Scientific Voyage
Vol. 3, No. 2,
Page 30-33 (2022)

SCIENTIFIC VOYAGE
ISSN: 2395-5546

GCECT
Publication
Apr - Jun

Making of a cryptographic mechanism to enhance security in message transmission

Sayantan Chakrabarti[1*] and Rahul Binani[2]

Department of Information Technology, B P Poddar Institute of Management and Technology, Kolkata 700052, West Bengal, India

Abstract: Cryptography is a familiar technique to safely send a message or data where privacy and secrecy needs to be maintained from the source to the destination. This transferring of confidential information has been considered under a threat now-a-days due to the intermediate attackers. The idea of making this machine started off with a hybrid security approach consisting of different algorithms, viz., Substitution and RSA, including some secret bit adding. Further transferring the encoded message over a network. When a certain encoded message is sent, each of its character gets shifted by a certain position, and then it is converted into bytes. RSA is applied over these bytes for several timesand finally some extra bits are added to these to end up with the encrypted text. Then this encrypted text is transferred over the network. At the receivers' end the same process chronologically opposite manner is applied to find the actual plaintext.

Keywords: Encryption; Decryption; RSA; Substitution; Bit padding

1 Introduction

A mechanism which deals with privacy of the message or information from attackers, i.e., keeps the message safe and secure by changing its actual form is known as Cryptography. This is generally segmented into two types: named as Symmetric Key Cryptography and Asymmetric Key Cryptography. Symmetric key cryptography has classical cryptographic mechanism such as Transposition Cipher and Substitution Cipher. On the other hand, Asymmetric cryptography has modern approaches like Stream Cipher and Block Cipher. However, we would be focusingupon both the kind of cryptographic techniques and will be building an asymmetric cryptographic machine. When a single key is introduced by both the sender of the data and the receiver of the data to encrypt and decrypt the data respectively is called Symmetric Key cryptography. However, if there are different multiple keys for this approach with the sender and the receiver, it is named as Asymmetric Key Cryptography. The keys that are required amongst the sender and receiver are shared through secretmeans.

This project aims at securing the confidentiality on the exchange of information between the sender and receiver using a mixture of existing algorithms making it much stronger. Many algorithms in the society have already been cracked by the unethical attackers, and now it's high time to introduce something new approach which successfully helps in maintaining privacy and confidentiality of data among the users.

2 LiteratureReview

Paper [1] states that Cryptography has a vital role in data security purpose. It ensures that the contents of a message are securely transmitted and would not be changed. Network security plays most vital role in information security as it is attached withall hardware and software function, characteristics, workings processes.

Paper [2] gives an idea that Nowadays security is very much needed to protect our sensitive data in computer or over the internet medium such as in online banking, online shopping, stock market and bill payments etc by proposing a new cryptographic algorithm AEDS (Advanced Encryption and Decryption Standard) which is designed by adding features of DES and AES algorithms and compared all the algorithms and it is discussed that AEDS is more robust for securing ofdata.

*Corresponding Author

[1]Email: 92sayantan@gmail.com
[2]Email: binanirahul1808@gmail.com

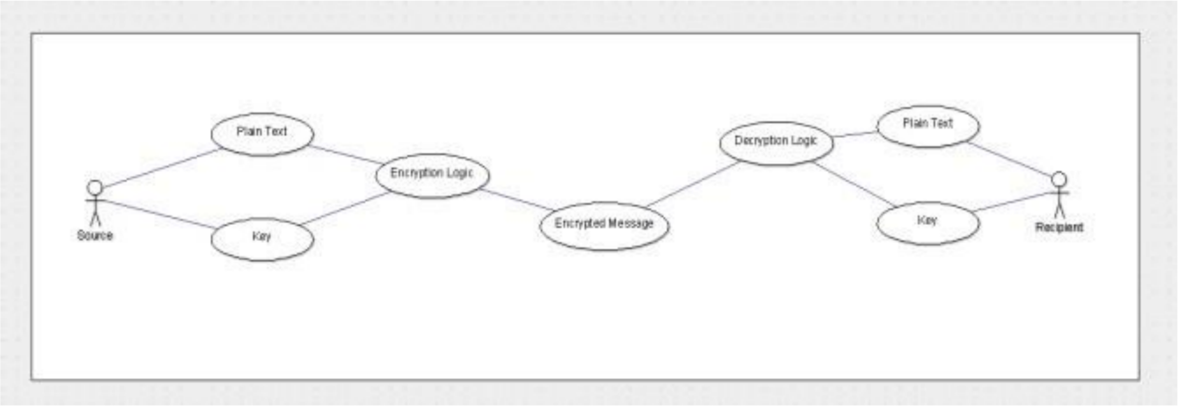


Fig. 1: Secure message passing mechanism

Paper [2] gives an idea that Nowadays security is very much needed to protect our sensitive data in computer or over the internet medium such as in online banking, online shopping, stock market and bill payments etc by proposing a new cryptographic algorithm AEDS (Advanced Encryption and Decryption Standard) which is designed by adding features of DES and AES algorithms and compared all the algorithms and it is discussed that AEDS is more robust for securing of data.

Paper [3] tells that The algorithm required for enhancing security should fulfil the requirements of authentication, confidentiality, integrity and non-repudiation. In this paper, the brief introduction of AES, DES, RSA, Diffie-Hellman, RC4, Blow Fish, El-Gamal, MD5 and Miller-Rabin gives an idea of different security approaches.

Paper [4] describes about the availability of multiple data security methods at market. They may vary by speed, strength and resource consumption that is use of CPU, Power, Storage device. Among them popular and interesting algorithms are described.

Paper [5] discussed a new cryptographic algorithmic method to secure the data for inducing Data Security that can be used to secure the various applications on cloud computing.

Paper [6] signifies the necessity of data security in modern days. It also signifies the utility of different data security algorithm like AES, DES and give some idea about data compression.

Paper [7] focuses on various types of cryptography algorithms that are already exists like AES, DES, TDES, DSA, RSA, ECC, EEE and CR4...etc. It also focuses on the different challenges in securedata transmission over different medium.

3 Proposedworks

Enhancement of security in data communication is the ultimate motive ofthis project. Here we have introduced a hybrid algorithm which has its base upon the RSA (Rivest, Shamir, Adleman) Algorithm, substitution and bit padding. Before moving to the task, some points about the individual algorithms. Starting off with the most important part of this algorithm, i.e., RSA Algorithm. Having its base set upon asymmetric cryptography the keys are generated using very large prime numbers. After the key formation, encryption starts. The formula for encryption reads $c = m$^e* (mod n) where c is cipher text. The decryption formula reads c^$d = m$ * (mod n). The encryption and decryption can be done by anyone but what plays an important role in security is the formation of keys using unbreakable primenumbers.

Secondly, the substitution algorithm is a cryptographic technique where the plain text is replaced with other characters following a set of sequence and shifting rules. Here we have used monoalphabetic substitution.

Lastly, we have implemented bit padding i.e., adding random bits to the end of the cipher text. These bits are added for the purpose of fooling the man in the middle who gets an incorrect idea about the exact length of the message. Moreover, if the attacker decrypts the whole message, it would not get the exact message.

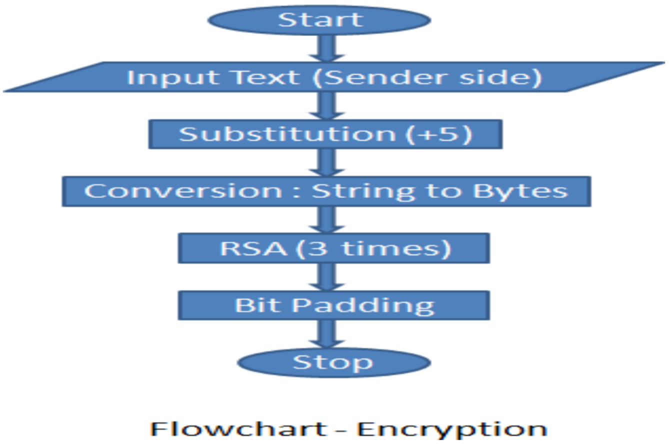


Fig. 2: Encryption Mechanism

At the beginning, 2 keys are generated, i.e., public and private at the server side and receiver side each.

When the sender generates a message and sends it to its receiver, firstly the message is substituted by its 5 successive characters. Then the resultant string is converted into bytes and this set of bytes undergoes RSA encryption for 3 times i.e., the output of each RSA acts as the input of the next. Finally, the output of the third RSA is added up with some random bits as a concept of bit padding. Ultimately this whole sequence is transferred over thenetwork.

As it is in the more secure form, the attacker even if attacks won't succeed easily in decrypting this cipher text into plain text. As this message reaches the receiver side the decryption process starts. The message leaving aside the padded bits is extracted. Reverse RSA is applied (decryption of RSA) for 3 times and finally this is shifted with 5 predecessor characters. Ultimately the plain text reaches the receiver.

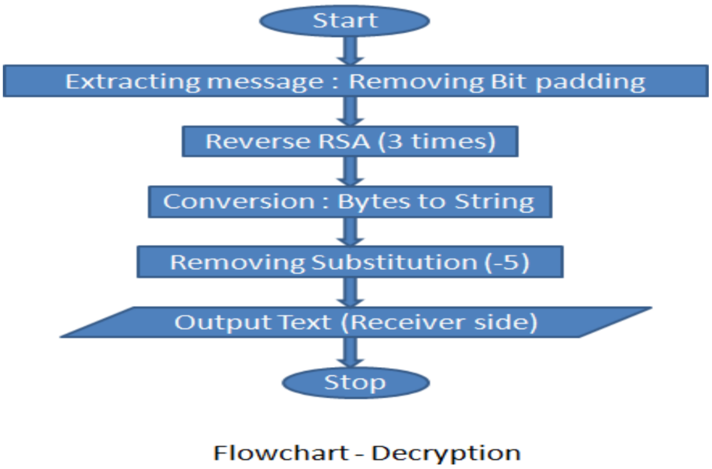
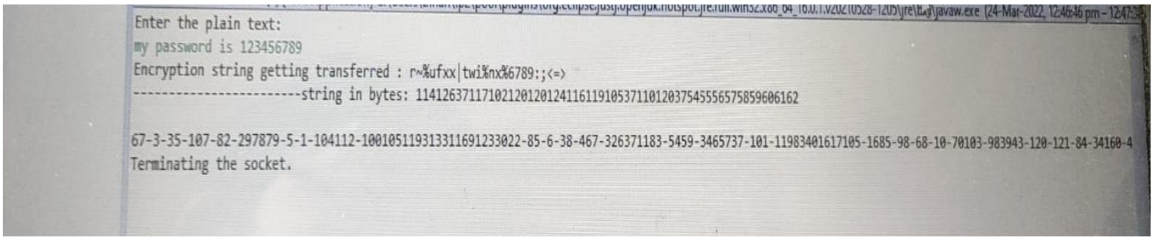

Start
Extracting message : Removing Bit padding
Reverse RSA (3 times)
Conversion : Bytes to String
Removing Substitution (-5)
Output Text (Receiver side)
Stop
Flowchart - Decryption

Fig. 3: Decryption Mechanism

4 Results

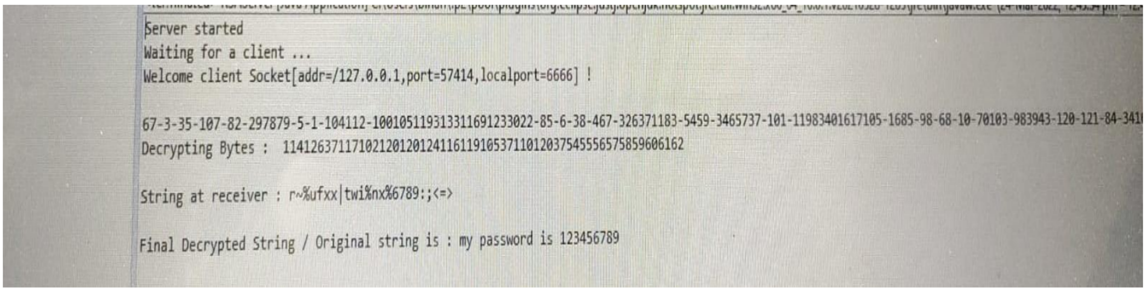
The plaintext generated by the sender when converted into cipher text is of the type Big Integer. This Big Integer variable is transferred over the network to the receiver side. Upon decryption it returns back the plain text. As we see the cipher text is long enough but is transferred easily over the network to the receiver. It also ensures security which is our main concern; however, time taken is also minimal.



```
Enter the plain text:
my password is 123456789
Encryption string getting transferred : r~%ufxx|twi%nx%6789:;<=>
------------------------string in bytes: 114126371171021201201241161191053711012037545556575859606162

67-3-35-107-82-297879-5-1-104112-1001051193133116912330 22-85-6-38-467-326371183-5459-3465737-101-11983401617105-1685-98-68-10-70103-983943-120-121-84-34160-4
Terminating the socket.
```

Sender side



```
Server started
Waiting for a client ...
Welcome client Socket[addr=/127.0.0.1,port=57414,localport=6666] !

67-3-35-107-82-297879-5-1-104112-100105119313311691233022-85-6-38-467-326371183-5459-3465737-101-11983401617105-1685-98-68-10-70103-983943-120-121-84-341
Decrypting Bytes :  114126371171021201201241161191053711012037545556575859606162

String at receiver : r~%ufxx|twi%nx%6789:;<=>

Final Decrypted String / Original string is : my password is 123456789
```

Receiver side

5 Conclusion

A build in technique which ensures safety, security and privacy of information through mathematical concepts and codes is generally referred to cryptography. With the help of different concepts, we have successfully formed a hybrid algorithm of asymmetric cryptography. We have reduced the chances of attacks over the messages flowing over a network. In today's world of new technology when we from all sides are surrounded by OTPs and Passwords, we sometime or the other find the need to exchange the same over the communication network itself with someone. A fear arises at this time that what if someone steals our confidential password or OTP over the transmission network. This feeling worsens if the credentials are of some Bank Account details. To release such stress this algorithm would play a vital role. Common people would be more assured about the security of their message.

References

[1] K. Acharya, M. Sajwan and S. Bhargava, *Int. J. Comp. Appl. Tech. Res.* **3** (2014) 130.

[2] A. Mohammed, A. Argabi and Md. I. Alam, *Int. Adv. Res. J. Sci., Engg. Tech.* **6** (2019) 1.

[3] M. Malhotra and A. Singh, *Int. J. Sci. Engg. Res.* **1** (2013) 77.

[4] Y. Alemami, M.A. Mohamed and S. Atiewi, *Int. J. Rec. Tech. Engg.* **8** (2019) 395.

[5] A. Tushar, A. Sharma and A. Mishra, *Int. J. Engg. Res. Tech.* **10** (2012) 274.

[6] S. Kumari, *Int. J. Engg. Comp. Sci.* **6** (2017) 20915.

[7] O.G. Abood and S.K. Guirguis, *Int. J. Sci. Res. Pub.* **8** (2018) 495.