# NITTE MEENAKSHI INSTITUTE OF TECHNOLOGY

(AN AUTONOMOUS INSTITUTION, AFFILIATED TO VISVESVARAYA TECHNOLOGICAL UNIVERSITY,
BELGAUM, APPROVED BY AICTE & GOVT.OF KARNATAKA

Report on

# "Encryption and Decryption using RSA Algorithm"

*Submitted in partial fulfilment of the requirement for the award of Degree of*

*Bachelor of Engineering*

*in*

*Computer Science and Engineering*

Submitted by:

| | |
|---|---|
| Thota Thanmai | 1NT19CS203 |
| Pola Udaya Sowjanya Reddy | 1NT19CS136 |
| Riya Yadav | 1NT19CS159 |

## Department of Computer Science and Engineering

2022

Nitte Meenakshi Institute of Technology
(AN AUTONOMOUS INSTITUTION AFFILIATED TO VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELGAUM)
PB No. 6429, Yelahanka, Bangalore 560-064, Karnataka
Telephone: 080- 22167800, 22167860
Fax: 080 - 22167805

# DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

## CERTIFICATE

This is to certify that the Project Presentation in Cryptography and Network Security lab(18CSL68) as lab mini project titled **"Encryption and Decryption with AES Algorithm"** is an authentic work carried out by **Riya Yadav(1NT19CS159), Pola Udaya Sowjanya Reddy (1NT19CS136)**, **Thota Thanmai(1NT19CS203)** bonafide students of **Nitte Meenakshi Institute of Technology**, Bangalore in partial fulfilment for the award of the degree of **Bachelor of Engineering** in COMPUTER SCIENCE AND ENGINEERING of Visvesvaraya Technological University, Belagavi during the academic year **2022.**

| **Signature of the Guide** | | **Signature of the HOD** |
|---|---|---|
| Mr. Janardhan D. R | Dr. Dileep Reddy Bolla | Dr. Sarojadevi H. |
| Assistant Professor | Associate Professor | Professor,Head,Dept. CSE |
| Department of CSE,NMIT | Department of CSE,NMIT | NMIT Bangalore |

# DECLARATION

We hereby declare that

(i) This Presentation/report does not contain text, graphics or tables copied and pasted from the Internet, unless specifically acknowledged, and the source being detailed in the report and in the References sections.

(ii) All corrections and suggestions indicated during the internal presentation have been incorporated in the report.

(iii) Content of the report has been checked for the plagiarism requirement

| NAME | USN | Signature |
|---|---|---|
| Riya Yadav | 1NT19CS159 | |
| Thota Thanmai | 1NT19CS203 | |
| Pola Udaya Sowjanya Reddy | 1NT19CS136 | |

Date: 05-07-2022

# ACKNOWLEDGEMENT

The satisfaction and euphoria that accompany the successful completion of any task would be incomplete without the mention of the people who made it possible, whose constant guidance and encouragement crowned our effort with success. I/we express my/our sincere gratitude to our Principal **Dr. H. C. Nagaraj**, Nitte Meenakshi Institute of Technology for providing facilities.

I/we wish to thank our HoD**, Dr. Sarojadevi H** for the support and encouragement for the project work. I/We also thank him for the invaluable guidance provided which has helped in the creation of a better technical report.

I/We thank our guide Mr. Janardhan D R & Dr Dileep Reddy Bolla for the guidance and support given while doing this project work and preparing the report & presentation. I/We also thank all our friends, teaching, and non-teaching staff at NMIT, Bangalore, for all the direct and indirect help provided in the completion of the presentation.

Date: 05-07-2022

# ABSTRACT

Cryptography plays a huge role in our highly technological daily life, and we are profoundly depending on the science of hiding information in plain sight. There are numerous ways to achieve this, where number theory plays a huge role in cryptography to ensure that information cannot be easily recovered without special knowledge. One of the most reliable and secure encryption algorithms available today is the RSA algorithm, which provides great encryption and performance using asymmetric cryptography, also known as public-key cryptography. This project focuses on core functionality and implementation. In addition, the code implementation and the encryption and decryption procedure are provided in detail. Cryptographic technique is one of the principals means to protect information security. Not only has it to ensure the information confidential, but also provides digital signature, authentication, secret sub-storage, system security and other functions. Key in the encryption algorithm has a pivotal position, once the key was leaked, it means that anyone can be in the encryption system to encrypt and decrypt information, it means the encryption algorithm is useless. Therefore, what kind of data you choose to be a key, how to distribute the private key, and how to save both data transmission keys are very important issues in the encryption and decryption algorithm. This project proposed an implementation of a practical RSA encrypt/decrypt solution based on the study of RSA public key algorithm.

# TABLE OF CONTENTS

# 1. INTRODUCTION

Encryption is one of the principals means to grantee the security of sensitive information. It not only provides the mechanisms in information confidentiality, but also functioned with digital signature, authentication, secret sub-keeping, system security etc. Therefore, the purpose of adopting encryption techniques is to ensure the information's confidentiality, integrity, and certainty, prevent information from tampering, forgery, and counterfeiting [1]. At present, the best known and most widely used public key system is RSA, which was first proposed in paper "A method for obtaining digital signatures and public-key cryptosystems" by RL Rivest et al. in 1978. It is an asymmetric (public key) cryptosystem based on number theory, which is a block cipher system. Its security is based on the difficulty of the large number prime factorization, which is a well-known mathematical problem that has no effective solution [2]. RSA public key cryptosystem is one of the most typical ways that most widely used for public key cryptography in encryption and digital signature standards. RSA is a public-key or asymmetric crypto system. It uses a public key for encryption and a private key for decryption. Anyone can use the public key to encrypt a message, but it can be decrypted only by the private key owner.

The RSA algorithm RSA (Rivest-Shamir-Adleman) is an asymmetric cryptographic algorithm used to encrypt and decrypt messages by modern computers. Asymmetric states that there are two different keys used in the encryption and decryption process, which also is called public-key cryptography. This is simply because one of the two key scans be given to anyone without exploiting the security of the algorithm. The RSA algorithm involves both private and public keys. The public key can be known and published to anyone, as it is used to encrypt the messages from plaintext to ciphertext. The messages that are encrypted with this specific public key can however only be decrypted with the corresponding private key. The key generation process of the RSA algorithm is what makes it so secure and reliable today, as it contains a high level of complexity compared to other cryptographic algorithms

## 2. Working of RSA:

It works on two keys:

**Public key:** It comprises of two numbers, in which one number is the result of the product of two large prime numbers. This key is provided to all the users.

**Private key:** It is derived from the two prime numbers involved in public key and it always remains private.

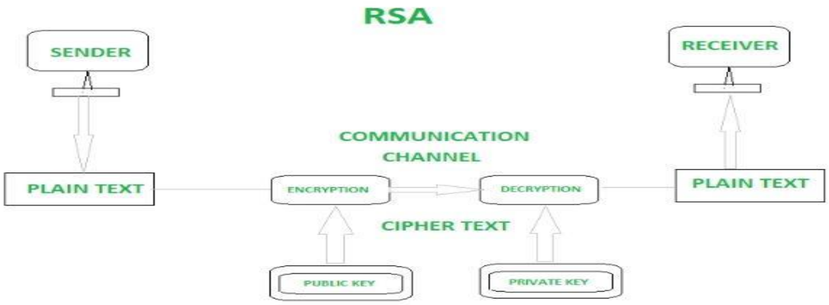


Fig 1: Encryption and Decryption using RSA

## 3. Characteristics of RSA

- It is a public key encryption technique.
- It is safe for exchange of data over internet.
- It maintains confidentiality of the data.
- RSA has high toughness as breaking into the keys by interceptors is very difficult.
- Advantages of RSA
- It is very easy to implement RSA algorithm.
- RSA algorithm is safe and secure for transmitting confidential data.
- Cracking RSA algorithm is very difficult as it involves complex mathematics.
- Sharing public key to users is easy.
- Disadvantages of RSA
- It may fail sometimes because for complete encryption both symmetric and asymmetric encryption is required and RSA uses symmetric encryption only.
- It has slow data transfer rate due to large numbers involved.
- It requires third party to verify the reliability of public keys sometimes.
- High processing is required at receiver’s end for decryption.

# 4. ADVANTAGES AND DISADVANTAGES

## ADVANTAGES:

- RSA is stronger than any other symmetric key algorithm.
- RSA has overcome the weakness of symmetric algorithm i.e., authenticity and confidentiality.
- More comfortable to implement.
- Easier to understand.
- Signing and decryption are similar; encryption and verification are similar.
- Widely deployed, better industry support.

## DISADVANTAGES:

- RSA has too much computation.
- Very slow key generation.
- Slow signing and decryption, which are slightly tricky to implement securely.
- The two-part key is vulnerable to GCD attack if poorly implemented.

# 5. DESIGN OF SOLUTION

In Asymmetric Encryption algorithms, you use two different keys, one for encryption and the other for decryption. The key used for encryption is the public key, and the key used for decryption is the private key. But, of course, both the keys must belong to the receiver.

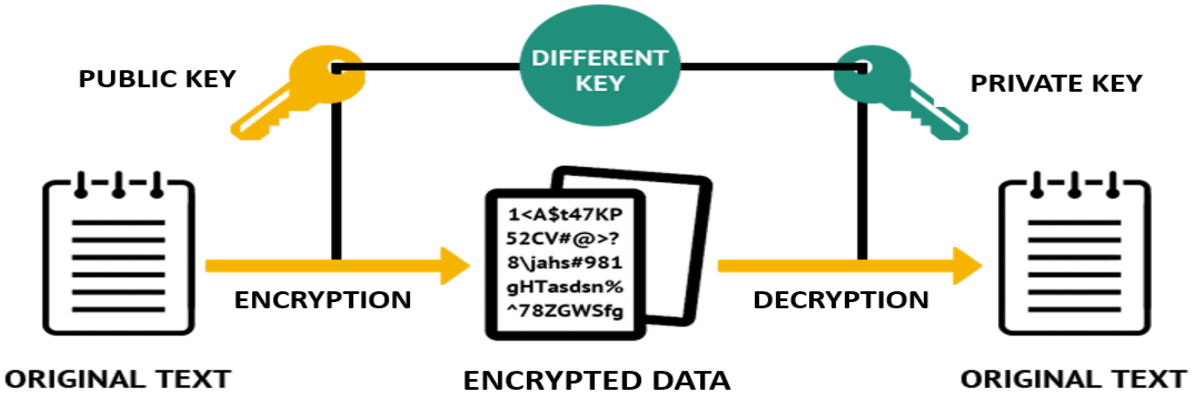


Fig 2:Asymmetric Encryption using RSA

As seen in the image above, using different keys for encryption and decryption has helped avoid key exchange, as seen in symmetric encryption.

For example, if Alice needs to send a message to Bob, both the keys, private and public, must belong to Bob.

## Encryption and Decryption Process :

After computing all the necessary variables for the key generation, it is time to encrypt and decrypt a message using the algorithm. This is of course given the fact that public has been generated, and consists of n and e. The formula is very simple for both the encryption and decryption process, which states that:

Encryption: c ≡ me (mod n), where m is the message in plaintext.

Decryption: m ≡ cd(mod n), where c is the ciphertext.

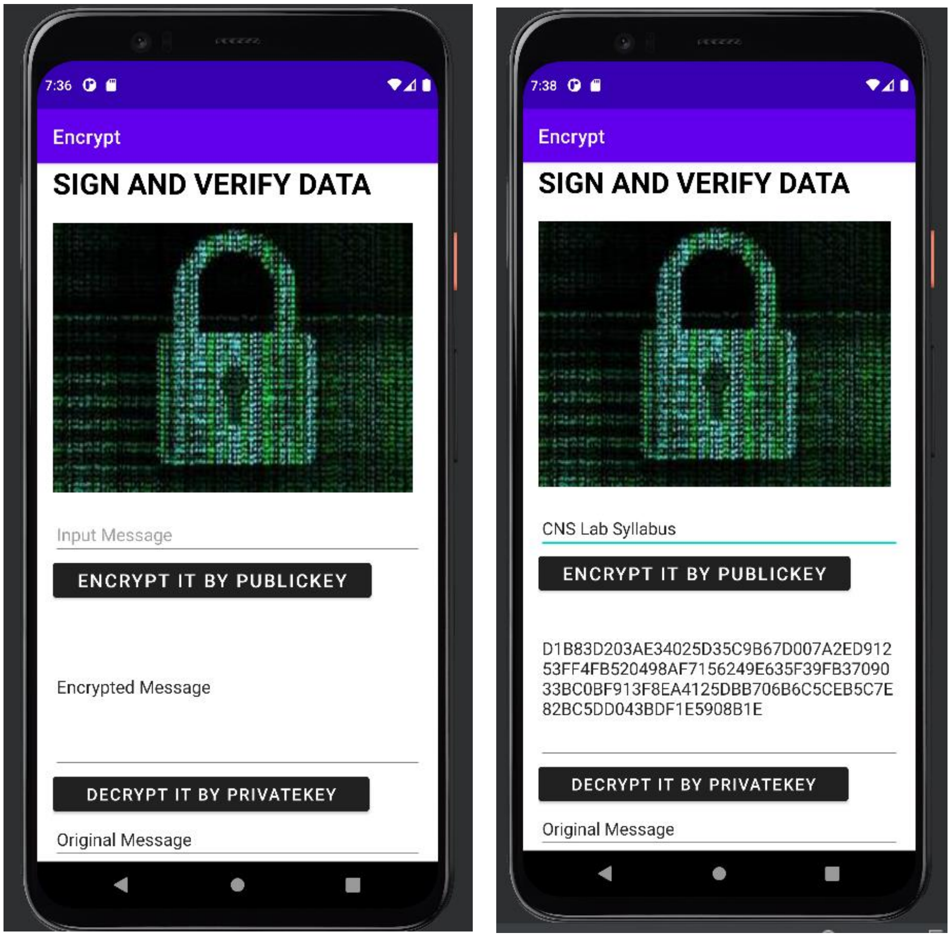
Anyone who wants to encrypt a message needs to use the public key of the recipient , to ensure that the message is only decryptable by the correct individual so that it only decrypts with a specific private key. The recipient shares the public key, while keeping the private key secret. The sender then wants to submit a message M, which gets transformed into a smaller number than n, and this is done by a reversible protocol known as a padding scheme. The message gets computed into an encrypted ciphertext, which at last gets submitted over to the recipient.

The padding scheme used in the encryption process is quite important, and without this scheme there would be some problems. The padding scheme ensures that no values of the message are insecure, such as for example the values m = 0 or m = 1 will respectively compute ciphertexts equal to 0 or 1, which is caused by the properties of the exponentiation. When the exponent used in the key generation process is small, this might cause the non-modular result of me to be less than the modulus n. This means that ciphertexts may be brute forced and decrypted easily by calculating the e-th root of the ciphertext without necessarily regarding the modulus.

For example, when encrypting a text with the numeric value of 0, it would encode as m = 0, which then again computes the ciphertext c = 0, with no concern about the values of n and e. The same goes for the numeric value of 1, which produces the value of 1 in ciphertext. This creates an insecure pattern, which might be analysed by attackers and easily decrypted after gaining some knowledge about the encryption process.

To avoid such problems in the algorithm, it is common to implement a randomized padding into the message before the encryption happens. This is to ensure that the message does not contain some insecure values and that the encrypted ciphertext contains some padded values that generate a larger ciphertext. This increases the level of complexity of the encryption and will most likely make a dictionary attack harder to succeed.

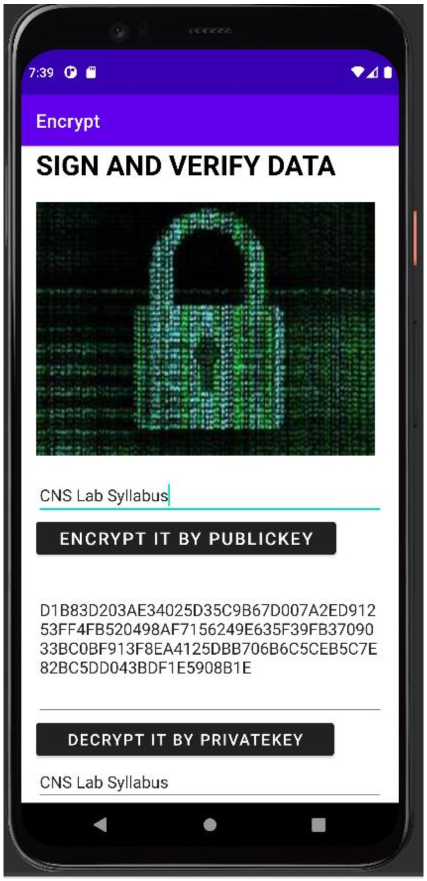
# 6. IMPLEMENTATION



CNS Lab Syllabus

```
D1B83D203AE34025D35C9B67D007A2ED912
53FF4FB520498AF7156249E635F39FB37090
33BC0BF913F8EA4125DBB706B6C5CEB5C7E
82BC5DD043BDF1E5908B1E
```

Fig 3: Encryption using public key



CNS Lab Syllabus

```
D1B83D203AE34025D35C9B67D007A2ED912
53FF4FB520498AF7156249E635F39FB37090
33BC0BF913F8EA4125DBB706B6C5CEB5C7E
82BC5DD043BDF1E5908B1E
```

CNS Lab Syllabus

Fig 4: Decryption using public key

# 7. CONCLUSION

The RSA algorithm is a very interesting cryptographic algorithm, and it is one of the best and most secure algorithms available as of today. It provides great encryption and is reliable in terms of security and performance. The encryption security relies on the fact that the prime numbers used during the key generation process must be large enough to be unbreakable, and this is quite interesting. There might be a time in the future when super-computers are able to break these, but that would not be anytime soon at least. Even though the algorithm provides great encryption and it is reliable, the overall security really relies on the program developer or the algorithm user. If the user picks small prime numbers, it compromises a lot of the security that the RSA algorithm provides, and therefore is very vulnerable to cryptanalysis and brute force attacks. So, in other words, just using the RSA algorithm is not enough - it must be used properly to gain the encryption level it initially provides, as it must be used correct in terms of the key generation process and the initial preparation of the algorithm.  In the end, it proposed a new program to improve RSA algorithm based on RSA cryptography and the extensive application .In summary, this issue of the RSA encryption and decryption keys, RSA algorithm, the new use of the RSA and other issues to study and make some new programs, future work should be in the new RSA cryptographic algorithms and a wide range of applications continue to research.

# REFERENCES

**[1]** W. Diffie and M. E. Hellman, New directions in cryptography, IEEE Trans. Inform. Theory, Nov. 1976,22: 644-654.

**[2]** R.L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM, Feb. 1978, 21(2): 120-126.

[3] Xin Zhou and Xiaofei Tang, "Research and implementation of RSA algorithm for encryption and decryption," Proceedings of 2011 6th International Forum on Strategic Technology, 2011, pp. 1118-1121,doi:10.1109/IFOST.2011.6021216.

Available: https://ieeexplore.ieee.org/document/6021216

[4]https://www.comparitech.com/blog/information-security/rsa-encryption/#:~:text=Under%20RSA%20encryption%2C%20messages%20are,known%20as%20the%20private%20key

[5] https://www.researchgate.net/publication/338623532_The_RSA_Algorithm