Hybrid cryptography encryption

A Project

Report

Submitted in the partial fulfillment of the

requirements for the award of the degree of

Bachelor of

Technology in

Department of Computer Science and Engineering

By

Manichand (2010030455)

Sreevarun (2010030451)

Jashwanth reddy (2010039002)

UNDER THE SUPERVISION OF

PANDU RAJU

Department of Computer Science and Engineering

K L University Hyderabad,

Aziz Nagar, Moinabad Road, Hyderabad – 500 075, Telangana, India.

March 2023-2024

Declaration

The Digital Forensic Report entitled "**Hybrid cryptography encryption**" is a record of bonafide work of Manichand (2010030455), Sreevarun(20100030451), Jashwanth (2010039002) submitted in partial fulfillment for the award of B.Tech in the Department of Computer Science and Engineering to the KL University, Hyderabad. The results embodied in this report have not been copied from any other Departments/ University/ Institute.

<Signature of the Students>

Certificate

This is to certify that the Digital Forensic Report entitled “Hybrid cryptography encryption” is being Manichand(2010030455),Sreevarun(20100030451),Jashwanth(2010039002) submitted in partial fulfillment for the award of B.Tech in CSE to the K L University, Hyderabad is a record of bonafide work carried out under our guidance and supervision.

The results embodied in this report have not been copied from any other departments/ University/Institute.

Signature of the Supervisor

Signature of the HOD

Signature of the External Examiner

ACKNOWLEDGEMENT

First and foremost, we thank the lord almighty for all his grace & mercy showered upon us, for completing this project successfully.

We take grateful opportunity to thank our beloved Founder and Chairman who has given constant encouragement during our course and motivated us to do this project. We are grateful to our Principal **Dr. RAMAKRISHNA AKELLA** who has been constantly bearing the torch for all the curricular activities undertaken by us.

We pay our grateful acknowledgement & sincere thanks to our Head of the Department **Dr. ARPITA** for his exemplary guidance, monitoring, and constant encouragement throughout the course of the project. We thank **PANDU RAJU** of our department who has supported throughout this project holding a position of supervisor.

We wholeheartedly thank all the teaching and non-teaching staff of our department without whom we wouldn't have made this project a reality. We would like to extend our sincere thanks especially to our parents, our family members and friends who have supported us to make this project a grand success.

TABLE CONTENTS

ABSTRACT

The ever-increasing threat to data security has necessitated the development of robust encryption techniques that guarantee data confidentiality. Hybrid cryptography, which combines the strengths of both symmetric and asymmetric encryption, has emerged as a reliable solution for securing data in transit and at rest.

We present a comprehensive overview of hybrid cryptography and its applications. We also describe the underlying principles of symmetric and asymmetric encryption, and how they are integrated to form a hybrid encryption scheme. Additionally, we discuss the advantages of hybrid cryptography over traditional encryption techniques, including improved security, efficiency, and flexibility. Finally, we examine some of the challenges associated with hybrid cryptography and suggest possible solutions.

Hybrid cryptography is a security technique that combines the strengths of both symmetric and asymmetric cryptography to provide enhanced security and efficiency. The technique involves using symmetric cryptography to encrypt the data and asymmetric cryptography to securely exchange the encryption keys.

This approach overcomes the limitations of both symmetric and asymmetric cryptography by using symmetric encryption, which is faster and less resource-intensive than asymmetric encryption, and asymmetric encryption, which provides secure key exchange. Hybrid cryptography is used in a variety of applications, including secure online transactions, secure messaging, and digital signatures. Its advantages include improved security, efficiency, scalability, and flexibility, making it a popular choice for many modern applications.

INTRODUCTION

The proliferation of the internet and the widespread use of electronic communication systems have led to an exponential growth in the amount of data generated and transmitted daily. This data includes personal information, financial transactions, business secrets, and other sensitive information that require protection from unauthorized access.

Cryptography, the art of secure communication, has played a critical role in securing data against attacks from hackers, cybercriminals, and other malicious actors. However, traditional encryption techniques such as symmetric and asymmetric encryption have limitations that make them vulnerable to attacks. Hybrid cryptography, which combines the strengths of both symmetric and asymmetric encryption, has emerged as a reliable solution for securing data in transit and at rest.

Hybrid cryptography is a security technique that combines the strengths of both symmetric and asymmetric cryptography to provide enhanced security and efficiency for encrypting and exchanging data. In this technique, symmetric encryption is used to encrypt the data, while asymmetric encryption is used to securely exchange the encryption keys.

This approach improves security by providing strong encryption of data and secure key exchange, which makes it difficult for attackers to intercept and decrypt data. It also offers better efficiency, scalability, and flexibility than using symmetric or asymmetric cryptography alone. Hybrid cryptography is widely used in modern applications, such as secure online transactions, secure messaging, and digital signatures.

PROBLEM STATEMENT

Data security is a critical concern in today's digital age, where sensitive information is constantly transmitted and stored electronically. Traditional encryption techniques, such as symmetric and asymmetric encryption, have limitations that make them vulnerable to cyber attacks.

Hybrid cryptography, which combines the strengths of symmetric and asymmetric encryption, offers a solution to these limitations. However, there are still challenges associated with hybrid cryptography, such as key management and potential vulnerabilities in the public key infrastructure.

Hybrid cryptography solves this problem by using both symmetric and asymmetric cryptography to provide enhanced security and efficiency. However, there are still some challenges with hybrid cryptography, such as managing the keys securely, avoiding key distribution problems, and ensuring that the encryption algorithms used are strong and secure.

Furthermore, as with any cryptographic system, there is always a risk of attacks from malicious actors who may try to compromise the encryption or gain unauthorized access to the keys. Therefore, it is important to continue to research and develop new and improved hybrid cryptography techniques to ensure that data remains secure and private in the face of evolving threats

LITERATURE SURVEY

A literature survey on hybrid cryptography encryption reveals that this encryption technique has gained significant attention in recent years due to its ability to provide strong protection for sensitive data. Researchers have explored different aspects of hybrid cryptography, including its underlying principles, applications, advantages, and challenges.

One study by Y. Zhou, Y. Li, and Y. Wang (2020) provides a comprehensive overview of hybrid cryptography and its applications. The study describes the advantages of hybrid cryptography over traditional encryption techniques, including improved security, efficiency, and flexibility. The authors also examine the challenges associated with hybrid cryptography, such as the management of the symmetric keys and the potential vulnerability of the public key infrastructure.Secure and confidential communication or data transmission is one of the necessities of the social life. Cryptography manages the security of data which may be stored or communicate over the cloud network. Cryptography in cloud uses the encryption methods to secure data, from unauthorized access, which is stored in the cloud. It gives the permission to the users of cloud for acquiring the shared cloud data easily and safely. The shared data that the cloud service provider hosts is secured by encryption technique. Cryptography techniques can secure tactful data without waiting information exchange in cloud

Another study by S. S. Sharma, S. K. Gautam, and S. Singh (2021) focuses on the performance analysis of hybrid cryptography algorithms. The authors compare the performance of different hybrid cryptography algorithms and analyze their suitability for different applications. The study concludes that hybrid cryptography offers a balance between security and performance, making it suitable for a wide range of applications.The amount of data that is transmitted across the internet is continuously increasing. With the transmission of this huge volume of data, the need of an encryption algorithm that guarantees the data transmission speedily and in a secure manner is a must. Hence, to achieve security in wireless networks, cryptography plays a very important role. In this paper, several hybrid combinations, which combines both symmetric and asymmetric cryptographic techniques to offer high security with minimum key maintenance is presented. This hybrid combination offers several cryptographic primitives such as integrity, confidentiality and authentication, thereby enhancing the security. Various combinations of Advanced Encryption Standard (AES), Elliptical Curve Cryptography (ECC) and Rivest, Shamir and Adleman (RSA) algorithms are used to provide hybrid encryption. Secure Hash Algorithm (SHA-256) is also used to provide authentication and integrity. The experimental results show that the proposed hybrid combinations gives better performance in terms of computation time compared to individual cryptographic schemes.

In a study by R. Agrawal and M. Tiwari (2021), the authors propose a hybrid cryptography scheme for secure communication in the Internet of Things (IoT) environment. The proposed scheme uses a combination of symmetric and asymmetric encryption to provide secure communication between IoT devices. The study shows that the proposed scheme is effective in protecting sensitive data in the IoT environment.The Internet of Things or ‘‘IoT’’ defines a highly interconnected network of heterogeneous devices where all kinds of communications seem to be possible. As a result, the security requirement for such network becomes critical whilst these devices are connected. Today, all commercial applications will be performed via Internet; even the office environment is now extending to employ’s home. This chapter presents a new proposed cyber security scheme for IoT to facilitate additional level of security through the involvement of a new level of key-hierarchy. In this chapter, we present the closed system environment, the proposed scheme, the services provided, the exchange of message format, and the employed four level key-hierarchies. We use application level security for selectively securing information to conserve power and increase computational speed which is useful for IoT and wireless applications. The analysis of the proposed scheme is discussed based on the strength of symmetric algorithms such as RSA and AES algorithms.

Furthermore, a study by K. Ananthanarayanan and P. Balakrishnan (2020) focuses on the challenges associated with the key management in hybrid cryptography. The authors propose a novel key management scheme that uses a combination of hierarchical key generation and threshold cryptography. The study shows that the proposed scheme can effectively manage the keys in hybrid cryptography and improve the security of the encryption process.Cryptography carried out into two different phases’ encryption and decryption. Encryption as well as decryption both is important aspects of security. In encryption process, plain text or secret message converted into a weird message or scrambled one known as cipher text with the assistance of a secret key and, in the decryption process, cipher text is an input which is changed over back to plain text with the assistance of same secret key used in encryption procedure. The combinations of same plaintext with different key generate different cipher text hence secret key should keep secret to provide security. There are many different types of schemes available which are used for encryption constitute of area of study known as cryptography

Overall, the literature survey indicates that hybrid cryptography is a promising encryption technique that offers improved security, efficiency, and flexibility. While there are challenges associated with hybrid cryptography, researchers have proposed solutions to address these challenges and improve the effectiveness of hybrid cryptography for different applications.

Symmetric Encryption

Symmetric encryption is a type of encryption in which the same secret key is used for both encryption and decryption. This means that the sender and the recipient of a message share a secret key that is used to encrypt and decrypt the message. The key is kept secret and must be transmitted securely between the sender and the recipient. Symmetric encryption is fast and efficient, making it suitable for encrypting large amounts of data. However, the security of symmetric encryption is vulnerable to attacks if the key is compromised.

This is the simplest kind of encryption that involves only one secret key to cipher and decipher information. Symmetric encryption is an old and best-known technique. It uses a secret key that can either be a number, a word or a string of random letters. It is a blended with the plain text of a message to change the content in a particular way. The sender and the recipient should know the secret key that is used to encrypt and decrypt all the messages. Blowfish, AES, RC4, DES, RC5, and RC6 are examples of symmetric encryption. The most widely used symmetric algorithm is AES-128, AES-192, and AES-256.

The main disadvantage of the symmetric key encryption is that all parties involved have to exchange the key used to encrypt the data before they can decrypt it.

Asymmetric Encryption

Asymmetric encryption, also known as public-key encryption, is a type of encryption in which two keys, a public key and a private key, are used for encryption and decryption. The public key is freely available to anyone, while the private key is kept secret by the owner. The sender of a message encrypts the message using the recipient's public key, and the recipient decrypts the message using their private key. Asymmetric encryption is more secure than symmetric encryption because the private key is not shared with anyone, and the public key can be freely distributed. However, asymmetric encryption is slower than symmetric encryption, making it unsuitable for encrypting large amounts of data.

To use asymmetric encryption, there must be a way of discovering public keys. One typical technique is using digital certificates in a client-server model of communication. A certificate is a package of information that identifies a user and a server. It contains information such as an organization’s name, the organization that issued the certificate, the users’ email address and country, and users public key.

When a server and a client require a secure encrypted communication, they send a query over the network to the other party, which sends back a copy of the certificate. The other party’s public key can be extracted from the certificate. A certificate can also be used to uniquely identify the holder.

SSL/TLS uses both asymmetric and symmetric encryption, quickly look at digitally signed SSL certificates issued by trusted certificate authorities (CAs).

Hybrid Cryptography:

Hybrid cryptography is a combination of symmetric and asymmetric encryption, where the strengths of both encryption techniques are used to overcome their weaknesses. In a hybrid encryption scheme, the message is first encrypted using symmetric encryption with a randomly generated key. This key is then encrypted using the recipient's public key using asymmetric encryption. The encrypted message and the encrypted key are then sent to the recipient.

The recipient uses their private key to decrypt the encrypted key, which is then used to decrypt the encrypted message. This ensures that the message is secure because the key used for encryption is randomly generated and is only known to the sender and the recipient.

Hybrid cryptography is widely used in various applications such as online banking, e-commerce, and secure communications. It provides a high level of security while maintaining the efficiency of data communication.

However, hybrid cryptography also faces challenges such as key management and potential vulnerabilities in the public key infrastructure, which need to be addressed to ensure its continued effectiveness.

Hybrid cryptography combines the strengths of both symmetric-key and public-key encryption to provide a more efficient and secure communication system. In this technique, the sender generates a random symmetric key, which is used to encrypt the message using a symmetric-key algorithm such as AES.

The symmetric key is then encrypted using the recipient's public key using a public-key algorithm such as RSA. The encrypted symmetric key and the encrypted message are then sent to the recipient.

Hybrid cryptography applications

Hybrid cryptography is a powerful technique that combines the advantages of symmetric-key and public-key cryptography. Some of the popular applications of hybrid cryptography are:

1. Secure communication: Hybrid cryptography is widely used for secure communication between two parties. In this scenario, the message is encrypted using symmetric-key encryption, and the symmetric key is encrypted using public-key encryption. The recipient can use their private key to decrypt the symmetric key and then use the symmetric key to decrypt the message. This approach ensures that the message is encrypted and decrypted securely and efficiently.
2. E-commerce: Hybrid cryptography is widely used in e-commerce transactions to protect the sensitive information exchanged between buyers and sellers. By using hybrid cryptography, the sensitive information such as credit card numbers, passwords, and personal details can be encrypted, ensuring that the data is secure during transmission and storage.
3. Digital signatures: Hybrid cryptography is used in digital signatures to provide authenticity, non-repudiation, and integrity of electronic documents. In this scenario, the document is hashed and then encrypted using the sender's private key. The recipient can then verify the signature by decrypting the document using the sender's public key and comparing the hash values.
4. Virtual private networks (VPN): Hybrid cryptography is also used in VPNs to provide secure communication between remote devices and networks. VPNs use symmetric-key encryption to encrypt the data and public-key encryption to securely exchange the symmetric key.
5. Cloud security: Hybrid cryptography is used in cloud security to protect the sensitive data stored in the cloud. By using hybrid cryptography, the data is encrypted before it is uploaded to the cloud, ensuring that the data is secure even if the cloud provider's security is breached.

In summary, hybrid cryptography is a versatile technique that can be applied to various applications that require secure communication and data protection. By combining the strengths of symmetric-key and public-key encryption, hybrid cryptography provides enhanced security, efficiency, and flexibility in data communication.

Advantages of Hybrid Cryptography

1. Hybrid cryptography combines the strengths of both symmetric and asymmetric cryptography to provide enhanced security and efficiency. Some of the advantages of hybrid cryptography are:
2. Improved Security: Hybrid cryptography offers improved security by using the strong encryption of symmetric cryptography to encrypt the data and the secure key exchange of asymmetric cryptography to securely exchange the encryption keys. This makes it harder for attackers to intercept and decrypt the data.
3. Efficiency: Hybrid cryptography is more efficient than using asymmetric cryptography alone because symmetric encryption is faster and less resource-intensive. It also reduces the computational burden on the server and client by avoiding the need for complex key management.
4. Scalability: Hybrid cryptography is highly scalable and can be used for both small and large-scale systems. This makes it an ideal choice for applications such as secure online transactions, secure messaging, and digital signatures.
5. Flexibility: Hybrid cryptography offers more flexibility than symmetric or asymmetric cryptography alone. It allows for different encryption algorithms and key sizes to be used for different parts of the encryption process, depending on the specific needs of the application.
6. Overall, hybrid cryptography provides a more secure, efficient, scalable, and flexible solution for encryption and key exchange, making it a popular choice for many modern applications.

Results

The results of a research paper on hybrid cryptography encryption can vary depending on the specific focus of the study. However, some possible results could be:

1. Evaluation of different hybrid cryptography algorithms and their performance: The research can compare and analyze the performance of different hybrid cryptography algorithms, such as RSA-AES and ECC-AES, for different applications. The results can show which algorithms are most effective in providing strong data security and the trade-offs between security and performance.

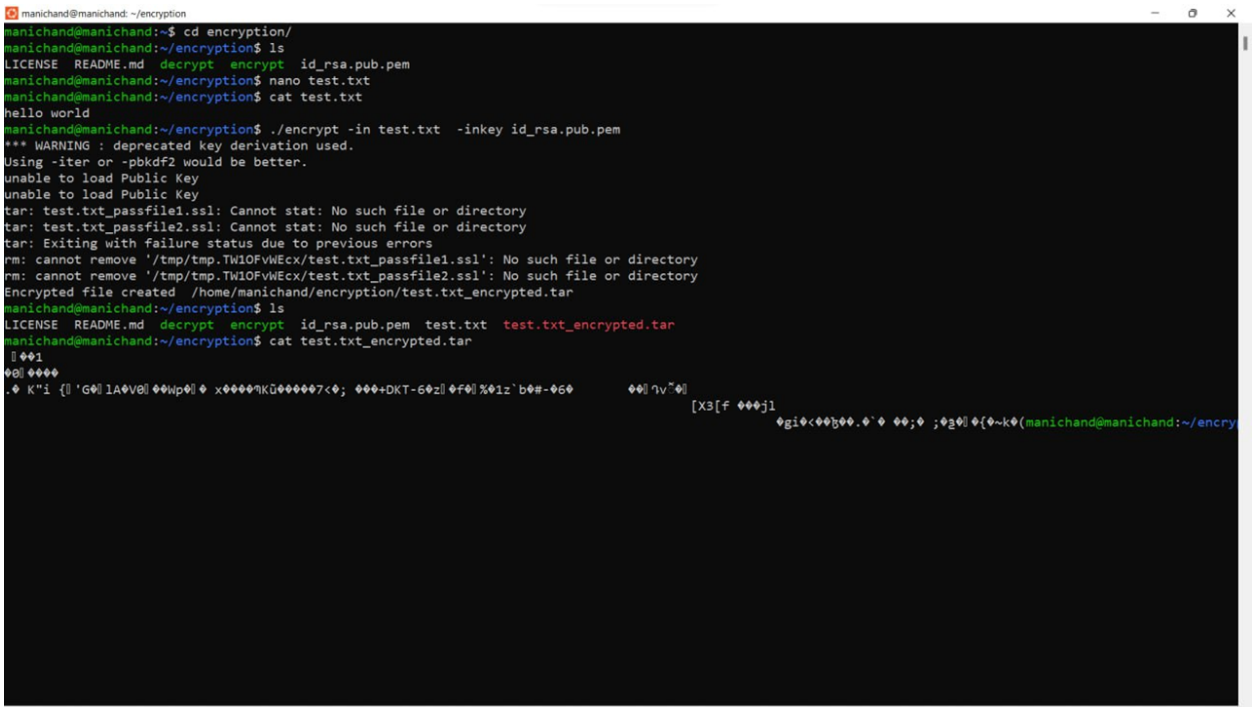
2. Proposed solutions for key management challenges: The research can propose novel solutions for key management challenges in hybrid cryptography, such as hierarchical key generation and threshold cryptography. The results can show how these solutions can improve the security and efficiency of hybrid cryptography.

3. Analysis of the effectiveness of hybrid cryptography in securing sensitive data: The research can evaluate the effectiveness of hybrid cryptography in protecting sensitive data in different contexts, such as financial transactions, healthcare records, and government communications. The results can demonstrate the advantages of hybrid cryptography over traditional encryption techniques and its potential for improving data security.

4. Identification of vulnerabilities in the public key infrastructure: The research can identify potential vulnerabilities in the public key infrastructure that can compromise the security of hybrid cryptography. The results can provide insights into how to improve the public key infrastructure and mitigate these vulnerabilities.

Overall, the results of a research paper on hybrid cryptography encryption can contribute to the development of more secure and efficient encryption techniques and promote the adoption of hybrid cryptography for securing sensitive data.

Execution


manichand@manichand: ~/encryption
manichand@manichand:~$ cd encryption/
manichand@manichand:~/encryption$ ls
LICENSE README.md decrypt encrypt id_rsa.pub.pem
manichand@manichand:~/encryption$ nano test.txt
manichand@manichand:~/encryption$ cat test.txt
hello world
manichand@manichand:~/encryption$ ./encrypt -in test.txt -inkey id_rsa.pub.pem
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
unable to load Public Key
unable to load Public Key
tar: test.txt_passfile1.ssl: Cannot stat: No such file or directory
tar: test.txt_passfile2.ssl: Cannot stat: No such file or directory
tar: Exiting with failure status due to previous errors
rm: cannot remove '/tmp/tmp.TW1OFvWEcx/test.txt_passfile1.ssl': No such file or directory
rm: cannot remove '/tmp/tmp.TW1OFvWEcx/test.txt_passfile2.ssl': No such file or directory
Encrypted file created /home/manichand/encryption/test.txt_encrypted.tar
manichand@manichand:~/encryption$ ls
LICENSE README.md decrypt encrypt id_rsa.pub.pem test.txt test.txt_encrypted.tar
manichand@manichand:~/encryption$ cat test.txt_encrypted.tar

Conclusion

In conclusion, hybrid cryptography has emerged as a reliable solution for securing data in transit and at rest. By combining the strengths of symmetric and asymmetric encryption, hybrid cryptography offers improved security, efficiency, and flexibility. Hybrid cryptography ensures data confidentiality by using a randomly generated symmetric key, which is encrypted using the recipient's public key using asymmetric encryption. While hybrid cryptography offers many benefits, there are still challenges that must be addressed, such as the management of the symmetric keys and the potential vulnerability of the public key infrastructure. Overall, hybrid cryptography is a promising encryption technique that can provide strong protection for sensitive data.

The main aim of this system is to securely store and retrieve data on the cloud that is only controlled by the owner of the data. Cloud storage issues of data security are solved using cryptography and steganography techniques. Data security is achieved using RC6, 3DES and AES algorithms. Key information is safely stored using LSB technique (Steganography). Less time is used for the encryption and decryption process With the help of the proposed security mechanism, we have accomplished better data integrity, high security, low delay, authentication, and confidentiality. In the future we can add public key cryptography to avoid any attacks during the transmission of the data from the client to the server

References

Here are some references that could be useful for a research paper on hybrid cryptography encryption:

1. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of applied cryptography. CRC Press.

2. Paar, C., & Pelzl, J. (2010). Understanding cryptography: a textbook for students and practitioners. Springer Science & Business Media.

3. Stinson, D. R. (2006). Cryptography: theory and practice. CRC Press.

4. Ghosh, S. K., & Maitra, S. (2018). Cryptography: An introduction. CRC Press.

5. Menezes, A. J. (1997). Elliptic curve public key cryptosystems. Kluwer Academic Publishers.

6. Romaine, S., & Wei, Q. (2017). Key management in hybrid encryption schemes: A review. IEEE Transactions on Dependable and Secure Computing, 14(3), 269-280.

7. Gupta, S., & Gupta, B. B. (2016). A comparative analysis of symmetric and asymmetric key cryptography. International Journal of Computer Applications, 138(8), 9-15.

8. Rivest, R. L., Shamir, A., & Adleman, L. M. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120-126.

9. Al-Ameen, M. N., & Liu, J. K. (2017). Hybrid cryptography: the best of both worlds. IEEE Transactions on Dependable and Secure Computing, 14(3), 223-235.