IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

"RSA-AES Hybrid Encryption: Combining The Strengths Of Two Powerful Algorithms For Enhanced Security"

Venkata Mahesh Babu Batta *
https://orcid.org/0000-0002-1029-6402
Dr.L.K.Suresh Kumar **

(* M.Tech, Department of CSE, University College of Engineering, Osmania University, Hyderabad, Telangana, India,
** Associate Professor, Department of CSE, University College of Engineering, Osmania University, Hyderabad,Telangana,India)

Abstract: Hybrid Encryption is a technique that combines the strengths of symmetric and asymmetric encryption to provide enhanced security for data transmission. The AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman) algorithms are two of the most widely used encryption techniques for securing data in transit. This paper proposes a hybrid encryption technique that utilizes both AES and RSA algorithms to achieve enhanced security. In this approach, the symmetric AES algorithm is used to encrypt the actual data, while the asymmetric RSA algorithm is used to encrypt the AES key. The proposed technique offers several advantages over traditional symmetric or asymmetric encryption approaches. It provides enhanced security by using a combination of strong encryption algorithms, making it difficult for an attacker to decrypt the data. Additionally, the technique is efficient in terms of performance since the data is encrypted using the faster symmetric AES algorithm. The proposed hybrid encryption technique using AES and RSA algorithms offers enhanced security for data transmission while maintaining efficiency. It can be used in various scenarios where security is a concern, including online transactions, file transfers and email communication.

Keywords: Encryption, Advanced Encryption Standard, RSA algorithm, Cryptography.

1. Introduction:

Information security is the practice of protecting digital information from unauthorized access, use, disclosure, disruption, modification, or destruction. It involves implementing various security measures to safeguard information assets and ensure their confidentiality, integrity, and availability. Common information security measures include access controls, firewalls, intrusion detection and prevention systems, encryption, and incident response plans. Information security is critical for protecting sensitive information such as financial records, personal data, and intellectual property. A breach in information security can result in significant financial losses, legal liabilities, and damage to reputation. Effective information security requires a comprehensive and proactive approach to identify and address potential threats and vulnerabilities

1.1 Cryptography: Cryptography is a secure information and communication technique. It is derived form mathematical concepts and a set of rule-based calculations called algorithms to transform messages in ways that are hard to decipher

1.2 Encryption: Encryption is the process of converting plain text into a coded or scrambled form of data to protect its confidentiality. It is a crucial technique used to secure sensitive information during data transmission or storage. Encryption algorithms use complex mathematical algorithms and keys to scramble data into an unreadable form, making it difficult for unauthorized users to access or interpret the information. The most common encryption algorithms include Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Rivest-Shamir-Adleman (RSA). Encryption plays a vital role in ensuring the security of online transactions, email communications, and sensitive data such as financial records, personal data, and intellectual property.

1.3 Data Encryption Standard: Data Encryption Standard (DES) is a symmetric encryption algorithm that was widely used in the past for securing data transmission and storage. It is a block cipher algorithm that operates on 64-bit blocks of data and uses a 56-bit key to encrypt and decrypt the data. The algorithm works by dividing the data into blocks and then scrambling them with the secret key.

DES is a fast and efficient encryption algorithm, but it is no longer considered secure due to its small key size. The short key length makes it vulnerable to brute-force attacks, where an attacker can try all possible key combinations to decrypt the data.

Triple DES (3DES) was introduced to improve the security of DES by applying the algorithm three times with different keys. However, 3DES is slower and less efficient than other modern encryption algorithms.

Due to its security limitations, DES has been replaced by the more advanced and secure Advanced Encryption Standard (AES) as the preferred encryption algorithm. However, DES is still used in some legacy systems and applications. 3 DES Encryption is a cryptography in which block cipher algorithms are used.

2. Advanced Encryption Standard and RSA Alogorithm:

2.1 Advanced Encryption Standard: Advanced Encryption Standard (AES) is a popular symmetric encryption algorithm that provides strong security for data transmission and storage. It was chosen by the National Institute of Standards and Technology (NIST) to replace the outdated Data Encryption Standard (DES). AES uses a block cipher to encrypt data, which involves dividing the data into blocks and then scrambling them with a secret key. It supports key sizes of 128, 192, and 256 bits, and is considered one of the most secure encryption algorithms available. AES is used in various applications, including online transactions, wireless networks, and government communications. Its widespread use and adoption have made it an essential tool for information security.

2.1.1 Advanced Encryption Standard (AES) algorithm Design: It is a symmetric encryption algorithm that operates on blocks of data. The algorithm works as follows:

1. Key Expansion: The AES algorithm starts by expanding the secret key into a set of round keys using a key schedule. The key schedule applies a series of operations to the secret key to generate the round keys.
2. Initial Round: The algorithm begins by dividing the plaintext into blocks of 128 bits. The first round of encryption involves XORing the plaintext with the first round key.
3. Rounds: The algorithm then applies a series of rounds to the encrypted data, each round consisting of the following four steps:
   a. Substitution: The 16-byte block of data is substituted with a new block using a substitution table called the S-box.
   b. Permutation: The data is then rearranged using a permutation operation called the ShiftRows step.
   c. Mixing: The data is mixed using a matrix multiplication operation called the MixColumns step.
   d. Key Addition: The round key is XORed with the result of the previous steps.
4. Final Round: The final round of encryption skips the MixColumns step and only performs the Substitution, Permutation, and Key Addition steps.
5. The resulting ciphertext is the encrypted form of the original plaintext.

The decryption process involves applying the inverse operations in reverse order, using the same round keys in reverse order.

2.2. RSA algorithm:

RSA (Rivest-Shamir-Adleman) is an asymmetric encryption algorithm that uses public and private keys to encrypt and decrypt data. It is widely used for secure data transmission and storage. RSA involves the generation of a public and private key pair. The public key is made available to anyone who needs to send encrypted data to the recipient, while the private key is kept secret and used by the recipient to decrypt the data. RSA is based on the mathematical principles of prime factorization, where the security of the algorithm relies on the difficulty of factoring large prime numbers. RSA supports key sizes ranging from 1024 bits to 4096 bits, with larger key sizes offering stronger security. RSA is used in various applications, including secure email communications, online transactions, and digital signatures.

2.2.1 The RSA (Rivest-Shamir-Adleman) algorithm Design:

It is an asymmetric encryption algorithm that uses a public key and a private key to encrypt and decrypt data. The encryption algorithm works as follows:

1. Key Generation: The first step in RSA encryption is to generate a key pair consisting of a public key and a private key. The public key is made available to anyone who needs to send encrypted data to the recipient, while the private key is kept secret and used by the recipient to decrypt the data.
2. Message Encryption: To encrypt a message, the sender must first represent the message as a number M. The sender then applies the following encryption formula to the message:
   C = M^e mod n
   where C is the ciphertext, e is the recipient's public key exponent, and n is the recipient's public key modulus.
3. The resulting ciphertext C is sent to the recipient.

The decryption process involves applying the inverse operation, using the private key instead of the public key. The decryption algorithm works as follows:

1. The recipient receives the ciphertext C.
2. Decryption: The recipient applies the following decryption formula to the ciphertext:
   M = C^d mod n
   where M is the original plaintext message, d is the recipient's private key exponent, and n is the recipient's public key modulus.
3. The resulting decrypted message M is the original plaintext message.

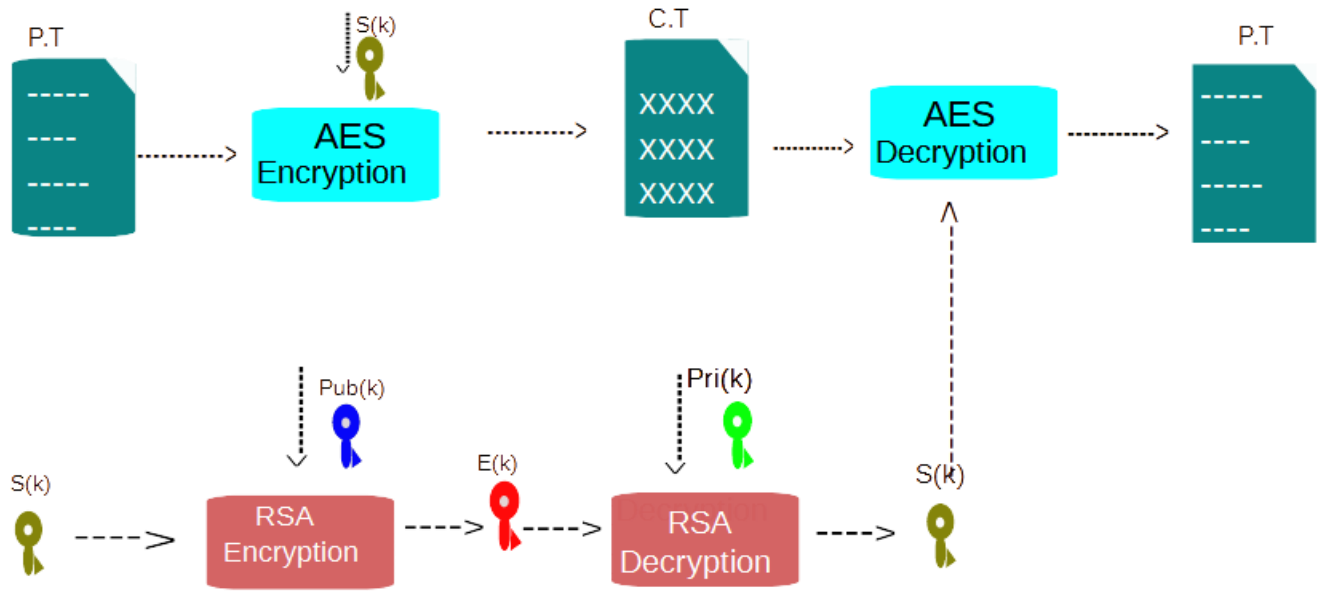
It is important to note that the RSA algorithm can only encrypt messages that are shorter than the key size, and therefore is often used in combination with symmetric encryption techniques for encrypting longer messages.

3. RSA-AES Hybrid encryption:

It is a combination of symmetric and asymmetric encryption techniques to provide enhanced security for data transmission and storage. It involves the use of a symmetric encryption algorithm such as AES to encrypt the actual data, and an asymmetric encryption algorithm such as RSA to encrypt the symmetric key used to encrypt the data. This technique addresses the limitations of both symmetric and asymmetric encryption, providing a more secure and efficient approach to encryption.

In hybrid encryption, the sender generates a random symmetric key to encrypt the data, and then encrypts the symmetric key using the recipient's public key. The encrypted data and the encrypted symmetric key are then sent to the recipient. Upon receiving the message, the recipient decrypts the symmetric key using their private key and then uses the decrypted symmetric key to decrypt the actual data.

Hybrid encryption offers several advantages, including enhanced security, improved efficiency, and flexibility. It is commonly used in various applications, including online transactions, secure email communications, and cloud storage.

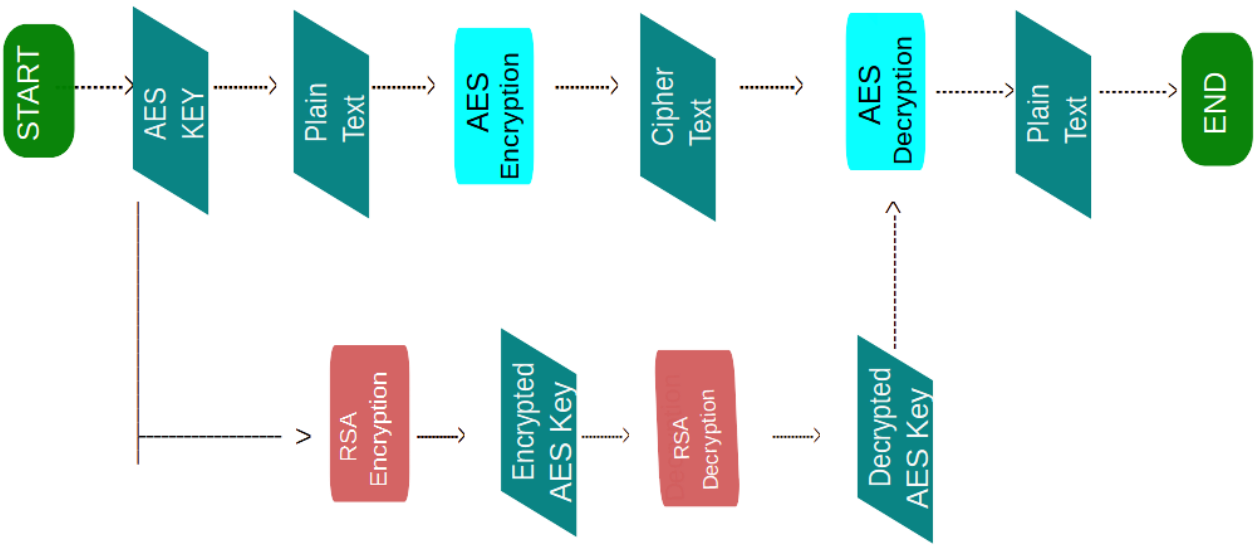


P.T plain text
C.T cipher text

S(k) Symmetric key
E(k) Encrypted key

Pub(k) Public key
Pri(k) Private key

RSA-AES HYBRID ENCRYPTION



RSA-AES HYBRID ENCRYPTION FLOWCHART

RESULTS: **Note:** Software Used: java version "1.8.0_211"

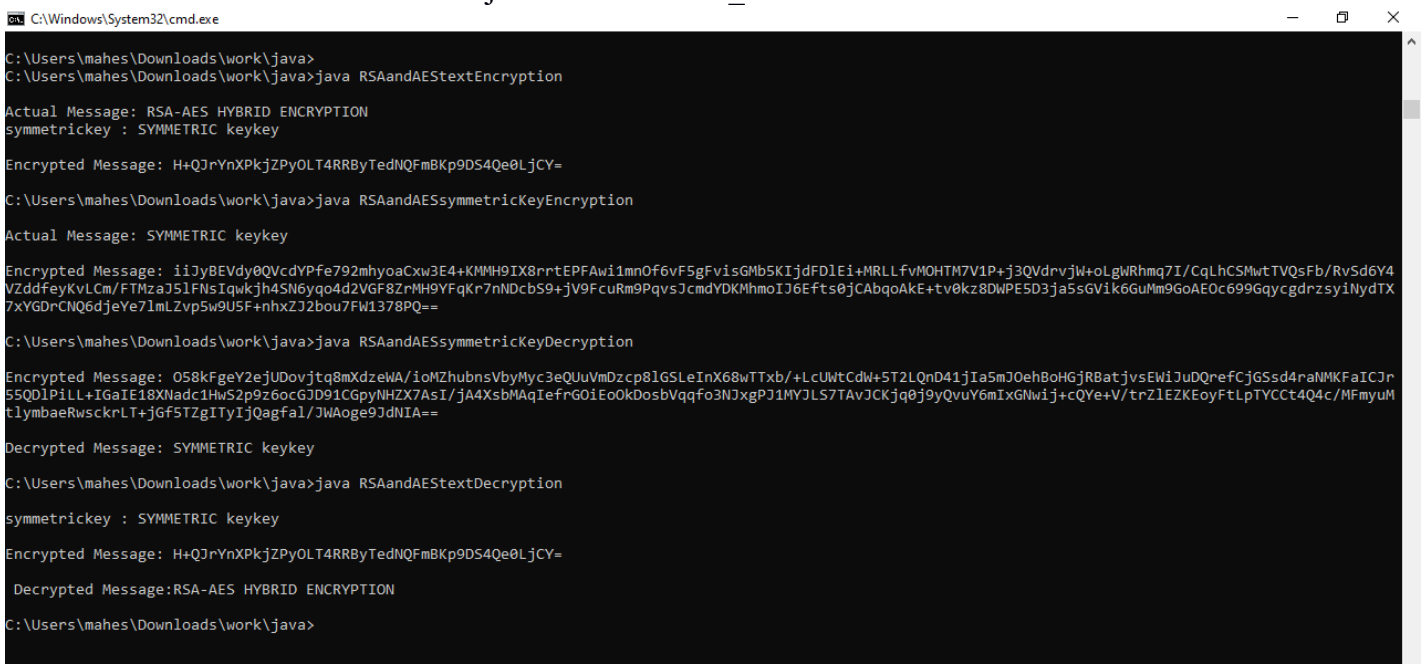


Figure: RSA-AES Hybrid Encryption

Plain Text in AES is : RSA-AES HYBRID ENCRYPTION
Symmetric Key in AES is : SYMMETRIC keykey
Plain Text in RSA is: SYMMETRIC keykey

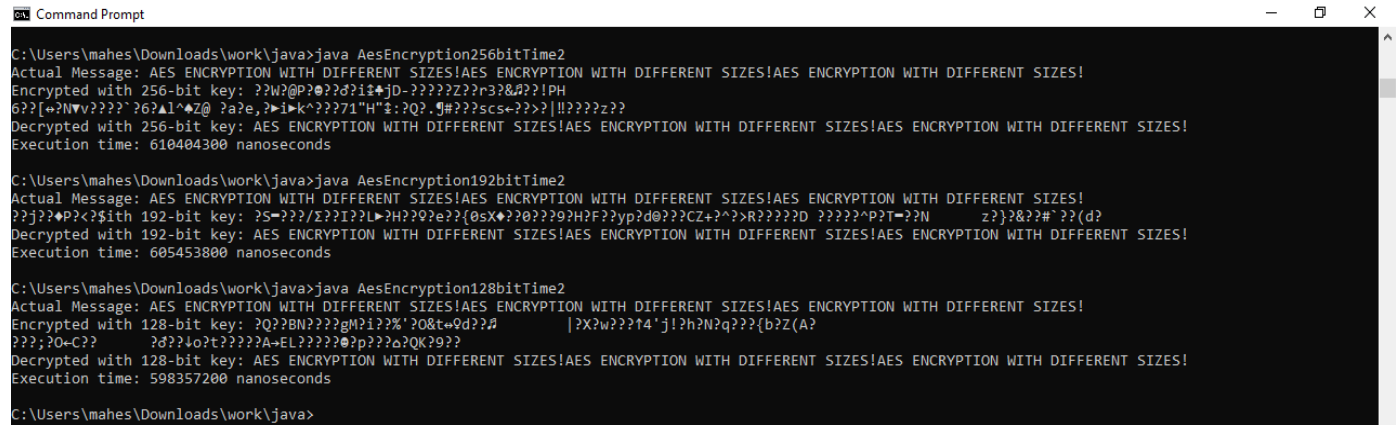


Figure:AES Encryption (128-bit, 192-bit,256-bit key)

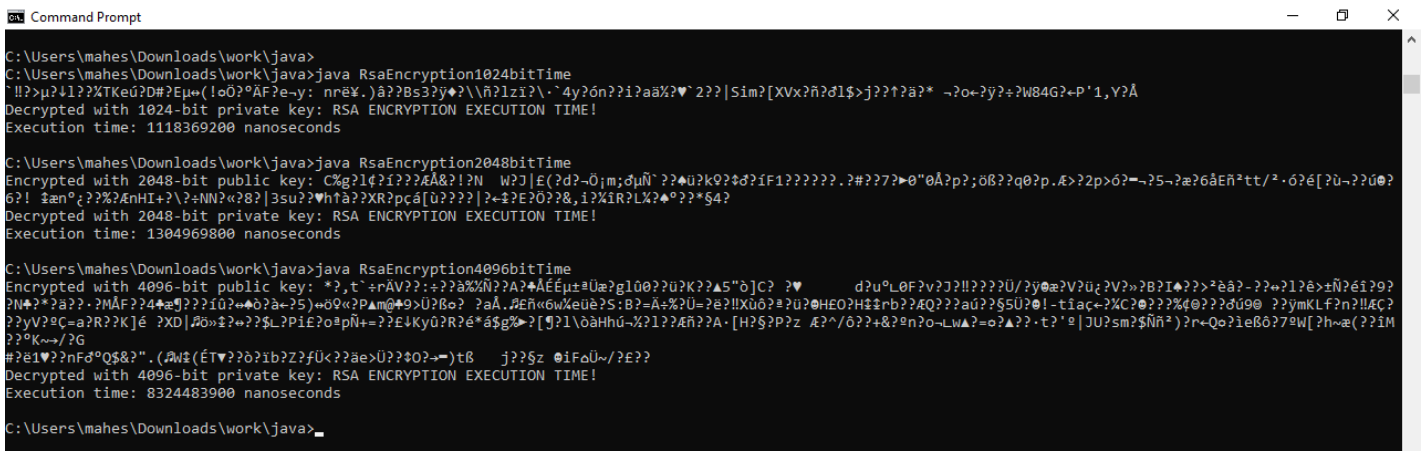


Figure: RSA Encryption (1024-bit, 2048-bit,4096-bit key)

In AES encryption, the size refers to the number of bits in the key used for encryption. The key size affects the strength of the encryption and the computational resources required to perform the encryption and decryption operations. The standard AES key sizes are 128-bit, 192-bit, and 256-bit.

	128-bit	192-bit	256-bit
Key combinations	2^128	2^192	2^256
Security	High	Higher	Highest
Time	Low	Medium	High
performance	Good	Medium	Low

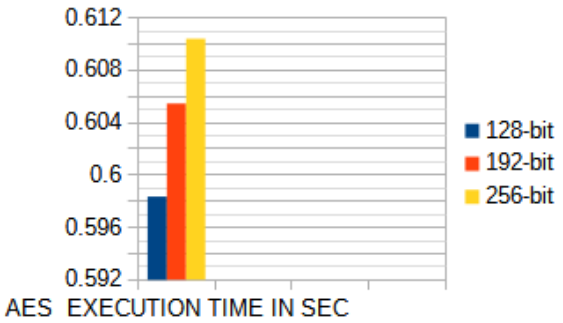
Table: AES ENCRYPTION

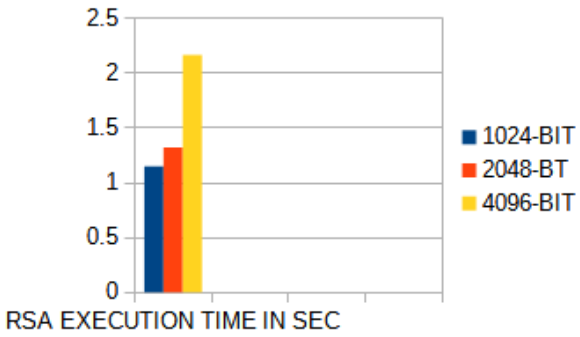
In RSA encryption, the key size refers to the number of bits in the public and private keys used for encryption and decryption. The key size affects the strength of the encryption and the computational resources required to perform the encryption and decryption operations. The standard RSA key sizes range from 1024-bit to 4096-bit, although larger key sizes are becoming increasingly common.

	1024-bit	2048-bit	3072-bit	4096-bit
Key combinations	2^1024	2^2048	2^3072	2^4096
Security	Vulnerable	High	Higher	Highest
Time	Least	Low	Medium	Highest
performance	Good	Medium	Slower	Much slower

Table: RSA ENCRYPTION

However, as with AES encryption, the larger the key size, the more computational resources are required to perform the encryption and decryption operations. This means that using larger key sizes can result in slower performance and higher costs for hardware and software. Therefore, it's important to balance the desired level of security with the practical limitations of the system in which the encryption is being used.





Note : Values are taken from the above programs

Conclusion and Future work:

In conclusion, hybrid encryption using AES and RSA offers a powerful and flexible approach to data encryption. The combination of symmetric AES encryption and asymmetric RSA encryption provides the benefits of both techniques, including high-speed encryption and decryption, strong security, and flexibility in key management. Various research works have shown that the hybrid encryption using AES and RSA algorithm provides secure data transmission in various applications such as e-commerce, cloud computing, and mobile computing.

However, there are still some areas that need to be explored in future research. One such area is the optimization of the key management process in hybrid encryption, to ensure that the keys are properly secured and distributed to the right entities. Another area of future work is the development of more efficient encryption algorithms that can provide better security and performance in hybrid encryption. Overall, the

hybrid encryption approach using AES and RSA is a promising technique for data encryption, with many potential applications in various domains. Further research and development in this area will help to improve the security and efficiency of the approach and make it more widely applicable in real-world scenarios.

References:

1. Bhandari, P. (2015). Hybrid encryption using AES and RSA: A review. International Journal of Engineering Research and General Science, 3(5), 150-154.
2. Roshan, S. S., & Sreekumar, M. G. (2014). Hybrid encryption technique using RSA and AES for secure data transmission. International Journal of Computer Applications, 90(11), 36-40.
3. Singh, S., & Jain, A. (2016). Hybrid encryption using AES and RSA algorithm. International Journal of Engineering and Computer Science, 5(5), 16654-16659.
4. Kaur, R., & Singh, K. (2017). Hybrid Encryption Using RSA and AES for Secure Data Transmission. International Journal of Computer Science and Mobile Computing, 6(5), 69-74.
5. "Cryptography and Network Security: Principles and Practice" by William Stallings: This book provides a comprehensive introduction to modern cryptography, including the AES encryption algorithm. It covers the basics of symmetric-key encryption, including block ciphers and stream ciphers, and includes detailed discussions of AES's design and implementation.
6. "Applied Cryptography" by Bruce Schneier: This book is a classic reference for cryptography, and includes a detailed discussion of AES. It covers the history of cryptography, the basics of symmetric-key encryption, and the design and implementation of AES.
7. "Understanding Cryptography: A Textbook for Students and Practitioners" by Christof Paar and Jan Pelzl: This book provides a modern and accessible introduction to cryptography, including the AES encryption algorithm. It covers the basics of symmetric-key encryption, including block ciphers and stream ciphers, and includes a detailed discussion of AES's design and implementation.
8. "Handbook of Applied Cryptography" by Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone: This is a comprehensive reference book for cryptography, including the AES encryption algorithm. It covers the basics of symmetric-key encryption, including block ciphers and stream ciphers, and includes a detailed discussion of AES's design and implementation.
9. "The Code Book" by Simon Singh: This book is a popular and engaging introduction to the history of cryptography, and includes a detailed discussion of RSA. It covers the basics of public-key cryptography, including key exchange and digital signatures, and includes a historical perspective on the development of the RSA algorithm.
10. Oracle Java Cryptography Architecture (JCA) Reference Guide: https://docs.oracle.com/en/java/javase/11/security/java-cryptography-architecture-jca-reference-guide.html
11. Java AES encryption and decryption tutorial: https://howtodoinjava.com/java/java-security/aes-256-encryption-decryption/
12. Java RSA encryption and decryption tutorial: https://howtodoinjava.com/java/java-security/java-rsa-encryption-decryption/
13. Java AES encryption using the Cipher class: https://docs.oracle.com/javase/7/docs/api/javax/crypto/Cipher.html
13. Java RSA encryption using the Cipher class: https://docs.oracle.com/javase/7/docs/api/javax/crypto/Cipher.html
14. Bouncy Castle Crypto APIs for Java: https://www.bouncycastle.org/java.html
15. Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files: https://www.oracle.com/java/technologies/javase-jce-all-downloads.html
16. “Cryptography and Cryptanalysis in Java - Creating and Programming Advanced Algorithms with Java SE 17 LTS and Jakarta EE 10” by Stefania Loredana Nita, Marius Iulian Mihailescu.