International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Security and Complexity Analysis of Synchronous and Asynchronous Security

Upadrista Mahesh

Student, Rajam, Vizianagaram, 535127, India.

ABSTRACT

Technical apps, software, and government agencies all place a high priority on cyber security. The procedures of data encrypting and decrypting are crucial for safe and secure communications in cyber security. The act of converting unencrypted data into something that seems random and meaningless is known as encryption (ciphertext). The process of decryption involves converting ciphertext to plaintext. Both sensitive and non-sensitive data types must be encrypted. The usage of this encryption method is widespread, including in WhatsApp communication. We use RSA (Rivest Shamir Adleman), an asymmetric algorithm, and AES, a symmetric technique, for data encryption (Advanced Encryption Standard). The most effective and established public key cryptosystem is RSA (method of protecting information). One key is used for encryption, and the second key is used for decryption. A private key is one that is kept private, whereas a public key is one that is made public. The AES algorithm, which employs a single Secret key for encryption and decryption, is the best and quickest method available. In RSA, the message is encrypted using a public key, and in contrast to AES, which uses a single key for both encryption and decryption, the message can only be unlocked using the private key.

Keywords: Cyber Security, Encryption, Decryption, RSA, AES, private key, public key.

1.Introduction

Cryptography's primary goal is to protect data and information from cyber-crimes. Because it offers many security properties, cryptography is still in use today. Here are a few of cryptography's objectives.

I. Authentication is a procedure to establish identification. Here, we check the message's security. Peer entity authentication and Data origin authentication are the two forms of authentication.

II. Privacy: Privacy is the defense against unapproved information disclosure. It might be used for the entire message. The protection of transmitted data against stale assaults is provided by privacy.

III. Integrity: It reassures the recipient that the original message they have received has not been modified in any way.

IV. Nonrepudiation: Neither the sender nor the recipient may dispute an electronic message. The recipient of a communication can confirm that the message was indeed sent by the sender.

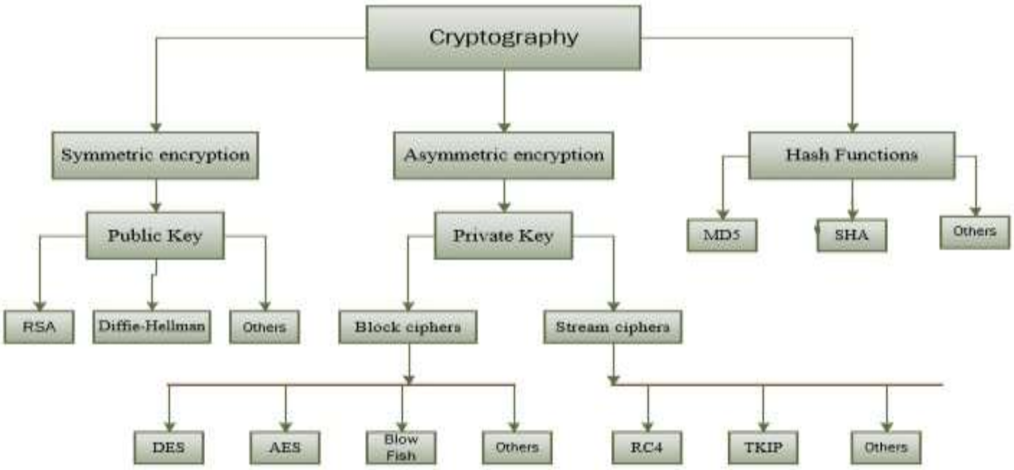


Fig-: Types of Ciphers

2. Literature Survey

In paper [1]. Data security is the process of protecting data from all forms of unauthorized access and data corruption throughout its entire life. The data security is deteriorating due to technology's constant advancement**.** Hackers occasionally attempt to access someone's data. As a result, consumers are most concerned about the security of their data. Data security can be done through hardware or software methods. Hardware methods of data protection are now receiving greater attention. This is because using hardware makes data protection more dependable, adaptable, and simple. Additionally, the hardware solution has less latency and increases the effectiveness of data protection. There are two different sorts of security algorithms that shield the data from any unauthorized access. Data Encryption Standard (DES) and Advanced Encryption Standard are covered under the first one, which is symmetric security methods (AES). The Elliptic Curve Cryptosystem and Rivest- Shamir-Adleman (RSA) are covered in the second category, Asymmetric Security Algorithms (ECC)

In paper [2]. To protect the confidentiality, authenticity, and integrity of data sent through networks, cryptography is necessary. Over the years, the RSA technique has been applied in several applications to increase the security of information through encryption and decryption. However, improvements in hacking and computer technology have made the original RSA algorithm assault less secure in terms of data protection. In light of this, several scholars have focused on the strategy of enhancing the RSA algorithm by introducing more complexity. The RSA public key cryptographic algorithm, also known as the RSA (Rivest, Shamir, Adleman) cryptosystem, is one of the most well-known and widely used cryptographic algorithms. It is named after its three creators, Ron Rivest, Adi Shamir, and Leonard Adleman, who released the RSA white paper for the first time in 1977. Key exchanges, digital signatures, online browsers, chat programs, emails, VPNs, and other forms of communication requiring data transmission between two parties all use the most modern applications of standard RSA.

In paper [3]. Due to its low cost and low power consumption, the Advanced Encryption Standard (AES) algorithm has evolved to be the standard option for many security services in a wide range of varied applications. Bit permutation is used to modify AES, which produces improved efficiency and reduced CPU utilization. The dispersion and confusion features of AES have been enhanced using modulo arithmetic in the cypher round. The avalanche effect has been improved over the original AES algorithm employing the original S-Box by the updated AES algorithm. The avalanche effect is employed to gauge how strong certain cryptographic methods are. This study demonstrated the avalanche effect's suitability for classic algorithms like AES and DES. Avalanche effect is a crucial metric for evaluating an algorithm's level of security.

In paper [4]. A symmetric block cypher algorithm is AES. Each of AES's three blocks is 128, 192, or 256 bits in size [18, 19]. AES encrypts and decrypts data using keys of various lengths. AES-128, for instance, employs a key that is 128 bits long. AES requires a varying number of rounds during encryption due to the different key lengths. AES key sizes of 128 bits, 192 bits, and 256 bits will result in 10, 12, and 14 rounds, respectively. AES uses extremely little hardware and is quite effective.

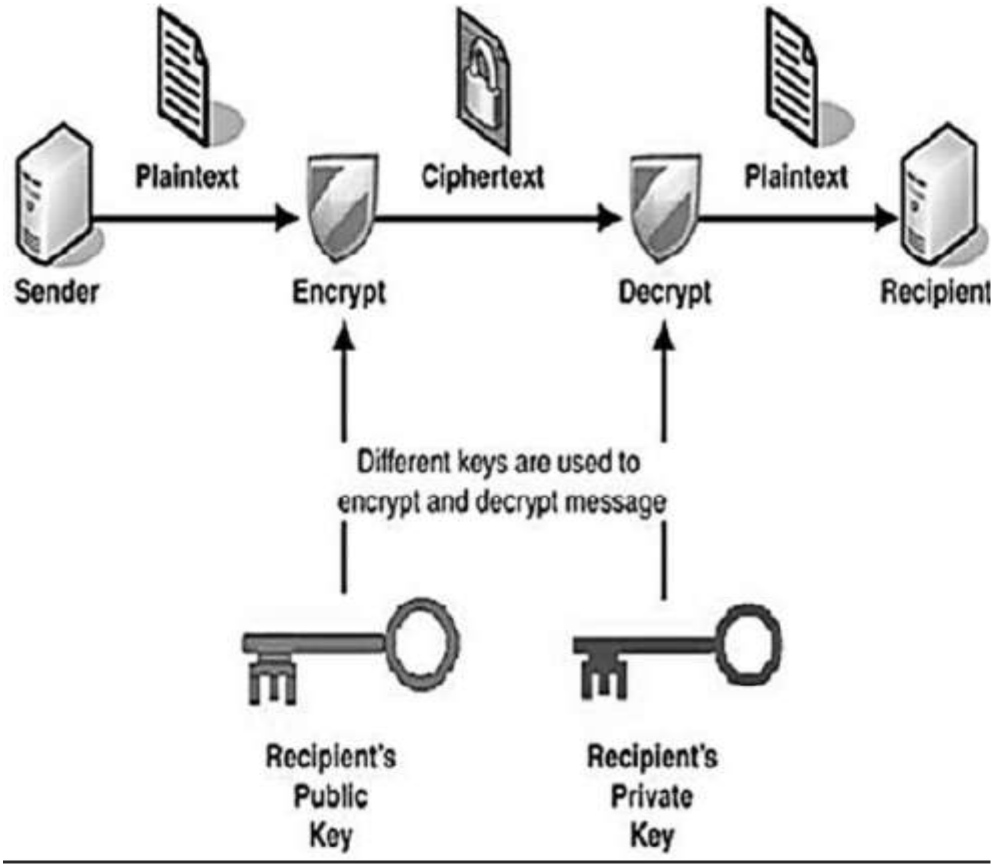
In paper [5]. Safeguarding the tract entailed securing the data in conventional communication networks. Securing the tract is no longer probabilistic or efficient with the advent of packet switching methods and the introduction of networks. This makes cryptography more ponderable. In order to keep information safe, written or produced codes must be created using cryptography.

Public-key cryptography includes the RSA encryption technique, which is regarded as one of its greatest achievements. It works well for encryption and decryption. Users using symmetric key encryption encrypt and decrypt data or information using the same key. Faster than asymmetric key cryptography is symmetric key cryptography.

3.Methodology

Encryption and decryption using RSA

A well-liked public-key encryption method is RSA. The RSA algorithm is regarded as being among the most reliable and secure asymmetric algorithms available to date. There are several key lengths for the RSA algorithm. The speed of RSA is dependent on security. RSA uses keys with various lengths that range from 512 to 2048 bits. Over the years, RSA has been regarded as the most dependable and secure algorithm among others, according to various cryptanalysis.



Comparison of hybrid encryption times for AES+RSA and TWOFISH+RSA in nanoseconds the asymmetric algorithm is another name for the public key encryption technique. Asymmetric algorithms are ones in which the encryption and decryption keys used by the sender and the receiver are distinct. A set of keys is given to each sender:

Private key and public key

Encryption is performed using the **public key**, while decryption is performed using the **private key**. A public key cannot be used for decryption. Although the two keys are connected, it is impossible to extract the private key from the public key. While the private key is kept private and only known by the key's owner, the public key is widely known. It implies that anybody can send the user a message using the user's public key. However, the communication can only be decrypted by the user using his private key.

Working On Algorithm

Find n = p x q by multiplying two big prime integers, p and q, where n is referred to as the modulus for encryption and decoding.

A number e smaller than n should be chosen so that n is close to (p - 1) x's prime number (q -1). This indicates that the only factor that e and (p - 1) x (q -) share is 1. Select "e" so that 1e (n), e is prime to (n), and gcd (e, d(n)) = 1.

If n = p x q, then e, n is the public key. Public key e, n> is used to encrypt a plaintext message m. The following formula is used to obtain ciphertext C from plain text: C=memod n in this case, m must be lower than n. Each message in a bigger message (>n) is handled as a distinct communication and is encrypted independently.

We compute the d according to the method below to get the private key: Demod{(p-1) x(q-1)} =1 Or De mod = 1 mod (n) d, n is the private key. The private key d, n> is used to decipher the ciphertext message c. The following formula is used to compute plain text m from the ciphertext c. M = CD Modulus N.

7. Results and Discussion

Additionally, memory use was evaluated amongst proposed techniques (in bytes). A comparison revealed that the hybrid architecture of Twofish and RSA uses less memory than AES and RSA. Following comparison, the described algorithms can be arranged as follows: Twofish+RSA and AES+RSA, in increasing order.

Plainte xt Size (KB)	**AES+RSA Encryption time (Nanoseconds)**	**Twofish+RSA Encryption time (Nanoseconds)**
32	372459622	4544528
64	477603055	8938837
128	501921935	15617401
256	529911193	30601856
512	570362262	49784215

8. Conclusion

Comparative assessments of the AES, RSA, and Twofish cryptosystems are presented in the study. New hybrid cryptosystems Twofish+RSA and AES+RSA are based on those techniques. The following criteria were used to compare suggested algorithms and hybrid models: memory use, encrypted file size, security level, and encryption speed. AES+RSA, one of the new hybrid models offered (AES was also chosen as a contender for the Advanced Encryption Standard contest, NIST), takes full use of both symmetric and asymmetric systems, making it substantially safe, but Twofish+RSA hybrid cryptosystem is quicker, according to study. Future research can use the entropy index to evaluate suggested hybrid models. Entropy research will make it feasible to assess each algorithm's resilience to various assaults, most notably against ciphertext frequency analysis.

REFERENCES

- Keshav Kumar, K.R. Ramkumar, Amanpreet Kaur “A Design Implementation and Comparative Analysis of Advanced Encryption Standard (AES)Algorithm on FPGA” 8th International Conference on Reliability, Amity University, Noida, India. (IEEE)June 4-5,2020 DOI: 10.1109/ICRITO48877.2020.9198033

- Raza Imam, Qazi Mohammad Areeb, Abdulrahman Alturki and Fasal Anwer “Systematic and Critical Review of RSA Based Public Key Cryptographic Schemes: Past and Present Status” (IEEE) Volume 9,2021, DOI: 10.1109/ACCESS.2021.3129224

- Sharmni Sharmee, Sadia Nowshin “Functional Modification of Advanced Encryption Standard Algorithm by Perturbing the Diffusion and Confusion Properties” 06 January 2021.

- Elza Jintcharadze, Maksim Iavich “Hybrid Implementation of Twofish, AES, ElGamal and RSA Cryptosystems” (IEEE) ,15 October 2020, DOI: 10.1109/EWDTS50664.2020.9224901

- Abhishek Guru, Asha Ambhaikar: "Development of “RSA” Encryption Algorithm for Secure Data Transmission"// Research Journal of Computer and Information Technology Sciences// ISSN 2320 – 6527 Vol. 8(1), 9-12, June (2020)"