iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** VII **Month of publication:** July 2021

DOI: https://doi.org/10.22214/ijraset.2021.36441

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VII July 2021- Available at www.ijraset.com

Implementation & Comparative Analysis of RSA, Caesar Cipher and Playfair Cipher

Pushkar Aneja[1], Maanya Manocha[2]
[1, 2]*Department of Computer Science and Engineering, Manav Rachna International Institute of Research and Studies, Faridabad, Haryana, India*

Abstract: ***With the growing use of the Internet, and more people being connected with it, the security of the data becomes a major concern. It is necessary that the data can only be accessed by the intended receiver and no person in the middle makes alterations to it. This is achieved by encryption of the data using cryptography.***
This paper presents a comparative analysis of RSA (Rivest-Shamir-Adleman), Caesar Cipher and Playfair Cipher cryptographic techniques. This paper also presents a comparative analysis of Symmetric Key Cryptography and Asymmetric Key Cryptography. Also, this paper includes the basic working of the above-mentioned techniques along with their implementation in C language over Visual Studio Code 1.49.3.
Keywords: Cryptography, encryption, decryption, symmetric key cryptography, asymmetric cryptography, RSA (Rivest-Shamir-Adleman), Caesar Cipher, Playfair Cipher.

I. INTRODUCTION

Cryptography is basically the art of encrypting data in order to enhance security. This is done by converting the data into codes using a key, which can then be decrypted at the receiving end using the same key or a different key, depending upon the algorithm used. A very vital part of secure communication is to maintain the integrity and privacy of data which can be achieved by cryptography.
Cryptography is primarily performed by applying algorithms on the given data for its secure transmission and storage. Cryptographic algorithms are basically techniques which are derived from mathematical concepts and contain a set of calculations to be performed on the data, and convert it into a code, so that it becomes difficult to understand for anyone in case there is a security breach. The receiver on the other end can decode the data using the algorithm used to encode the data, and thus use and modify the data as per need.

A. Basic Terms used in Cryptography

1) *Plain Text:* The original data or text is known as plain text.
2) *Cipher Text:* The data or text obtained after applying a cryptographic algorithm on the plain text. Cipher text is meaningless and unreadable.
3) *Encryption:* The process of converting Plaintext to Cipher Text is known as encryption.
4) *Decryption:* The process of converting Ciphertext to Plain Text is known as decryption.
5) *Cryptanalysis:* It is the study of techniques or methods to get the meaning of the encrypted data or text.
6) *Key:* A key is a combination of numeric or alpha-numeric characters. It takes place on the plain text in the process of encryption and on the cipher text in case of decryption.
7) *Key-Size:* It is the measure of length of the key used in any algorithm. It is measured in bits.
8) *Round:* Round of encryption means how much time the encryption function is executed in the whole process of encryption till it gives cipher text as output.

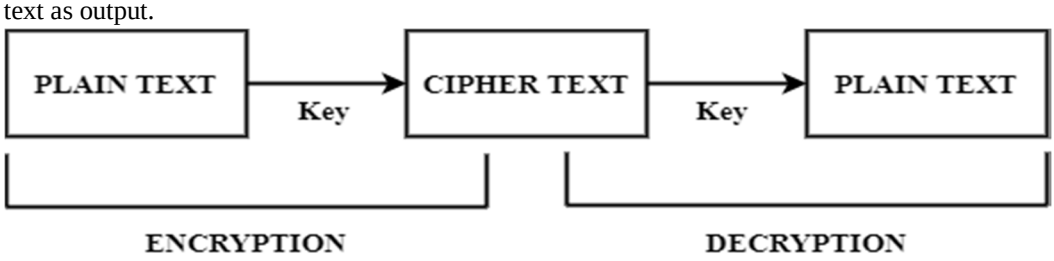


Figure 1: Basic flowchart of cryptography

B. Main objectives of Cryptography

The main goals of cryptography are:

1) *Authentication:* As per this property, both the sender and the receiver can confirm each other's identity, origin and destination of the data.
2) *Confidentiality:* This means that the main information can only be understood and altered by only the people who are authorized/intended to use the data.
3) *Integrity:* This means that the information should not be altered or changed while transferring or while in storage. The receiver must receive the exact data sent by the creator/sender.
4) *Non-repudiation:* According to this the original creator/sender of the data cannot deny his or her intention in the creation or transfer of data, at a later stage.

II. TYPES OF CRYPTOGRAPHIC ALGORITHMS

There are mainly 2 types of cryptographic algorithms:

A. Symmetric cryptographic algorithms, also known as private key cryptography, involves a single key for both encryption and decryption purposes on the sender and receiver side. This key is kept private between both of them so that no data is stolen by an attacker while the transfer or storing of data.

B. Asymmetric cryptographic algorithms, also known as public key cryptography, consists of a key pair for encryption and decryption of data. The key pair is composed of a private key and a public key. If the data is encrypted using the public key then decryption will be done with the private key and vice-versa.

Thus, asymmetric key encryption is more secure, however, symmetric key cryptography is faster in terms of encryption speed.

III. SYMMETRIC KEY CRYPTOGRAPHY Vs ASYMMETRIC KEY CRYPTOGRAPHY

Table 1: Difference between Symmetric and Asymmetric Key Cryptography

SYMMETRIC KEY CRYPTOGRAPHY	ASYMMETRIC KEY CRYPTOGRAPHY
The same key, known as the private key is used for both the encryption and decryption of the data.	In this, a key pair is involved, consisting of a private key and a public key. If one key is used for encryption then the other key will be used for the decryption.
Its encryption/decryption speed is very fast.	It is comparatively slower than symmetric key cryptography.
The size of the encrypted text is usually the same or less than that of the original text.	The size of the encrypted data is usually more than that of the original text.
The process is quite simple as only one key is used in both the operations.	The process is quite complex as separate keys are used for both the operations.
This type of cryptography is mostly done in modern computer systems to protect the privacy of the user and improve the security.	This type of cryptography is used mainly for sharing information or data between different organizations and to secure online transactions.
Some common examples of symmetric key cryptography are: 1. RC4, 2. AES, 3. DES, 3DES.	Some common examples of asymmetric key cryptography are: 1. Diffie-Hellman, 2. RSA, 3. ECC.

There are various ways developed to perform the encryption and decryption of the data. Our main focus will be RSA, Caesar Cipher and Playfair Cipher.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VII July 2021- Available at www.ijraset.com

IV. WORKING OF RSA (RIVEST-SHAMIR-ADLEMAN)

RSA is a public key cryptographic algorithm, named after the surnames of its designers, Ron Rivest, Adi Shamir and Leonard Adleman. This algorithm was described publicly by its designers in 1977. It is an asymmetric key cryptosystem which is mainly used for secure data transmission. The RSA algorithm relies widely on the practical difficulty of factoring the product of two large prime numbers, making it a quite secure algorithm. However, it is a slow algorithm and is not commonly used to directly encrypt the data.

A. *Steps of encrypting and decrypting data in RSA*

1) Select two numbers p and q, such that, p and q are not equal, and are prime numbers.
2) Calculate the value of n as:
$$n = pq$$
3) Calculate Φ(n) as
$$\Phi(n) = (p-1)(q-1)$$
4) Select an integer e, such that gcd (Φ(n), e) = 1 and 1 < e < Φ(n).
5) The value of d is calculated using the formula
$$d = e^{-1} \pmod{\Phi(n)}$$
6) Public Key is given as = { e, n }.
7) Private Key is given as = { d, n }.

B. *Encryption Process*

1) Consider the plain text, M.
2) The cipher text, C will be given as

$C = M^e \bmod n.$

C. *Decryption Process*

1) Consider the cipher text, C.
2) The plain text, M will be given as
$$M = C^d \bmod n.$$

V. WORKING OF CAESAR CIPHER

Caesar Cipher is an example of symmetric key cryptography. It is one of the most early and simple forms of encryption. It is a type of substitution cipher, in which each letter of the text is replaced by a letter which is some fixed position down the alphabet. For example – with a shift of five, A would become F, B would become G and so on. Shift is basically just an integer value that indicates the number of positions each letter has to be moved.

The process can be represented using the modular arithmetic as follows:

1) Transform the letters into numbers using the scheme, A=0, B=1, … , Y=24 and Z=25.
2) Consider the value of shift as n, the value of Cipher text as C and the value of Plain text as M then:

Encryption would be done using the formula, C = (M + n) mod 26.

Decryption would be done using the formula, M = (C – n) mod 26.

VI. WORKING OF PLAYFAIR CIPHER

Playfair Cipher is a type of symmetric key cryptography and is the first practical digraph substitution cipher. This technique encrypts a set of letters instead of a single letter (as in the case of Caesar Cipher). The Playfair cipher uses a 5 by 5 table containing the word or the phrase which needs to be encrypted.

A. *Steps*

1) A key square is to be generated, which is a 5x5 matrix, consisting of the alphabets that act as the key for encrypting the plaintext. All the 25 elements for the matrix must be unique and usually the letter J is omitted from the table (as there are only 25 cells). If the plaintext contains J it is replaced by I. The initial alphabets in the key square are the unique alphabets in the key square are the unique alphabets of the key.
2) The plain text is divided into pairs of two letters called digraphs. If the number of letters is odd, then Z is added to the last letter.

B. Encryption Process

1) If both the letters are in the same column, take the letter below each one.

2) If both the letters are present in the same row then pick the letter to the right of each one.

3) If none of the above rules is true, then form a rectangle with the two letters and consider the letters which are on the horizontal opposite corner of the rectangle.

VII. IMPLEMENTATION OF RSA (RIVEST-SHAMIR-ADLEMAN)

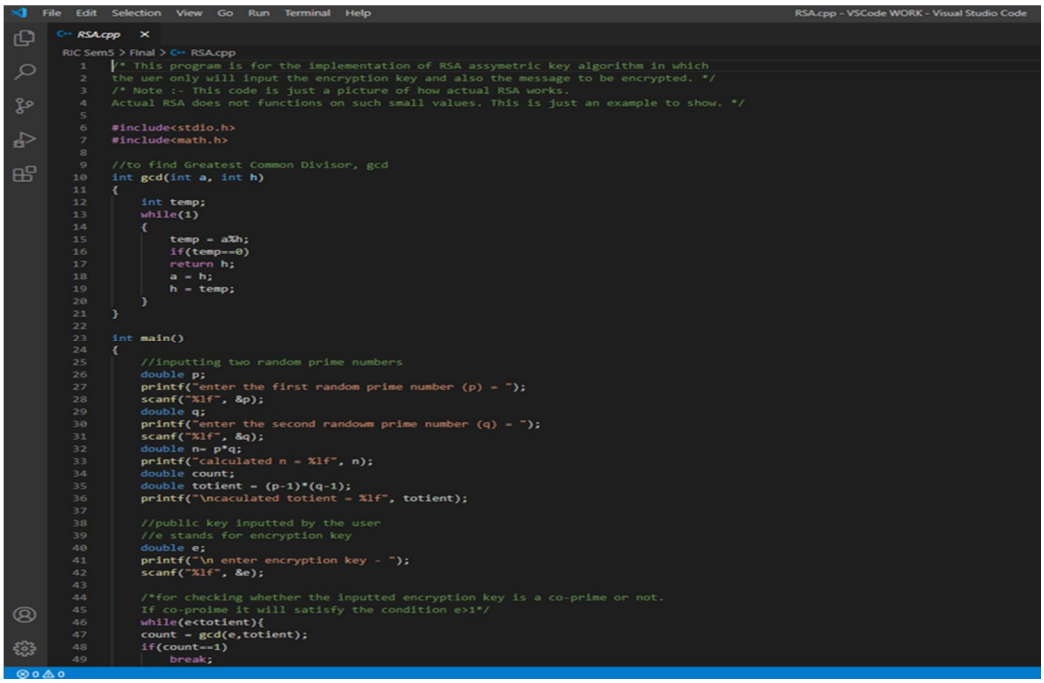


Figure 2(a)

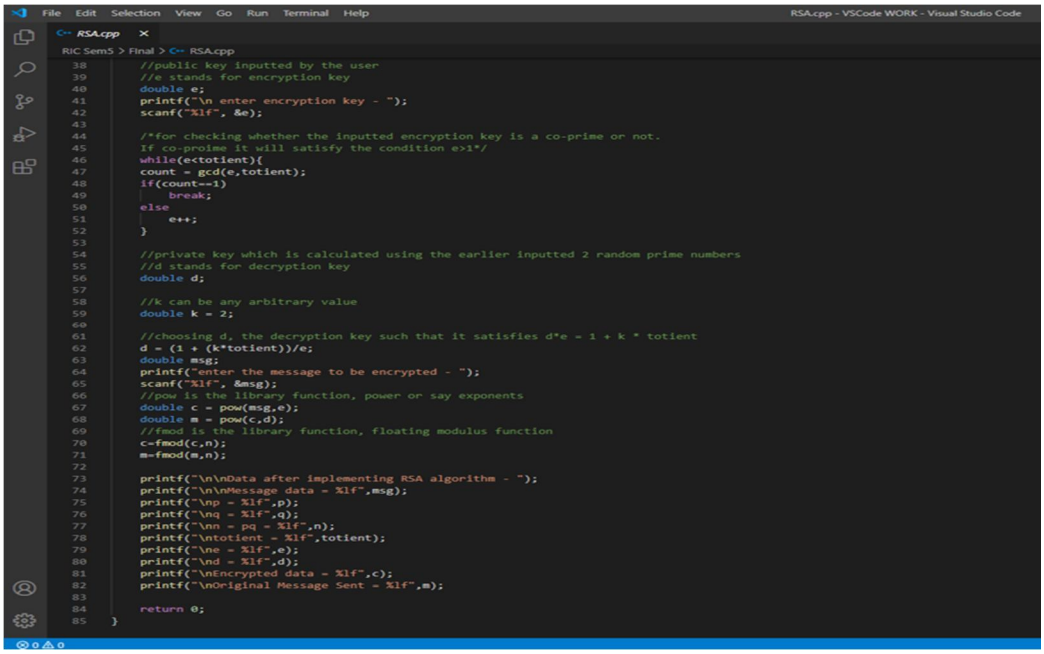


Figure 2(b)

Figure 2(a) and 2(b) Source code of RSA (Rivest-Shamir-Adleman)

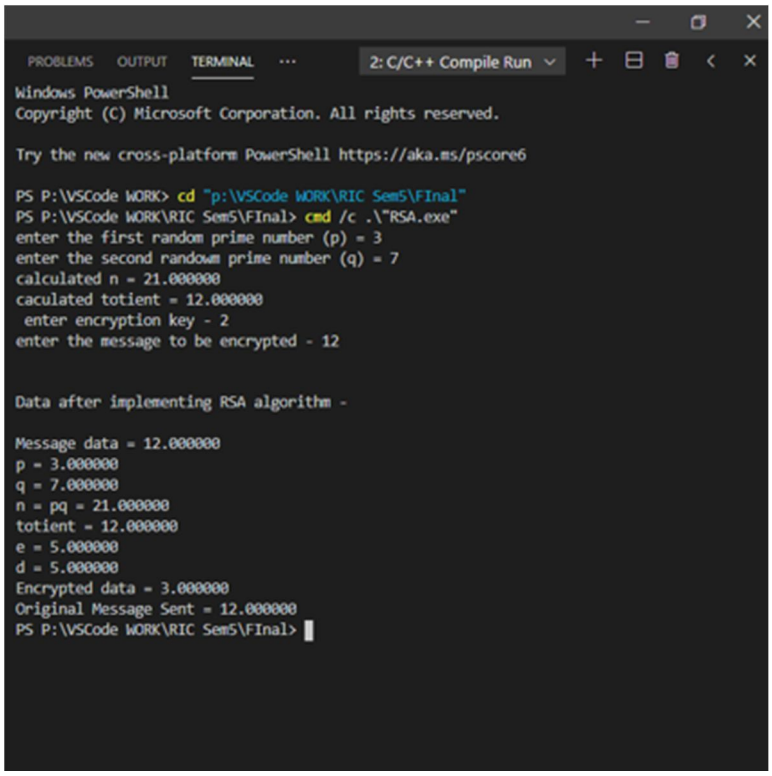


Figure 3. Output of RSA (Rivest-Shamir-Adleman)

VIII. IMPLEMENTATION OF CAESAR CIPHER

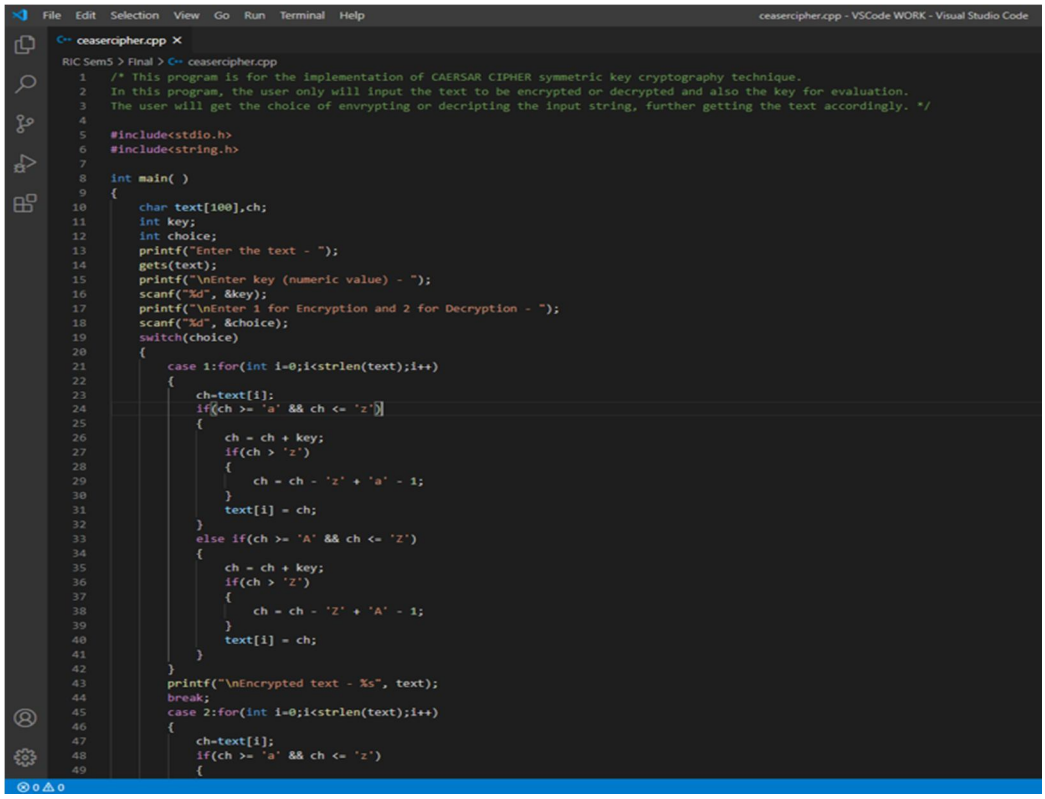
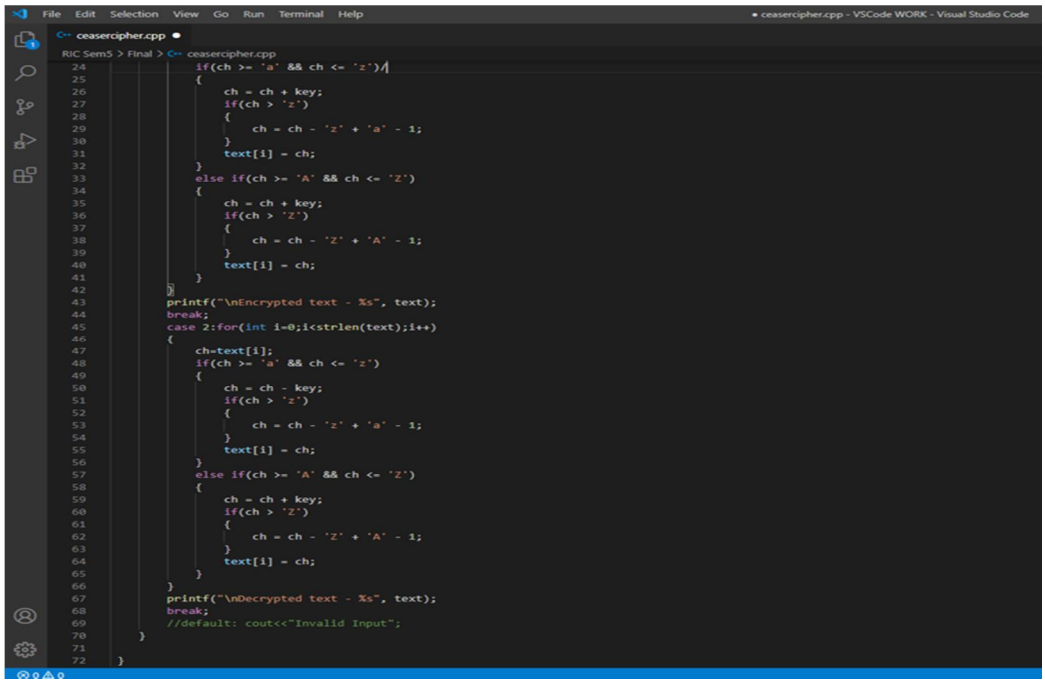


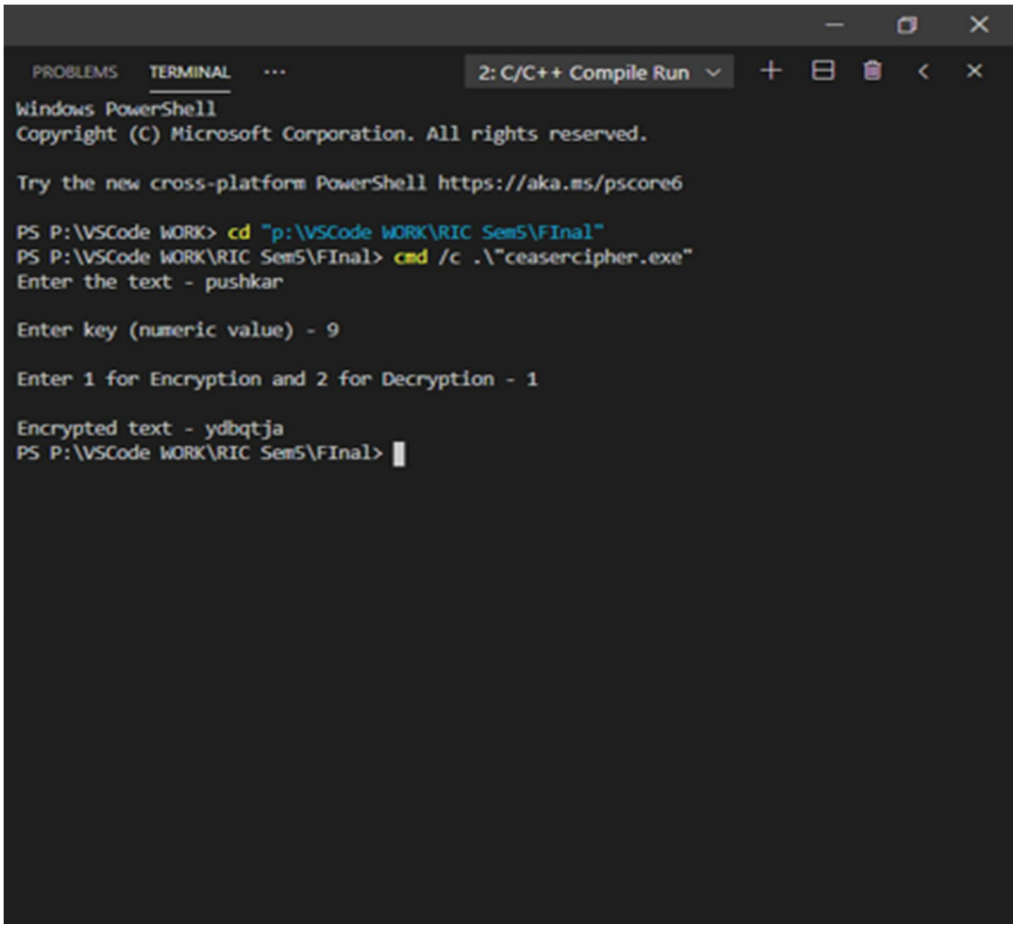
Figure 4(a)



```
            if(ch >= 'a' && ch <= 'z')
            {
                ch = ch + key;
                if(ch > 'z')
                {
                    ch = ch - 'z' + 'a' - 1;
                }
                text[i] = ch;
            }
            else if(ch >= 'A' && ch <= 'Z')
            {
                ch = ch + key;
                if(ch > 'Z')
                {
                    ch = ch - 'Z' + 'A' - 1;
                }
                text[i] = ch;
            }
        }
        printf("\nEncrypted text - %s", text);
        break;
        case 2:for(int i=0;i<strlen(text);i++)
        {
            ch=text[i];
            if(ch >= 'a' && ch <= 'z')
            {
                ch = ch - key;
                if(ch > 'z')
                {
                    ch = ch - 'z' + 'a' - 1;
                }
                text[i] = ch;
            }
            else if(ch >= 'A' && ch <= 'Z')
            {
                ch = ch + key;
                if(ch > 'Z')
                {
                    ch = ch - 'Z' + 'A' - 1;
                }
                text[i] = ch;
            }
        }
        printf("\nDecrypted text - %s", text);
        break;
        //default: cout<<"Invalid Input";
    }
}
```

Figure 4(b)

Figure 4(a) and 4(b) Source code of Caesar Cipher



```
PROBLEMS  TERMINAL  ...   2: C/C++ Compile Run

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS P:\VSCode WORK> cd "p:\VSCode WORK\RIC Sem5\FInal"
PS P:\VSCode WORK\RIC Sem5\FInal> cmd /c .\"ceasercipher.exe"
Enter the text - pushkar

Enter key (numeric value) - 9

Enter 1 for Encryption and 2 for Decryption - 1

Encrypted text - ydbqtja
PS P:\VSCode WORK\RIC Sem5\FInal>
```

Figure 5. Output of Caesar Cipher

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VII July 2021- Available at www.ijraset.com

IX. IMPLEMENTATION OF PLAYFAIR CIPHER

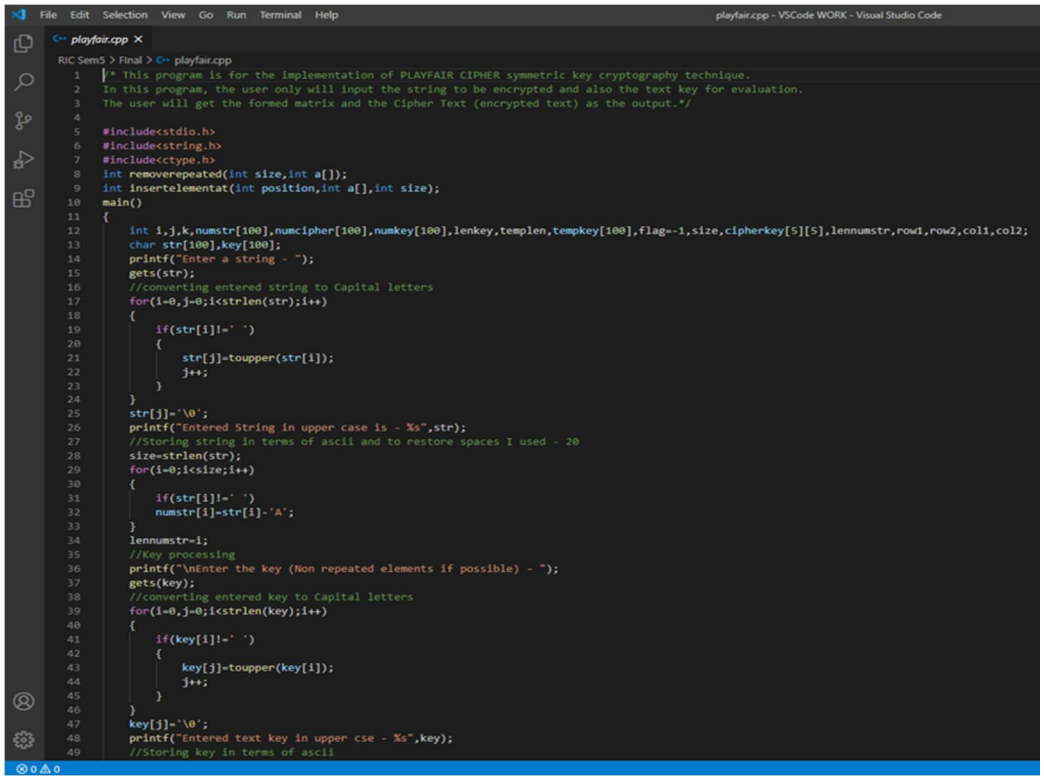


Figure 6(a)

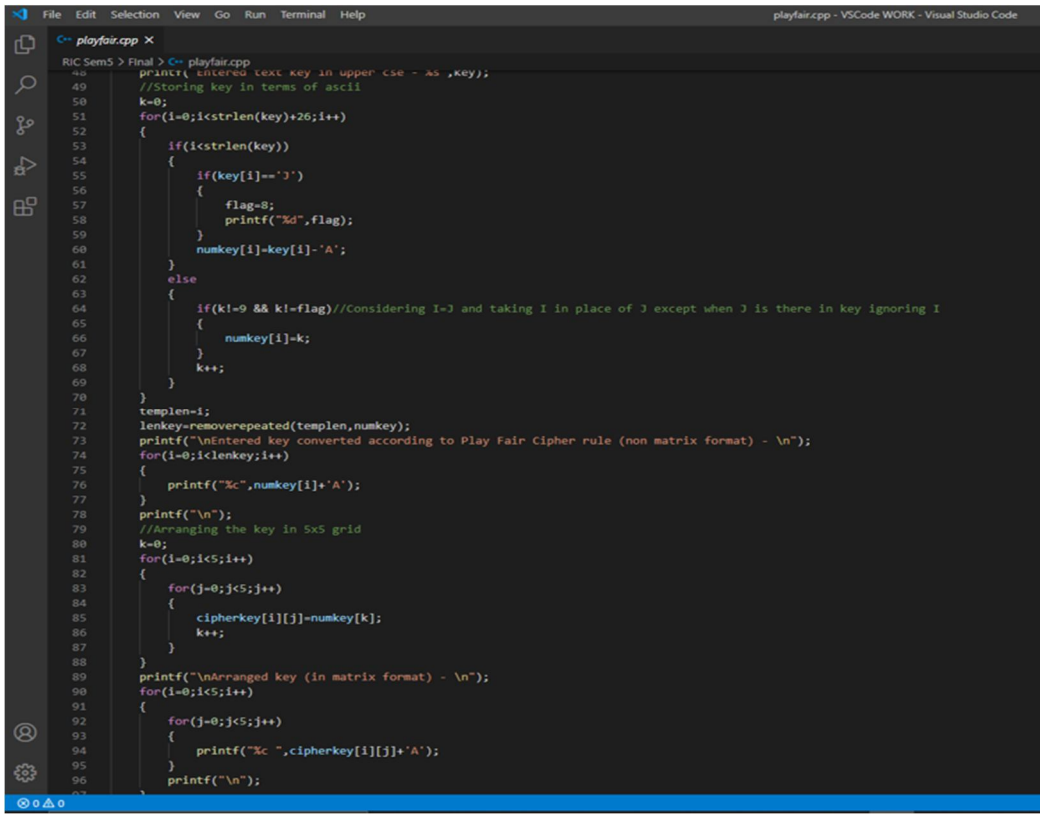


Figure 6(b)

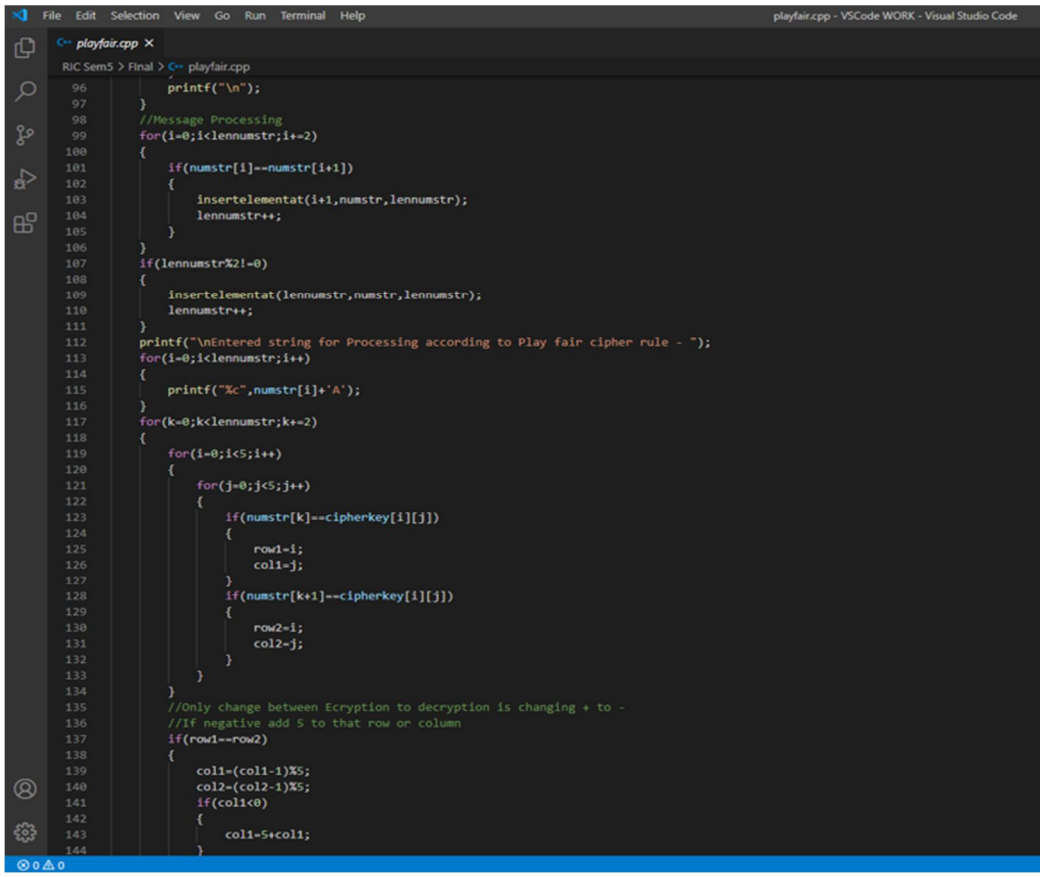


Figure 6(c)

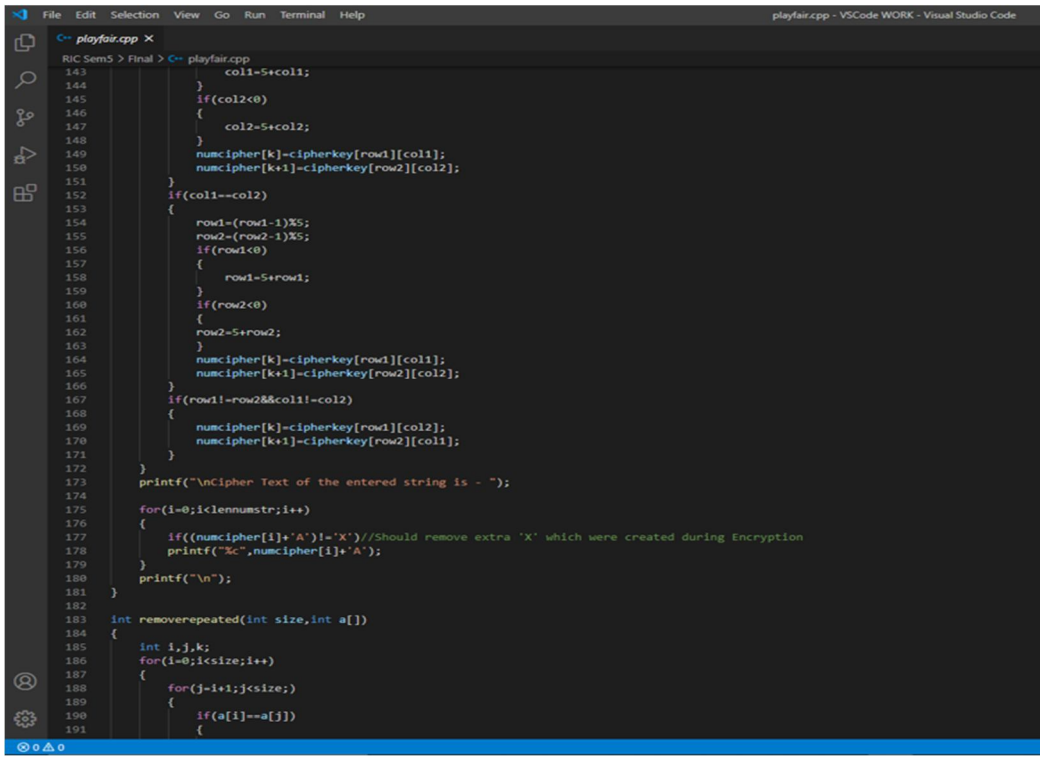


Figure 6(d)

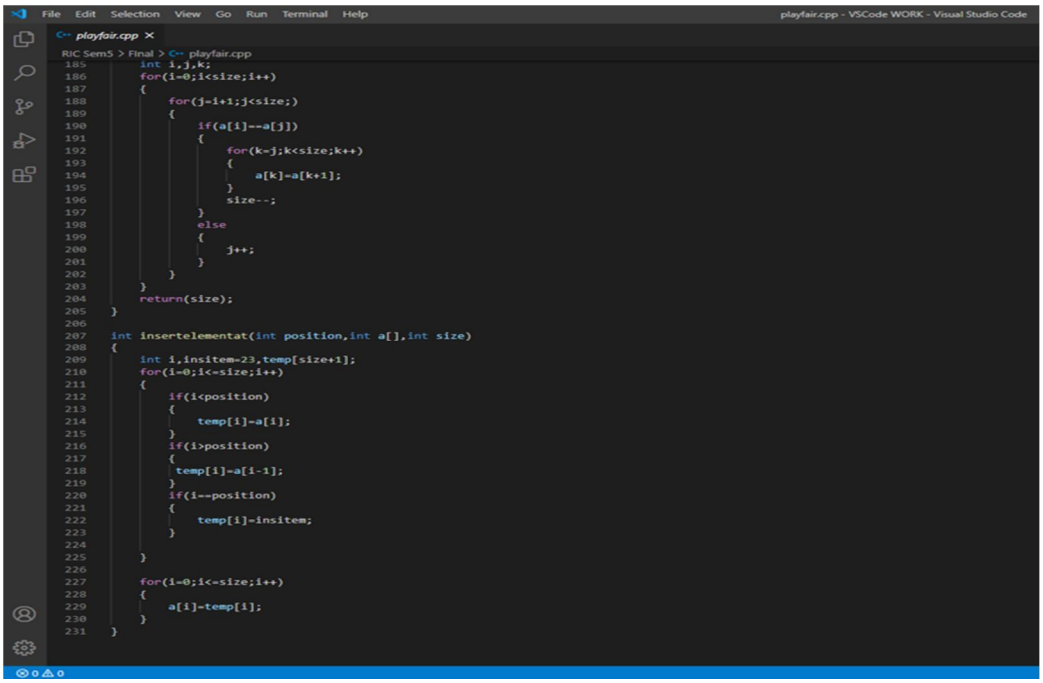


Figure 6 (e)

Figure 6(a), 6(b), 6(c), 6(d) and 6(e) - Source Code of PlayFair Cipher

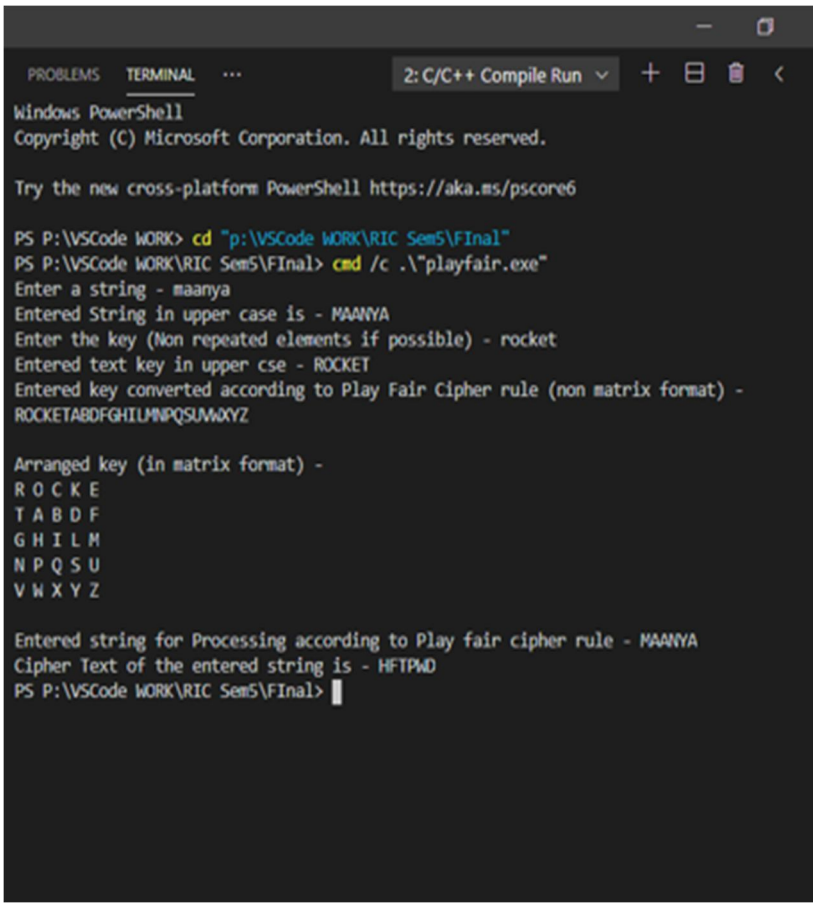


Figure 7. Output of PlayFair Cipher

A. Comparative Analysis Of RSA, Caesar Cipher, Playfair Cipher

Table 2. A comparative analysis of RSA, Caesar Cipher and Playfair Cipher

S.no	Name of algorithm	Features/Functionality	Complexity	Security/Drawbacks
1.	RSA	• RSA creates digital signatures. • RSA is also used to verify the digital signatures. • RSA performs encryption and decryption in the memory strings or in the byte arrays of any size. It is not size specific. • Performing RSA, gives a method to ensure confidentiality, integrity, authenticity and also the non-repudiation of communications held electronically and also to the data stored.	• The calculated **time complexity** of the RSA **algorithm** is $O(n^2)$. It is also observed that as the size of private key length increases, the increase in **time** becomes exponential and nonlinear. • The relation between the private key length and the run time memory is approximated as a polynomial equation of order 2 and thus, the space complexity of RSA can be expressed as $O(n^2)$.	• RSA works mainly by using the product of two prime numbers as a trapdoor function. Thus, to break an RSA cipher, it requires factoring very large numbers. • The RSA algorithm can be quite slow in cases where a large amount of data needs to be encrypted by the same device. • It also needs a third party to verify the **reliability** of public keys.
2..	Caesar Cipher	. The Caesar Cipher is a type of substitution cipher that encrypts the data by replacing the original letters with those "x" number of characters ahead in the alphabet. . The Caesar cipher is not that secure and it can be easily broken even in a ciphertext-only scenario. There are two possible: 1) an attacker knows or guesses that some sort of simple substitution cipher has been used, though he might not be aware that specifically it is a Caesar scheme; and 2) an attacker knows that a Caesar cipher is used to encrypt the data, but does not know the exact shift value. . With 26 letters in the English alphabet, the possible permutations are 26! (Factorial of 26) which equals 4x1026. The sender and the receiver may choose any one of the possible permutations as a ciphertext alphabet.	• In Caesar cipher encryption/ decryption is done by calculating the result of applying all of the n−1 (i.e., 25), the computational complexity is just O(n).	• Caesar Cipher is not a very secure cryptosystem as there are only 26 possible keys to try out and an attacker can carry out an exhaustive key search with available computing resources. • The frequency of the letter pattern often provides a big hint in decoding the complete message.

3.	Playfair Cipher	• In plaintext digraphs encryption is done with the matrix by first locating the two plaintext letters in the matrix. They are either in different rows/ columns or in the same row/ column. • The encryption is done using a 5 × 5-square matrix containing the letters of the alphabet and the letters I and J are treated as the same. • Decrypting the Playfair cipher is also quite simple as it involves doing the same process in reverse. The receiver has the same key and can thus create the same key table, and then decrypt any messages made using that particular key.	• A Playfair cipher is comparatively harder to cryptanalyze than a monoalphabetic cipher. This is because it is done on pairs of letters instead of individual letters and this Frequency Analysis is significantly difficult to crack. • In the case of the Playfair Cipher, one cannot encrypt to a double letter, so we have to remove the 26 possibilities of double letters, which gives us 650 possible digraphs that we will have to check.	• Ciphering methods should satisfy the properties of **confusion and diffusion** for them to be successful whereas the playfair cipher only provides the property of confusion. ***diffusion*** – This property is related with the driving away of statistical structure of plaintext over the bulk of ciphertext ***confusion*** – This property makes the relationship between the ciphertext and the key as complex as possible. • The Playfair cipher was used to protect important, yet non-critical secrets, because it was quick and easy to use and it required no special equipment/tool.

X. CONCLUSION

Cryptography is one of the most important things in our lives today. All the data exchanged is expected to be safe from any intervention in between the sender and the receiver, hence cryptography plays a big role in today's world. Encryption and Decryption are the two main processes to perform cryptography. Everyone wishes their data to be encrypted from their end and to only be decrypted at the authentic user's end, and nowhere in between.

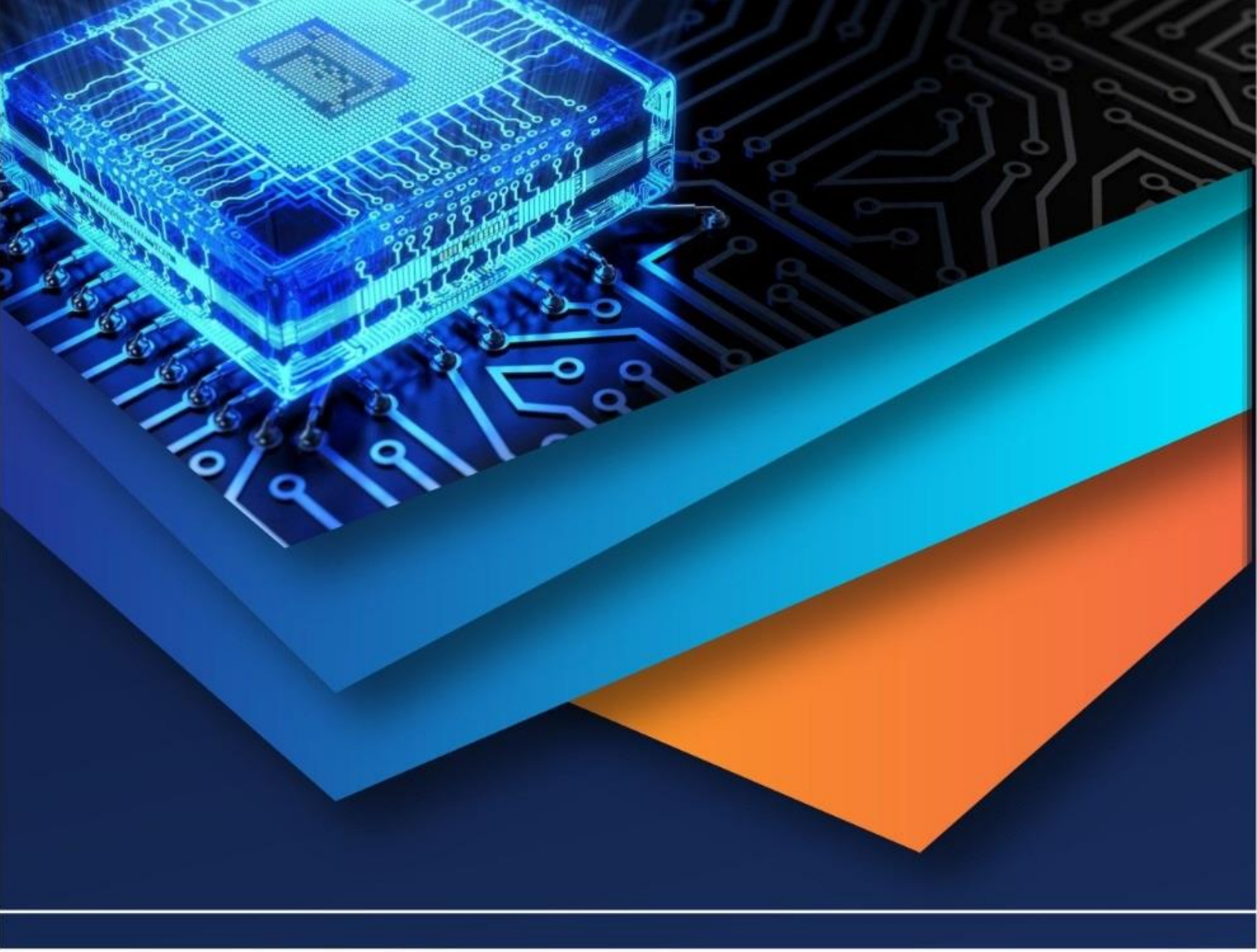
A lot of strategies/techniques/algorithms are used to perform cryptography. Three amongst them namely, RSA, Caesar Cipher and Playfair CIpher were implemented to have a comparative analysis to check their features/functionality, complexity, the level of security they provide and also the drawbacks faced with them. All these three were performed on an open source platform, Visual Studio Code version 1.49.3.

Implementing and Comparing these three techniques for cryptography, we conclude that Asymmetric Encryption (also known as Public Key Encryption) is more secure than Symmetric Encryption (also known as Private Key Encryption). Though it's more complex than the symmetric encryption technique, the approach of using two different keys, one for encryption and the other for decryption makes it more difficult for an attacker to break the encryption and get the original data out of it. Asymmetric cryptography is performed with large prime numbers giving more security to the data encrypted.

REFERENCES

[1] Dalal, N., Shah, J., Hisaria, K. and Jinwala, D., 2010. A comparative analysis of tools for verification of security protocols. Int'l J. of Communications, Network and System Sciences, 3(10), p.779.
[2] Prajapati, P., Patel, N., Macwan, R., Kachhiya, N. and Shah, P., 2014. Comparative analysis of DES, AES, RSA encryption algorithms. International Journal of Engineering and Management Research (IJEMR), 4(1), pp.132-134.
[3] Hall, J., 2013. C implementation of cryptographic algorithms. Texas Instruments.
[4] Bhardwaj, K. and Chaudhary, S., 2012. Implementation of Elliptic Curve Cryptography in'C'. International Journal on Emerging Technologies, 3(2), pp.38-51.
[5] Mahto, D. and Yadav, D.K., 2017. RSA and ECC: a comparative analysis. International journal of applied engineering research, 12(19), pp.9053-9061.
[6] Bhanot, R. and Hans, R., 2015. A review and comparative analysis of various encryption algorithms. International Journal of Security and Its Applications, 9(4), pp.289-306.
[7] Qadir, A.M. and Varol, N., 2019, June. A Review Paper on Cryptography. In 2019 7th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-6). IEEE.
[8] Forouzan, B.A., 2007. Cryptography & network security. McGraw-Hill, Inc..
[9] Menezes, A.J., Van Oorschot, P.C. and Vanstone, S.A., 2018. Handbook of applied cryptography. CRC press.
[10] Katz, J. and Lindell, Y., 2014. Introduction to modern cryptography. CRC press.

[11] Kumar, S.N., 2015. Review on network security and cryptography. International Transaction of Electrical and Computer Engineers System, 3(1), pp.1-11.
[12] Gupta, A. and Walia, N.K., 2014. Cryptography algorithms: A review.
[13] Mishra, R. and Bhanodiya, P., 2015, March. A review on steganography and cryptography. In 2015 International Conference on Advances in Computer Engineering and Applications (pp. 119-122). IEEE.
[14] Jirwan, N., Singh, A. and Vijay, D.S., 2013. Review and analysis of cryptography techniques. International Journal of Scientific & Engineering Research, 4(3), pp.1-6.
[15] Tayal, S., Gupta, N., Gupta, P., Goyal, D. and Goyal, M., 2017. A Review paper on Network Security and Cryptography. Advances in Computational Sciences and Technology, 10(5), pp.763-770.
[16] https://symbiosisonlinepublishing.com/computer-science-technology/computerscience-information-technology32.php
[17] https://symbiosisonlinepublishing.com/computer-science-technology/computerscience-information-technology32.php



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY