Technical Survey on Cryptography Algorithms for Network Security

Sonia Rani, Harpreet Kaur

Department of Computer Science Applications, University Institute of Computer Science Applications and Information Sciences, SBBSU Jalandhar, Punjab, India

Abstract- Cryptography is a concept to protect network and data transmission over wireless network. Data Security is the main aspect of secure data transmission over unreliable network. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. There are two types of cryptography algorithms such as symmetric key cryptography and asymmetric key cryptography. This paper gives the review of various cryptography algorithms for network security, some related work already done by various authors, problems in existing work and some proposals for proposed work.

Keywords- Symmetric key cryptography, asymmetric key cryptography algorithms.

I. INTRODUCTION

Cryptography means “secret writing” which is the science and art of transforming messages to make them secure and immune to attacks by unauthorized user. The original data/message, before being transformed is called cipher text. An encryption is a process to transform the plaintext into cipher text and decryption transforms the cipher text back into plaintext. The sender uses an encryption algorithm and the receiver uses a decryption algorithm. Thus, encryption and decryption help to secure transmission of the message and protect the message from unauthorized users.

Cryptography Goals:

There are five main goals of cryptography. Every security system must provide a bundle of security functions that can assure the secrecy of the system. These functions are usually referred to as the goals of the security system. These goals can be listed under the following five main categories:

i. Authentication: The process of proving one’s identity. This means that before sending and receiving data using the system, the receiver and sender identity should be verified.

ii. Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver. Usually this function is how most people identify a secure system. It means that only the authenticated people are able to interpret the message content and no one else.

iii. Integrity: Assuring the receiver that the received message has not been altered in any way from the original. The basic form of integrity is packet check sum in IPv4 packets.

iv. Non-repudiation: A mechanism to prove that the sender really sent this message. Means that neither the sender nor the receiver can falsely deny that they have sent a certain message.

v. Service Reliability and Availability: Since secure systems usually get attacked by intruders, which may affect their availability and type of service to their users. Such systems provide a way to grant their users the quality of service they expect.

There are two types of cryptography algorithm that are given below:

1.1. Symmetric key cryptography algorithm

1.2. Asymmetric key cryptography algorithm

![Cryptography Algorithms Diagram](image_url)
I.1. Symmetric (Secret) Key Cryptography

This cryptographic method uses two different algorithms for encryption and decryption respectively, and a same key are used both the sender and the receiver. The sender uses this key and an encryption algorithm to encrypt data, the receiver uses the same key and the corresponding decryption algorithm to decrypt that data [1].

![Diagram of symmetric key cryptographic algorithms process]

Some widely used Symmetric key cryptographic algorithms are given below:

i. DES (Data Encryption Standard)
   DES is developed in 1970s and it uses the Fiestel Structure. It is a symmetric and block cipher algorithm that is DES uses the same key for both encryption and decryption. So the sender and receiver must know the private key. The key length is 64 bits, where 8 bits are taken for parity check. It has 16 rounds of permutation process to encrypt a message. Almost the encryption and decryption process is same except, the decryption is done in reverse order. [2]
   The possible attack to DES is brute-force attack. Also there are three fast attack is possible to DES algorithm. Those are,
   a) Differential Cryptanalysis
   b) Linear Cryptanalysis
   c) Davies Attack

ii. 3-DES(Triple–Data Encryption Standard)
   It uses 64 bit block size with 192 bits of key size. The method of encryption is same as to the one in the original DES but applied 3 times to increase the encryption level and the average safe time. [2]
   Triple data encryption standard is the next level of DES it was designed to break the attacks that DES met. To enhance the security, it processes DES in three times. 48 rounds are needed for TDES process and it has key length of 168 bits. By using this longer key, it applies to each block and encrypts the original text. The disadvantage regarding 3DES is that it is slower than other block cipher methods.

iii. AES (Advanced Encryption Standard):
   It overcomes the drawback of DES algorithm, AES is also a symmetric and block cipher algorithm. The original name of AES is Rijindeal and published in 1977. It has 128 bit block size and key sizes are 128 (10 rounds), 192 (12 rounds) and 256 bits (14 rounds).
   This key is expanded into individual sub keys, which is for every process round. This methodology is termed KEY EXPANSION. As AES is associate iterated block cipher means the similar operations are performed many times on a fixed number of bytes. The AES permutation process has four stages of substitute bytes, shift rows, mix columns and add round key.

![Diagram of one round of encryption and decryption in AES]
1) **Substitution bytes** – In this step, each byte \((a_{i,j})\) of matrix is replaced with a sub byte \((s_{i,j})\), that is Rijinideal S-Box. At the decryption end, the sub bytes are inverted to reach the original state.

2) **Shift Rows** - The shift rows operation, shift each rows with a certain constraint. That is first row of matrix is left same, the second, third and forth rows are shifted to one place left.

3) **Mix Columns** – In this step, the each column is multiplied with a fixed polynomial and the new value of the columns is placed.

4) **Add Round Key** – This sub key is derived from the main key and the sub key is added into this step by applying XOR to the matrix. [2]

**iv. Blowfish:**

Blowfish is a symmetric block cipher that can be effectively used for encryption and safeguarding of data. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data. Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms.

Blowfish is a variable-length key block cipher. It is suitable for applications where the key does not change often, like a communications link or an automatic file encryptor. It is significantly faster than most encryption algorithms when implemented on 32-bit microprocessors with large data caches. [4]

**v. RC4 (Rivest cipher 4):**

RC4 is developed by Ron Rivest also known as Rivest Cipher 4. Here the stream cipher is used for encryption of the plain text. Pseudorandom stream of bits (key stream) are generated by the RC4 algorithm, and bit-wise encryption/decryption has been performed. The generation key system involves two stages,

- One is the permutation of all 256 bytes.
- Another is two 8-bit index-pointers.

The key length for this RC4 is between 40-128 bits. If the common block ciphers are not used MAC strongly, bit-flapping attack is possible and the stream-cipher attack is also vulnerable if they are not correctly implemented. [3]

### I.2. Asymmetric (public) Key Cryptography

This cryptographic method makes use of two different algorithms for encryption and decryption respectively, a public key for encryption and a private key for decryption. The public key of the sender is used to encrypt the message by the sender. The receiver decrypts the cipher text with the help of a private key [1].

The some widely used Asymmetric key cryptographic algorithms are given below:

i. **RSA**

ii. **DIFFIE-HELLMAN**

iii. **PAILLIER**

iv. **Elgamal**

**Fig 4: Asymmetric key cryptographic algorithms process**

**i. RSA (Rivest–Shamir-Adlemen)**

This is public key encryption algorithm developed by Adi Shamir, Ron Rivest and Len Adlemen in 1977. It is most popular asymmetric key cryptographic algorithm. RSA may use to provide both secrecy and digital signature. It uses the prime no. to generate the public and private key based on mathematical fact and multiplying large numbers together. the block size data is used in which plaintext and cipher text are integers between \(\text{nand n1}\) for some \(\text{n values}\). Consider the Size of \(\text{n}\) is 1024bits or 309 decimal digits. In this two different keys are used for encryption and decryption purpose. And also the sender knows encryption key and receiver knows decryption key. [2]

**ii. DIFFIE-HELLMAN:**

The scheme was first revealed by Whitfield Diffie and Martin Hellman in 1976. Diffie–Hellman key exchange is a specific method of exchanging cryptographic keys. It permits two parties that have no prior knowledge of each other to jointly make a shared secret key over an insecure communications channel. This key can then be used to encrypt posterior communications using a symmetric key cipher. [1]

© 2016, IJARCSSE All Rights Reserved
iii. **PAILLIER:**

The Paillier cryptosystem is an asymmetric algorithm. It has homomorphic property permits this scheme to do normal addition operations on several encrypted values and achieving the encrypted sum, the encrypted sum can be decrypted later without even knowing the values ever that made up the sum.[1]

iv. **ELGAMAL:**

El-Gamal is the asymmetric key cryptography. It is a public key cryptography which is based on Diffie Hellman key exchange. It was introduced by Taher El-Gamal in 1985. It is consist of signature, encryption algorithms as well as discrete logarithm problems [5]. ElGamal encryption consists of three components: the key generator, the encryption algorithm, and the decryption algorithm.

**II. RELATED WORK**

This section gives the overview of related work by various authors in network security algorithms

Diasa Salama Abd Elminaam et al. [2010], presents evaluation of six of the most common encryption algorithms namely: AES (Rijjindeal), DES, 3DES, RC2, Blowfish, and RC6. A comparison has been conducted for those encryption algorithms at different settings for each algorithm such as different sizes of data blocks, different data types, battery power consumption, different key size and finally encryption/decryption speed. [6]

Jawahar Thakur et al. [2011], provides a fair comparison between three most common symmetric key cryptography algorithms: DES, AES, and Blowfish. Since main concern here is the performance of algorithms under different settings, the presented comparison takes into consideration the behavior and the performance of the algorithm when different data loads are used. The comparison is made on the basis of these parameters: speed, block size, and key size. [2]

Shashi Mehrotra Seth et al. [2011], performs comparative analysis of three algorithm: DES, AES an RSA considering certain parameters such as computation time, memory usages and output byte. A cryptographic tool is used for conducting experiments. Experiments results are given to analyses the effectiveness of each algorithm. [7]

Prapat Chandra Mandal et al. [2012], provides a fair comparison between four most common and used symmetric key algorithms: DES, 3DES, AES and Blowfish. A comparison has been made on the basis of these parameters: rounds block size, key size, encryption/decryption time, CPU process time in the form of throughput and power consumption. These results show that blowfish is more suitable than AES. [8]

Lalit Singh et al. [2013], provides a fair comparison between five most common and used symmetric and asymmetric key algorithms: Two fish & Blowfish, IB_nRSA, RSA, RC. A comparison has been made on the basis of these parameters: rounds block size, key size, and encryption/decryption time, CPU process time in the form of throughput. These results show that IB_nRSA is more suitable than other algorithms. [9]

Jitendra Singh Chauhan et al. [2105], focuses on the comparative study of various cryptographic algorithms like AES, DES, RSA, Blowfish, Elliptic Curve, SHA and MD5 and give a proper direction to the users for use of proper algorithm for securing of data. MD5 algorithm takes least encryption time whereas, RSA takes largest encryption time. [10]

Jitendra Singh Laser et al. [2016], surveyed the conventional algorithms, based on their benefits and drawbacks. We additionally have in comparison the significance of each these cryptographic techniques. This paper also offer an appropriate future opportunity related to these cryptographic techniques. [11]

Md. Alam Hossain et al. [2016], describes the basic characteristics (Key Length, Block size) of symmetric (AES, DES, 3DES, BLOWFISH, RC4), Asymmetric (RSA, DSA, Diffie-Hellman, El-Gamal, Paillier), Hashing (MD5, MD6, SHA, SHA256) algorithms. Also we implemented five well-known and widely used encrypt techniques like AES, DES, BLOWFISH, DES, RC4, RSA algorithms and compared their performance based on the analysis of their encryption and decryption time for different file sizes in the local system. [1]

V. Kapoor et al. [2016], a hybrid cryptographic technique for improving data security during network transmission is proposed and their implementation and results are reported. The proposed secure cryptographic technique promises to provide the highly secure cipher generation technique using the RSA, DES and SHA1 technique. [12]

Dr. D. Vimal Kumar et al. [2016], some well-known cryptographic algorithms have been analyzed in this paper to demonstrate the basic differences between the existing encryption techniques. Regardless of the mathematical theory behind an algorithm, the best algorithm are those that are well-known and well-documented because they are well-tested and well studied. [13]

**III. PROBLEM FORMULATION**

Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. The information being transmitted through a network is vulnerable to various types of passive and active attacks. Cryptography is an emerging technology, which is important for network security. There are two methods of sending such data using the Asymmetric and Symmetric key cryptography [16].

From the literature survey, it is reviewed that all cryptography algorithms have their own pros and cons. There are many security algorithms available and they require more time for encryption and decryption and the ones which require less encryption and decryption time are easy to crack and have low throughput. To overcome the drawbacks of existing system and to increase the security, to decrease the encryption and decryption time, to increase the throughput, a hybrid encryption model using AES and ElGamal algorithms can be designed.

**IV. PROPOSED WORK**

To design a hybrid encryption model using AES and ELGAMAL algorithms for enhancing the security, to reduce encryption and decryption time, data size, space complexity, power consumption and to increase throughput following are some points as a proposals to implement.
1. To implement AES and El-Gamal algorithms.
2. To combine AES and El-Gamal algorithms.
3. To compare the algorithms implemented in step 1 and 2.

V. CONCLUSION

In order to protect the intended data from hacking, cryptography is performed. In this paper we briefly discussed about cryptography and various symmetric and asymmetric algorithms. Cryptographic algorithms play a very important role in Network security. In the review of literature work there are some drawbacks. To overcome these drawbacks, if we implement proposed technique the results may be better than the existing work.

REFERENCES


