INDIAN INSTITUTE OF INFORMATION TECHNOLOGY

Security Engineering

Advanced Secure Messaging System: A Unified Approach Using AES and RSA

B.Jagadish (20bcs032)

Context:

- Introduction
- Related Work
- Datasets
- Methodology
- Experiments
- Results and Discussion
- Conclusion
- Acknowledgments
- References

Introduction

The security of communications is critical in the digital era. The requirement for reliable and secure communications solutions is growing as cyber threats change. The goal of this project is to create a secure messaging system that uses Rivest-Shamir-Adleman (RSA) for key exchange and Advanced Encryption Standard (AES) for encryption. The purpose of this system is to safeguard secret messages from tampering and unauthorized access by guaranteeing confidentiality, integrity, and authenticity.

Related Work

Previous work in the field of secure communications has explored various cryptographic techniques. AES is widely recognized for its efficiency and security in encrypting data. RSA is commonly used for secure key exchange due to its robustness against cryptographic attacks. Combining AES and RSA provides a balanced approach, leveraging the strengths of both symmetric and asymmetric encryption. Studies have demonstrated the effectiveness of digital signatures in verifying the authenticity and integrity of messages, adding an additional layer of security.

Datasets

This project will concentrate on the implementation and testing of the encryption and decryption methods rather than using conventional datasets. We'll build sample messages to mimic conversations that happen in real life. To fully test the capabilities of the system, the length and substance of these messages will vary.

Methodology

The following stages will be followed in the project's execution:
1. **AES Encryption and Decryption:** To guarantee message privacy, AES is implemented with PKCS7 padding.
2.**RSA Key Exchange:** RSA encryption will be used to create a safe method of transferring AES keys.
3.**Digital Signatures:** To confirm message integrity and authenticate the sender, use RSA-based digital signatures.
4.**Signature Verification:** Making sure the receiver may use the sender's public RSA key to confirm the message's integrity and validity.

Python and the `cryptography` library will be used in the development of the system to manage the cryptographic activities.

Experiments

Testing the encryption, decryption, key exchange, and signature verification procedures under various scenarios will be the focus of the experiments:

1. **Encryption/Decryption:** To guarantee consistency and security, encrypt and decode communications with varying lengths and contents.
2. **Key Exchange:** Verify the safe transfer of AES keys by running an RSA key exchange test.
3. **Digital Signatures:** Examine the precision and dependability of digital signatures in confirming the integrity and validity of messages.
4. **Performance Evaluation:** Calculate the system's efficiency, taking into account the time it takes to encrypt and decode data as well as the computational burden associated with key exchange and signature verification.

Results and Discussion

The anticipated outcomes will show how the system can safely exchange keys, encrypt and decode communications, and validate digital signatures. Performance metrics and security validation findings will be included in the results. There will be a discussion of any potential drawbacks or difficulties found throughout the testing and implementation stages, as well as suggested fixes or enhancements.

Conclusion

The expected results will demonstrate how the system can check digital signatures, encrypt and decode messages, and exchange keys reliably. The results will contain security validation findings and performance indicators. Any possible flaws or issues discovered throughout the testing and implementation phases will be discussed, along with any recommended improvements or remedies.

Acknowledgments

We would like to thank the open-source community for providing the tools and libraries that made this project possible. Special thanks to the authors and contributors of the `cryptography` library for their invaluable resources.

References

1. Shamir, A., Adleman, L., and Rivest, R. L. (1978). a technique for getting public-key cryptosystems and digital signatures. ACM Communications, 21(2), 120–126.
2. In 1999, Daemen, J., and Rijmen, V. The Rijndael AES proposal. NIST's proposal for AES.
3.Ferguson, N., Kohno, T., and Schneier, B. (2010). Design Principles and Real-World Applications of Cryptography Engineering. Wiley.
Dworkin (2001) p.
4. Methods and Techniques for Suggested Block Cipher Modes of Operation. 800-38A, NIST Special Publication.
5. 2001 saw the National Institute of Standards and Technology. Advanced Encryption Standard (AES), FIPS PUB 197.
6. Technology and Standards Institute (NIST) (2002). Digital Signature Standard (DSS), 32 FIPS PUB 186-2.