Implementation of security mechanisms using AES and RSA Hybrid Algorithm with Digital Signatures

Team Details
1. Shaista Firdous(20eg105442)
2. M.Sathvika(20eg105428)
3. K.Shiva Sai(19H61A05L6)

Project Supervisor
Dr.K.Madhuri
Associate Professor

Introduction

- It is a secured hybrid algorithm used to protect the safe transmission of data in the Network communication using AES and RSA algorithm. To secure the text as well as key.
- There are different parameters that are needed, those are AES Encryption/Decryption, RSA Encryption/Decryption, Hybrid Encryption, Secure Key Management, Random Number Generation, Secure E-mail transmission, Digital Signatures.

APPLICATIONS:

- **Secure Email Communication:** Implementing AES for symmetric encryption and RSA for asymmetric encryption can ensure that messages are securely transmitted and only accessible to authorized recipients. This is crucial for protecting sensitive information in message exchanges, such as personal data, financial information, or confidential business communications.
- **Digital Signatures:** RSA can be used for digital signatures, which verify the authenticity and integrity of messages. A sender can sign their message with their private key, and the recipient can verify the signature.

Literature

Author(s)	Method	Advantages	Disadvantages
Ye Liu	**File and Disk encryption:** AES is used to encrypt files and folders on computers.	• **Confidentiality** • **Efficiency** • **Security:** AES provides security and resistant to brute-force attacks.	As AES symmetric algorithm, there are high chances of leakage of data.
Wei Gong	**RSA algorithm:** Asymmetric encryption algorithm.	• **Security:** RSA algorithm is a very secure method of encrypting and decrypting sensitive information. • **Key Exchange:** RSA algorithm can be used to safely transmit the key.	• Computational Intensity • Key Management • Performance Impact
Wenqing Fan	**AES algorithm:** Symmetric encryption algorithm using Java language.	• Platform Independent • Security • Readability and Maintainability. • Community support.	• Hard to implement with software. • Every block is always encrypted in the same way.

Problem Statement

- To protect the safe transmission of data in the Network communication using AES and RSA algorithm. To secure the text as well as key.
- **Existed Method:** Implementation of E-mail security using AES and RSA Algorithm.
- **Proposed Method:** Implementation of security mechanisms using AES and RSA algorithm and Digital Signature is used to authenticate the user.

Objective

- To solve the problem we are using AES and RSA Hybrid algorithm.
- For User Authentication we are using Digital Signatures.
- The parameters that are needed in this project are public key, private key, AES encryption/decryption, RSA encryption/decryption, message, Cipher text, Cipher key, Digital Signature.

PROPOSED METHOD

AES Algorithm

1.Let us consider the input length of 128 bits(16 bytes)and divide the input as 4x4 matrix, where each block is of 8bits.

2.We are using key of length 128bits, so here AES uses 10rounds.

3.At each round it performs four sub-processes:

1.SubBytes

2.ShiftRows

3.MixColumns

4.AddRoundKey

4.Finally, we will get our cipher text.

RSA Algorithm

1.Let us select p, q , where p and q are largest prime numbers.

2.Calculate n=pxq

3.Calculate o(n)=(p-1)(q-1)

4.Select integer e ,where gcd(o(n),e)=1, whereas 1<e<o(n)

5.Calculate d ,where d=1/e(modo(n))

6.Public key={e, n}

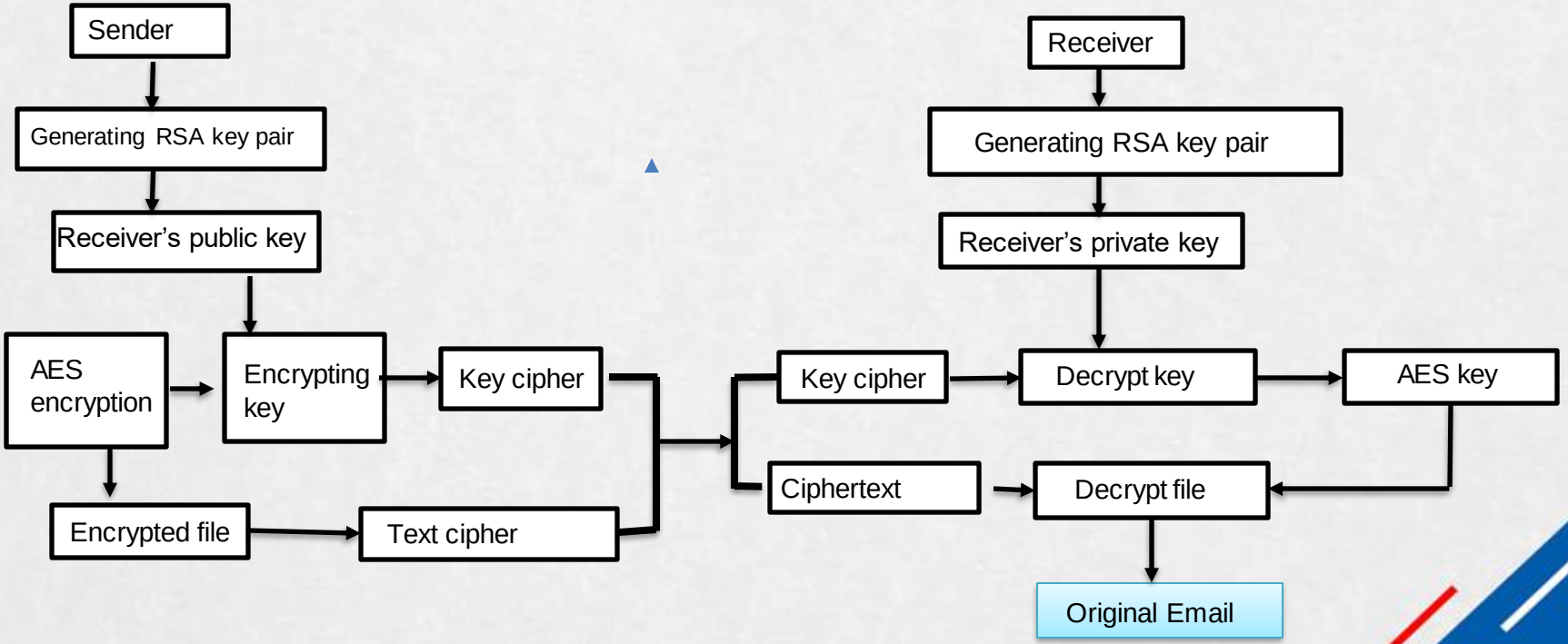
7.Private key={d, n}

Proposed Method

- Our proposed idea is we are using AES algorithm to encrypt the message using a key k, and we are using RSA algorithm to encrypt the key k using receiver's public key PU, that cipher key is considered as "ck".
- The encrypted key and message are transferred to the receiver, then the receiver uses his private key to decrypt the "ck" then we get k, using k he will decrypt the cipher text.
- Using above Hybrid algorithm we will ensure the confidentiality of the message, but in the next step we will check whether the sender is authorized or not.
- For that we are using Digital Signature to authenticate the user, we are using RSA approach to encrypt the Digital Signature.
- Using cryptographic hash function we generate a fixed-size hash value, which is a digital signature and using sender's private key we encrypt that key and send that to the receiver.
- Then, receiver will decrypt the digital signature using the sender's public key, the using the same hash function the receiver will generate a hash value and compare it with the sender's digital signature.

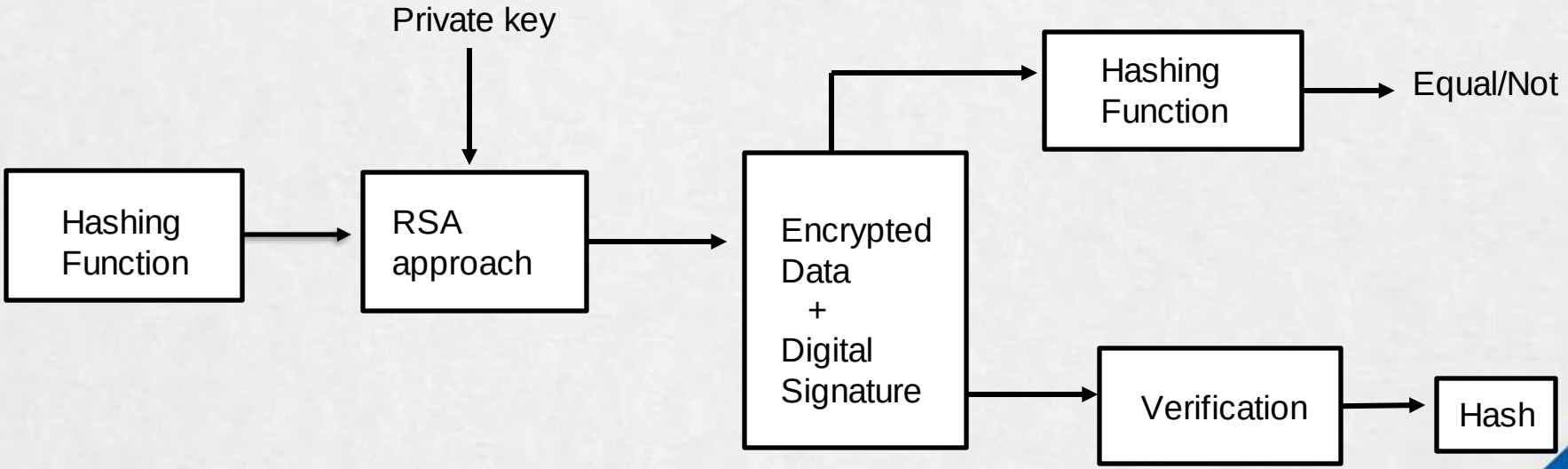
Proposed Method

Hybrid Algorithm flowchart for implementing E-mail system



Proposed Method

RSA approach to encrypt the Digital Signature



Project status

S.No	Functionality	Status (Completed /in-progress/Not started)
01	Abstract and Algorithm building	Completed
02	AES and RSA encryption of message and key	In progress
03	RSA approach in encryption of Digital Signature	Not started
04	Decryption of message, key and Digital Signature	Not started

Note: Submit Form 1,2 and 3

References

1. Leng Fei, Xu Jinhua, Yan Shixi. Network information security method based on RSA fusion AES algorithm [J]. Journal of Hua Qiao University. 2017.01. Vol.38, No.1.
2. Sun Quan. Analysis of Security Strength and Development Trend of Encryption Algorithm[J]. Software Industry and Engineering, 2016(3):29-32.
3. Xu Chang. Application of AES and RSA mixed encryption technology in network data transmission [J].2016.07.No.13.
4. Wang Fengzhong, Lu Yafei, Zou Raobangyan. Research on encryption and AES algorithm of military logistics database[J].2016.09. Vol.35, No.9
5. Gu Lize, Yang Yixian. Modern Cryptography Course [M]. Beijing: Beijing University of Posts and Telecommunications Press. 2009.08
6. Li Wei. Talk about common three encryption algorithms[J].Computer and Network.2017.06.12:52-54
7. Guo Yannan, Jiang Xueqin. Research and Implementation of RSA Information Security Encryption System[J].Net Security Technology and Application.2018.01.
8. Gao Yiwen. The Realization of RSA Algorithm and Its Application in Electronic Commerce[J].Journal of Chongqing University of Arts and Sciences.2009.08.No.4.

THANK YOU