1. System
2. RSA
3. Disadvantage
4. Proposed method
5. Results
6. Conclusion
7. Reference

A study of RSA

1.System

Symmetric key encryption uses the same key for encryption and decryption such as AES.

Asymmetric key encryption uses a public key for encryption and a private key for decryption such as RSA.

2.RSA

RSA algorithm is a generally known public-key cryptosystem.

3.Disadvantage

However, in the basic RSA, encrypting the same message with an identical public-key pair gives the same ciphertext.

Moreover, due to computing big prime number, RSA is slower than the standards symmetric key encryption.

4.Proposed method

M (aft Huffman) H and B (aft AES) H, B’ and K\_aes

(aft padding) R = H + K\_aes + pad, and B’ (aft RSA) R’, K\_rsa, and B’.

In the paper, we combine RSA with Huffman code, AES, and padding.

To reduce the redundancy in message (M), we use Huffman code. After applying Huffman code, the output is a header file (H) and a binary file (B).

Generally speaking, the size of the binary file is larger than the header file. To enhance its performance, we apply AES for encrypting the binary file. To improve the security, RSA for the header file, the key of AES, and padding.

5.Results

6.Conclusion

7.Reference