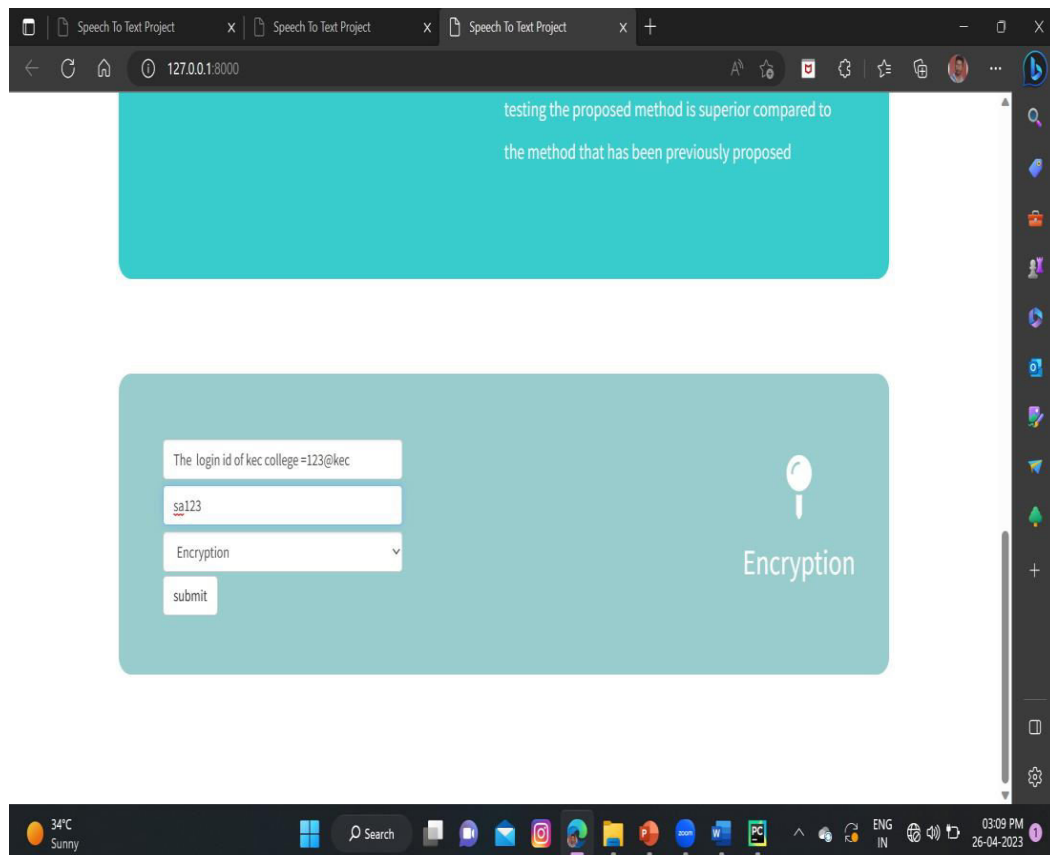
Step 3:- About project



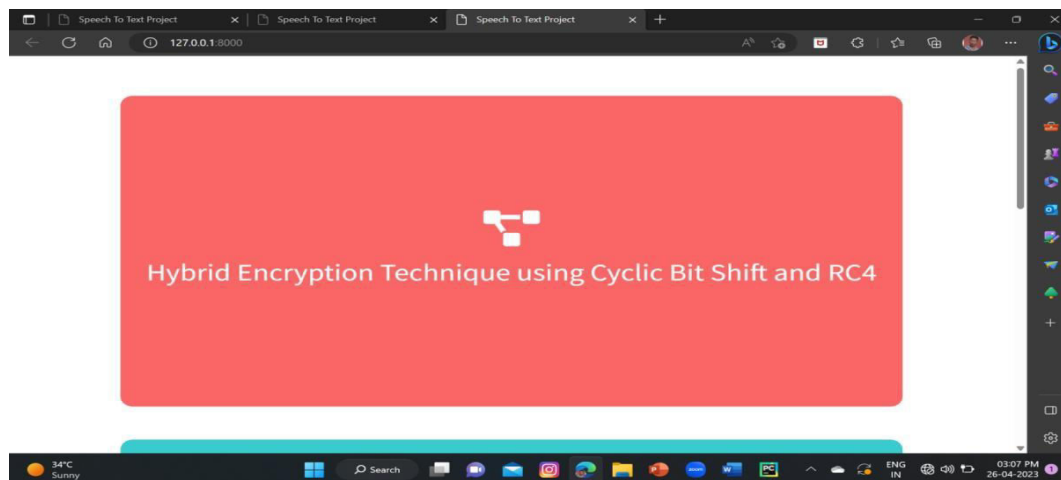
### Step 4:- Encryption



### Step 5:- After Encryption



## Step 6:- Decryption



## VII. CONCLUSION AND FUTURE WORK

This project concludes that the encrypt the input text by using RC4 encryption algorithm. Here user can give the text to server then that data is converted into cipher text by the process of encryption and user can give cipher text data to server again the server can convert that data into text with the help of decryption process. So, this project helps out the users to convert the text to chipper text and chipper text to text.

In Future, we can try different combination of different algorithms to increase the security of stream cipher. We can add Images, photos ,Videos and etc.

## REFERENCES

- [1] [1]. M. N. M. Najih, D. R. I. M. Setiadi, E. H. Rachmawanto, C. A. Sari, and S. Astuti, "An improved secure image hiding technique using PN-sequence based on DCTOTP," in 2017 1st International Conference on Informatics and Computational Sciences (ICICoS), 2017, pp. 47–52.
- [2] D. R. I. M. Setiadi, H. A. Santoso, E. H. Rachmawanto, and C. A. Sari, "An improved message capacity and security using divide and modulus function in spatial domain steganography," in 2018 International Conference on Information and Communications Technology (ICOIACT), 2018, pp. 186–190.
- [3] Y. Meena, R. Kumar Verma, M. Singh Sankhla, and R. Kumar, "Secure Cyber Network to Sharing Information through Cryptography & Stenography," Eng Technol Open Acc, vol. 2, no. 5, pp. 1–5, 2019.
- [4] E. J. Kusuma, O. R. Indriani, C. A. Sari, E. H. Rachmawanto, and D. R. I. M. Setiadi, "An imperceptible LSB image hiding on edge region using des encryption," in Proceedings - 2017 International Conference on Innovative and Creative Information Technology: Computational Intelligence and IoT, ICITech 2017, 207AD..
- [5] J. J. Amador and R. W. Green, "Symmetric-key block cipher for image and text cryptography," Int. J. Imaging Syst. Technol., vol. 15, no. 3, pp. 178–188, Jan. 2005.
- [6] M. Chase, "Multi-authority attribute based encryption," in Proc. Theory Cryptography. Conf. Berlin, Germany: Springer, Feb. 2007, pp. 515–534.





INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

 9940 572 462  6381 907 438  [ijircce@gmail.com](mailto:ijircce@gmail.com)



[www.ijircce.com](http://www.ijircce.com)

Scan to save the contact details