International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT2390130

File Encryption and Decryption using AES and RSA Algorithm

Manasvi Malhar Sudershan*, Sai Varshan Pydakula, Aarthi Priya R
Department of Information Technology, B V Raju Institute of Technology, Narsapur, Telangana, India

ARTICLEINFO

Article History:

Accepted: 15 Feb 2023
Published: 05 March 2023

Publication Issue
Volume 10, Issue 2
March-April-2023

Page Number
11-14

ABSTRACT

In the present scenario, no technology that's connected to the internet is unhackable. All digital services like internet communication, military and medical imaging systems, multimedia systems require reliable security in storage and transmission of digital images. The importance of protecting digital images cannot be overstated. Therefore, there is a need for image encryption techniques in order to hide images from such attacks.

In this encryption process, we use AES and RSA Algorithm in order to hide images. This encryption techniques helps us to avoid intrusive attacks. Since, the image is encrypted using the AES technique, only the receiver can view it, as the key is known only to the sender and receiver. Overall, image encryption improves data integrity and can raise consumer trust.

Keywords : Encryption, decryption, AES algorithm, RSA algorithm, vulnerability, Integrity

I. INTRODUCTION

File encryption and decryption are critical techniques used to protect sensitive information from unauthorized access. In recent years, the use of encryption and decryption has become increasingly important as more and more data is stored and transmitted electronically. With the rise of cybercrime, file encryption and decryption have become essential tools for safeguarding personal and corporate information. Organizations and individuals alike use encryption and decryption to protect sensitive information, such as financial data, personal information, and trade secrets. This research paper aims to explore the concepts of file encryption and decryption, the different types of encryption algorithms used, and their applications in the modern world.

A. Encryption

Encryption is the process of converting plaintext or unencrypted data into ciphertext or encrypted data. The encryption process involves the use of a secret key or a combination of keys and algorithms to transform the original data into an unreadable format. The encrypted data can only be decrypted and converted back to its original form using the appropriate decryption key.

B. Decryption

Decryption is the process of converting encrypted data back into its original form using a key or

password. The process involves reversing the encryption algorithm used to encrypt the data.

C. AES

AES (Advanced Encrypted Standard) is a symmetric-key encryption algorithm used to encrypt data. It uses a fixed block size of 128 bits and supports key sizes of 128,192, or 256 bits. It operates on a 4x4 matrix of bytes, called the state, and applies a series of substitution and permutation operations on the state based on a key.

D. RSA

RSA is a public-key algorithm based on the mathematical concept of modular arithmetic and the difficulty of factoring large prime numbers. It involves use of a public key and a private key. It involves the use of a public key and a private key. The public key is used for encrypting data, while the private key is used for decrypting the data.

II. METHODS AND MATERIAL

AES and RSA algorithms are used together to achieve secure file encryption and decryption. The symmetric key generated by AES is used to encrypt the file, while the asymmetric RSA algorithm is used to securely share the symmetric key with the recipient.

A. Phases

File Encryption and Decryption using AES and RSA algorithm includes following phases:

1) File Encryption
2) File Decryption

1) File Encryption: File encryption includes following steps.

- Input is given as file to the software.
- Generate a random symmetric key (secret key).
- Encrypt the file using the secret key.
- Public key and private keys are generated at receiver end using RSA algorithm.
- Public key is sent to sender from recipient.
- Encrypt the symmetric key using RSA.

2) File Decryption: File Decryption includes following steps.

- Send the encrypted file and the encrypted symmetric key.
- Secret key is decrypted from public key using private key (RSA).
- Encrypted file is decrypted using the decrypted secret key using AES.
- Original file is acquired by the receiver.

B. Algorithms

We have used:

1) Advanced Encryption Standard (AES) algorithm
2) Rivest Shamir Adleman (RSA) algorithm

1) Advanced Encryption Standard (AES) algorithm:
AES (Advanced Encryption Standard) is a widely used encryption algorithm that is used to protect sensitive information. It is a symmetric key encryption algorithm, which means that the same key is used for both encryption and decryption of the data. AES was developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, in 1998. It was adopted by the U.S. government as the official standard for encryption in 2001, replacing the earlier Data Encryption Standard (DES).

AES operates on 128-bit blocks of data and supports key lengths of 128, 192, or 256 bits. The algorithm consists of a series of rounds, each of which performs a series of substitutions and permutations on the data using a round key derived from the original encryption key.

2) Rivest Shamir Adleman (RSA) algorithm: RSA is an encryption algorithm that is widely used for secure communication over the internet. It was invented by Ron Rivest, Adi Shamir, and Leonard Adleman in 1977 and is named after their surnames. The RSA

algorithm is based on the mathematical properties of prime numbers and their factors.

In RSA encryption, a sender encrypts a message using the recipient's public key, and the recipient decrypts the message using their private key. The security of the algorithm relies on the difficulty of factoring large composite numbers into their prime factors.

III.RESULTS AND DISCUSSION

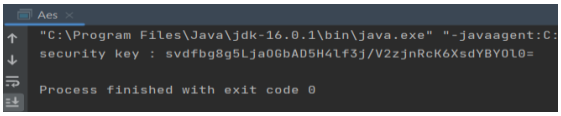
A. File Encryption

1) Input: Software asks for input file of format jpg/mp4/pdf/docx/ppt/apk/xlsx/mp3.

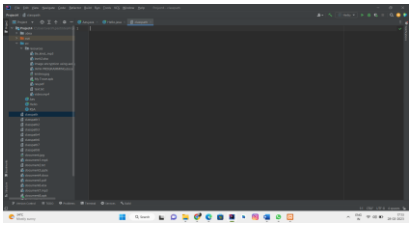
Input file (Image)

2) Generation of Asymmetric keys and transmission of public key from Recipient to sender: Public key and private keys are generated using RSA algorithm at recipient end. Then, public key sent the to the sender.

3) Generate a random symmetric key (Secret key): A random 256-bit security key is generated.



4) Encrypt the file and encrypt the security key : An encrypted file classpath.enc is generated using AES security key along with the encrypted secret key using RSA algorithm.

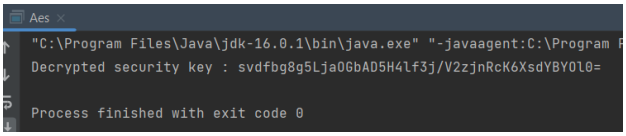


Encrypted file along with security key (showing blank)

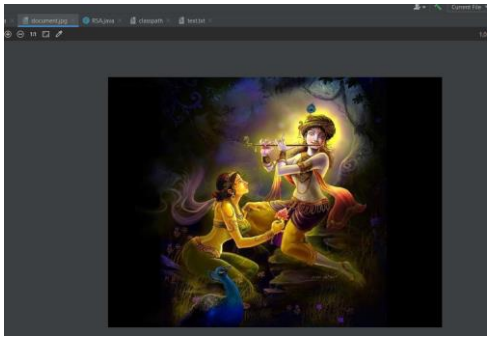
5) Send the encrypted file and the encrypted symmetric key: The encrypted file and the encrypted symmetric key are sent to the recipient.

B. File Decryption

1) Decrypt the encrypted security key using RSA: The encrypted security key is decrypted using RSA private key.



2) Decrypt the file using the security key: The encrypted file is decrypted using the decrypted security key.



Decrypted image

IV.CONCLUSION

Overall, the encryption and decryption have numerous applications, such as protecting financial information, confidential business documents, personal information, and intellectual property. It is

also used in securing communications over the internet, such as email and instant messaging.

file encryption and decryption are essential tools for securing sensitive data, and it is crucial to choose the right encryption algorithm and key management strategies to ensure maximum security. It is also important to keep the encryption key secure and to follow best practices for encryption and decryption to avoid any security breaches or data loss.

V. REFERENCES

[1]. "Handbook of Applied Cryptography" by Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone.

[2]. "A survey of symmetric key encryption techniques" by H. Abdalla, J. Garay, and P. Papadimitriou

[3]. https://www.itprotoday.com/windows-78/how-do-i-encryptdecrypt-file

[4]. https://blog.box.com/what-is-file-encryption

[5]. https://www.researchgate.net/figure/RSA-algorithm-structure_fig2_298298027

[6]. https://www.researchgate.net/figure/The-basic-AES-128-cryptographic-architecture_fig1_230853805

[7]. https://docs.huihoo.com/globus/gt4-tutorial/ch09s02.html

Cite this article as :

Manasvi Malhar Sudershan, Sai Varshan Pydakula, Aarthi Priya R, "File Encryption and Decryption using AES and RSA Algorithm", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 2, pp.11-14, March-April-2023. Available at doi : https://doi.org/10.32628/CSEIT2390130

Journal URL : https://ijsrcseit.com/CSEIT2390130