



Green University of Bangladesh

*Department of Computer Science and Engineering (CSE)
Semester: (Fall, Year: 2024), B.Sc. in CSE (Day)*

Comprehensive Analysis of RSA and Playfair Cipher

*Course Title: Computer and Cyber Security
Course Code: CSE-323 ; Section: 221-D10*

Student Details

Name	ID
Mahfuzur Rahman	221002014
Musfikur Rahman	221902023

Course Teacher's Name: Ayesha Banu
[For teachers use only: **Don't write anything inside this box**]

<u>KSA-Project Status</u>	
Marks:	Signature:
Comments:	Date:

Contents

Contents	1
1 Introduction to Cryptography	2
1.1 Brief of RSA	2
1.1.1 Sample Problem of RSA	2
1.2 Brief of Playfair Cipher	3
1.2.1 Sample Problem of Playfair Cipher	3
2 Implementation	4
2.1 Algorithm for RSA	4
2.2 Algorithm for Playfair Cipher	4
3 Snapshot	5
4 Comprehensive Analysis of RSA and Playfair Cipher	7
4.1 Security Comparison	7
4.2 Ease of Implementation	7
5 Conclusion	8

Chapter 1

Introduction to Cryptography

Cryptography is the practice of securing information by transforming it into a format that is unreadable without the correct decryption key. The two primary types of cryptographic systems are symmetric-key cryptography, where the same key is used for both encryption and decryption, and asymmetric-key cryptography, where different keys are used. In this report, we will explore two important cryptographic methods: RSA and Playfair cipher.

1.1 Brief of RSA

The RSA algorithm is an asymmetric-key cryptosystem that relies on the mathematical properties of large prime numbers. RSA uses a pair of keys: a public key for encryption and a private key for decryption. It is widely used in secure communications, digital signatures, and data encryption.

1.1.1 Sample Problem of RSA

Consider the following example to demonstrate RSA encryption and decryption.

Let $p = 11$ and $q = 13$. Compute the public and private keys, followed by encryption and decryption steps.

$$n = p \times q = 11 \times 13 = 143$$

$$\phi(n) = (p - 1)(q - 1) = 120$$

Choose $e = 7$ such that $\gcd(e, \phi(n)) = 1$. Then compute d such that:

$$d \times e \equiv 1 \pmod{\phi(n)}$$

The modular inverse of $e = 7$ modulo 120 is $d = 103$.

The public key is $(e, n) = (7, 143)$ and the private key is $(d, n) = (103, 143)$.

For encryption, if the plaintext message is $m = 11$, the ciphertext c is computed as:

$$c = m^e \pmod{n} = 11^7 \pmod{143} = 48$$

For decryption, the ciphertext $c = 48$ is decrypted using the private key:

$$m = c^d \pmod{n} = 48^{103} \pmod{143} = 11$$

Thus, the original message is retrieved.

1.2 Brief of Playfair Cipher

The Playfair cipher is a symmetric-key cipher that encrypts digraphs (pairs of letters) instead of single letters. The encryption process uses a 5x5 matrix of letters, where each letter of the plaintext is replaced by another letter according to specific rules.

1.2.1 Sample Problem of Playfair Cipher

Consider the plaintext "HELLO" and the keyword "MONARCHY". The steps are as follows:

1. Construct the key table by arranging the keyword followed by the remaining letters of the alphabet (excluding 'J').

<i>M</i>	<i>O</i>	<i>N</i>	<i>A</i>	<i>R</i>
<i>C</i>	<i>H</i>	<i>Y</i>	<i>B</i>	<i>D</i>
<i>E</i>	<i>F</i>	<i>G</i>	<i>I</i>	<i>K</i>
<i>L</i>	<i>P</i>	<i>Q</i>	<i>S</i>	<i>T</i>
<i>U</i>	<i>V</i>	<i>W</i>	<i>X</i>	<i>Z</i>

2. Divide the plaintext into digraphs: "HE", "LL", "OX".
3. Apply the Playfair cipher rules to each digraph: - "HE" → "BM" - "LL" → "PM" - "OX" → "OY"

Thus, the ciphertext is "BMPMOY".

Chapter 2

Implementation

2.1 Algorithm for RSA

The steps for the RSA algorithm are as follows:

1. Choose two large prime numbers p and q .
2. Compute $n = p \times q$ and $\phi(n) = (p - 1)(q - 1)$.
3. Choose a public exponent e such that $\gcd(e, \phi(n)) = 1$.
4. Compute the private key d , which is the modular inverse of e modulo $\phi(n)$.
5. To encrypt a message, use the formula $c = m^e \mod n$, where m is the plaintext.
6. To decrypt a message, use the formula $m = c^d \mod n$, where c is the ciphertext.

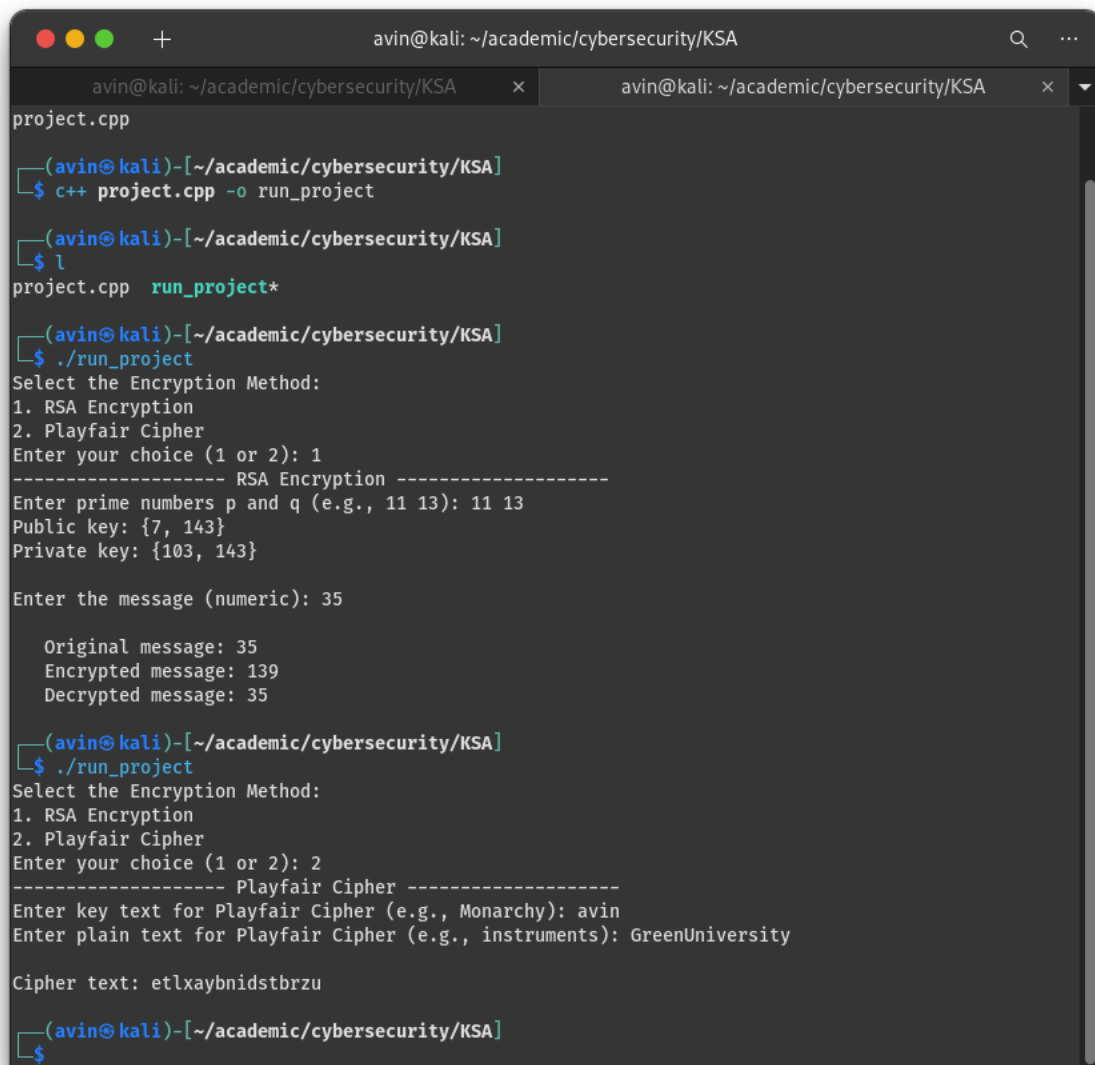
2.2 Algorithm for Playfair Cipher

The steps for the Playfair cipher are as follows:

1. Construct a 5x5 matrix using the keyword (exclude duplicates and fill the remaining spaces with the alphabet).
2. Divide the plaintext into digraphs.
3. For each pair of letters:
 - If both letters are in the same row, replace them with the letters to their immediate right.
 - If both letters are in the same column, replace them with the letters immediately below.
 - If the letters form a rectangle, replace them with the letters in the same row but in the column of the other letter.

Chapter 3

Snapshot



```
project.cpp
(avin@kali)~[/academic/cybersecurity/KSA]
$ c++ project.cpp -o run_project

(avin@kali)~[/academic/cybersecurity/KSA]
$ ./run_project
project.cpp  run_project*

(avin@kali)~[/academic/cybersecurity/KSA]
$ ./run_project
Select the Encryption Method:
1. RSA Encryption
2. Playfair Cipher
Enter your choice (1 or 2): 1
----- RSA Encryption -----
Enter prime numbers p and q (e.g., 11 13): 11 13
Public key: {7, 143}
Private key: {103, 143}

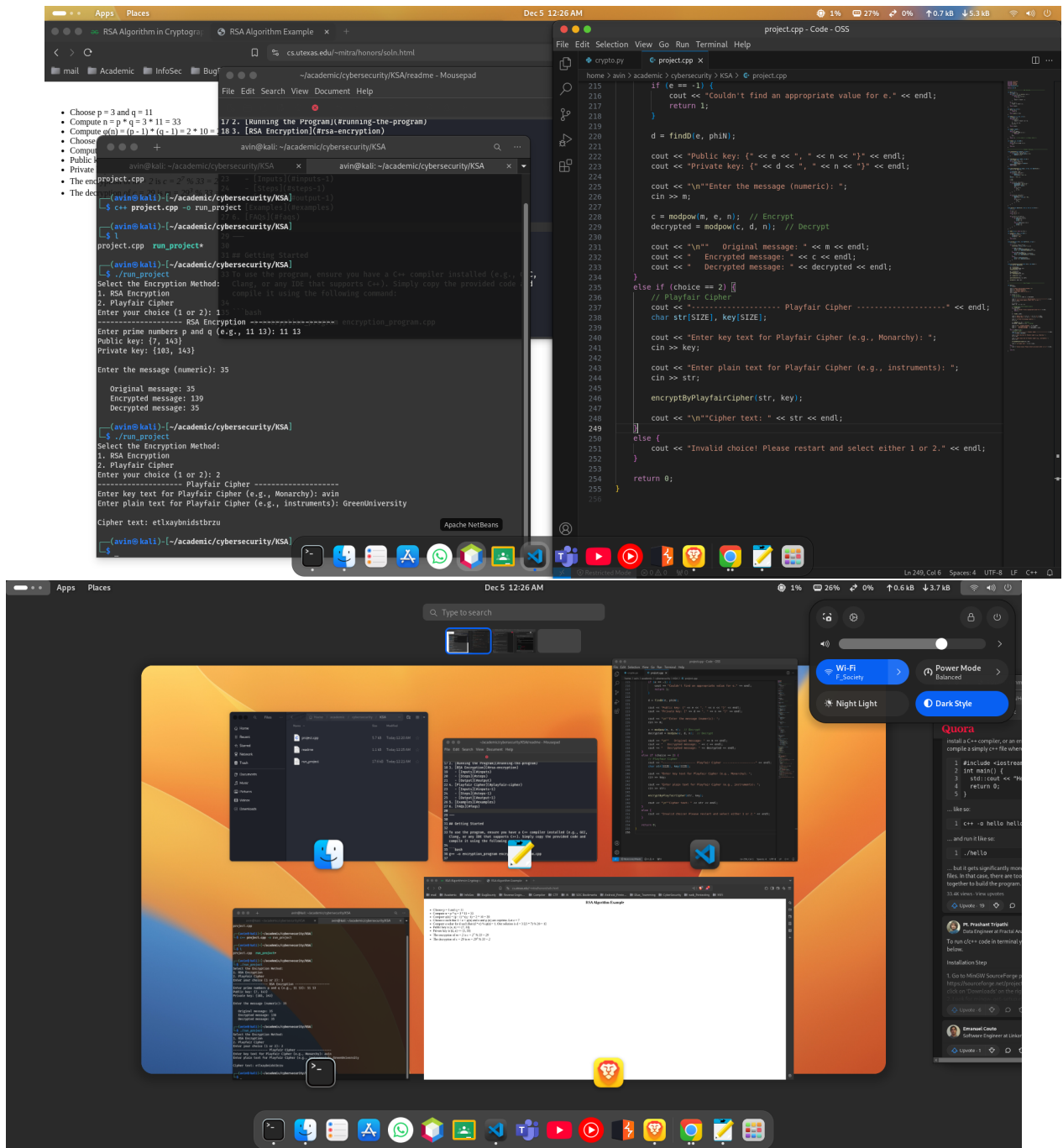
Enter the message (numeric): 35

    Original message: 35
    Encrypted message: 139
    Decrypted message: 35

(avin@kali)~[/academic/cybersecurity/KSA]
$ ./run_project
Select the Encryption Method:
1. RSA Encryption
2. Playfair Cipher
Enter your choice (1 or 2): 2
----- Playfair Cipher -----
Enter key text for Playfair Cipher (e.g., Monarchy): avin
Enter plain text for Playfair Cipher (e.g., instruments): GreenUniversity

Cipher text: etlxaybnidstbrzu

(avin@kali)~[/academic/cybersecurity/KSA]
$
```



Chapter 4

Comprehensive Analysis of RSA and Playfair Cipher

In this chapter, we will compare and analyze the strengths and weaknesses of both RSA and Playfair cipher.

4.1 Security Comparison

RSA: RSA is stronger in terms of security compared to Playfair because it uses asymmetric encryption. The security relies on the difficulty of factoring large numbers, and with sufficiently large primes, it is considered highly secure.

Playfair: Playfair is relatively weak by modern standards. It can be broken using frequency analysis and is susceptible to various cryptanalysis techniques. It is best used for educational purposes or in scenarios where security is not a primary concern.

4.2 Ease of Implementation

RSA: RSA is more complex to implement due to the need for large prime numbers, modular arithmetic, and key generation. It requires more computational resources, especially for key generation and encryption.

Playfair: Playfair is easier to implement compared to RSA. It is a classical cipher that involves basic matrix manipulation and is simpler to understand and program.

Chapter 5

Conclusion

In conclusion, RSA is a highly secure encryption algorithm based on number theory, suitable for applications that require high security but also involve significant computational resources. On the other hand, Playfair is a simpler cipher, more suitable for educational purposes and low-security applications, as it does not offer the same level of protection as RSA.

References

1. William Stallings, *Cryptography and Network Security: Principles and Practice*, 7th Edition, Pearson, 2017.
2. Neal Koblitz, *A Course in Number Theory and Cryptography*, Springer, 2007.
3. Alfred J. Menezes, *Handbook of Applied Cryptography*, CRC Press, 1997.