Asymmetric Algorithms and Symmetric Algorithms: A Review

Tannu Bala
Research Scholar(MTech)
BGIET,Sangrur

Yogesh Kumar
Assistant Professor
BGIET,Sangrur

ABSTRACT

In these days securing a network is an important issue. Many techniques are provided to secure network. Cryptographic is a technique of transforming a message into such form which is unreadable, and then retransforming that message back to its original form. Cryptography works in two techniques: symmetric key also known as secret-key cryptography algorithms and asymmetric key also known as public-key cryptography algorithms. In this paper we are reviewing different symmetric and asymmetric algorithms.

Keywords

RSA (Rivest Shamir Aldeman), El-gamal, Symmetric cryptography, Asymmetric cryptography.

1. INTRODUCTION

1.1 Cryptography

Information security plays a very important role when communication is provides by using internet. It is very important for people who are committing by e-transaction service. [1] There are various cryptography methods that provide security to password and payments that relay on internet. To achieve this level of security, various security protocols that are of Symmetric-key and asymmetric-key type have been developed. Cryptography is necessary for secure communications. Cryptography has many uses and applications such as protecting private company information. It allows the user to order a product on the internet without the fear of their credit card number being stolen and used against them anymore. [1] Cryptography is all about increasing the level of privacy of individuals and groups.

1.2 Termed Used in Cryptography

Plain text: The original message that the person want to send is known as plain text. For an example, Tom is a sender who want to send message “hello, how are you” to person bob which is at receiver side. Then the message “hello, where are you?” is known as plain text.

Cipher text: When plain text is coded by using encryption then the generated text is known as cipher text. This message cannot be understood by anyone. For an example “unjn122%$if “is a cipher text produced for plain text “hello, where are you “.

Encryption: Converting plain text to cipher text is referred as encryption. A message in original form is known as Plaintext.

For security reasons, this message is then coded using a cryptographic algorithm. This process is called Encryption.

An encrypted message is known as Cipher text. It requires two processes: - Encryption algorithm and a key. Encryption algorithm is used by sender.

Decryption: Converting cipher text back to plain text is known as decryption. This may also need two requirements: Decryption algorithm and key. Decryption is done by receiver.

Key: Key is the Combination of any numeric or alpha numeric text or special symbol. Key is used at the time of encryption or decryption. Encryption and Decryption process directly depend upon it so key is very important.

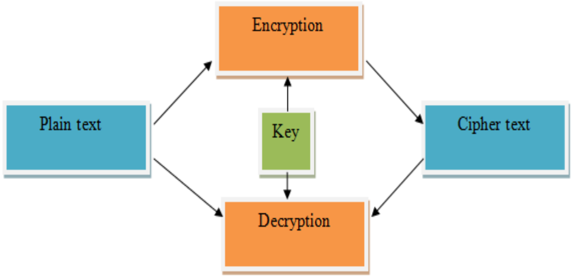


Fig 1: encryption and decryption with key

1.3 Approaches

The Cryptography or methods used for securing the information are classified into following categories:

- Symmetric Key Cryptography
- Asymmetric Key Cryptography

Symmetric-Key Cryptography (also known as single-key encryption and private key encryption) is a type of encryption in which same secret key is used to encrypt and decrypt information. A secret key can be a number, a word, or simple a string of random letters. Secret key is applied to plain text to change the content. This is done simply by shifting each letter in a number of places. In this technique both the sender and receiver has to know about secret key, so they can encrypt and decrypt all information. In any symmetric-key encryption techniques, both encryption and decryption process are carried out using a single key.DES is a symmetric key algorithm. [2]

These algorithms have many advantages:

1. Efficient and secure
2. Execute at high speeds
3. Consume less computer resources of memory and processor time.

However, symmetric key cryptographic techniques suffer from many problems:

1. Key distribution problem

2. Key management problem
3. Inability to digitally sign a message.

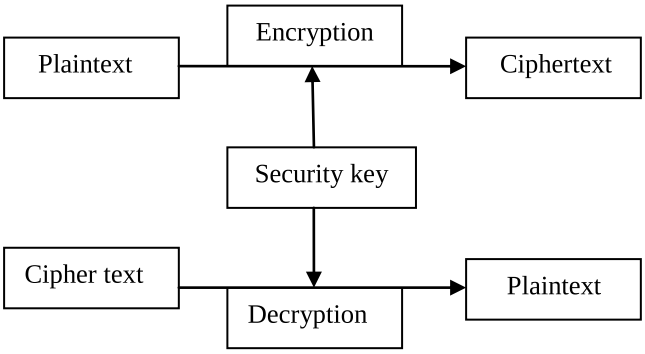


Fig 2: Symmetric key cryptography process [3]

Asymmetric Key Cryptography: The problem with secret keys is exchanging them over the Internet while preventing them from thief. Anyone who knows the secret key can decrypt the message. To overcome this, we have asymmetric encryption technique, in which there is related pair of keys. [4] A public key is available to anyone who might want to send you a message. A second, private key is kept secret, so that only receiver knows it. Any messages that are encrypted by using the public key can only be decrypted by applying the same algorithm, but by using the matching private key. Any message that is encrypted by using the private key can only be decrypted by using the matching public key. This means that you do not have to worry about passing public keys over the Internet. A problem with asymmetric encryption, however, is that it is slower than symmetric encryption. It requires far more processing power to both encrypt and decrypt the content of the message. In it, instead of a single key, every person has a pair of keys. One key, called the public key is known to everyone and the other one, the private key is known only to the owner. There is a mathematical relationship between both these keys. Thus, if any message ‘m’ is encrypted using any of the key, it can be decrypted by the other portion. Various asymmetric encryption algorithms (RSA, Elgamal) have been implemented [4].

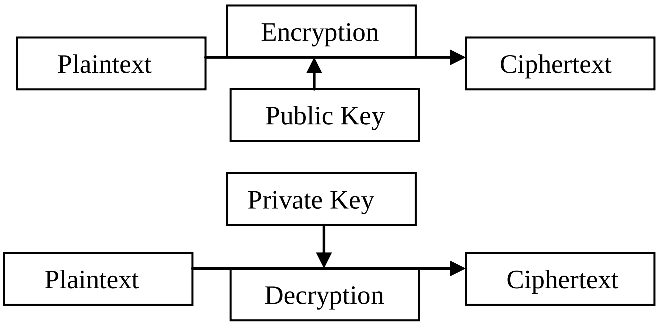


Fig 3: Asymmetric key cryptography process [3]

2. LITRATURE REVIEW

Ankit Gambhir (2014) in this paper [1] performance as well as comparison between two cryptographic algorithms (RSA and DES) was implemented. There are two techniques of cryptography: symmetric key that is also called secret-key cryptography algorithms and asymmetric that is also called public-key cryptography algorithms. DES is secret- key based algorithm and RSA is public key based algorithm. Both the algorithms are very efficient.

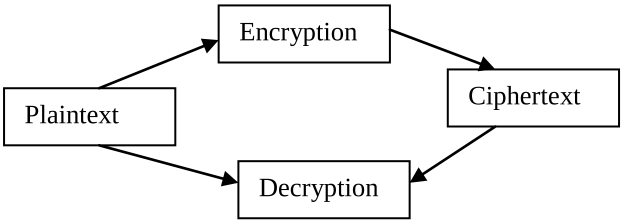


Fig 4: The process of encryption and decryption [5]

DES algorithm with its steps to provide encryption and decryption was discussed same RSA algorithm was discussed with all its steps.

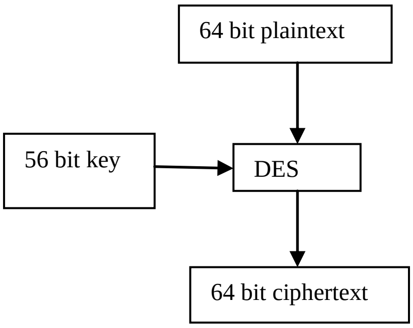
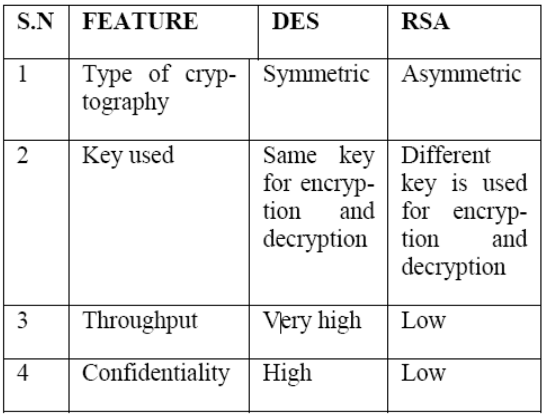


Fig 5: DES process [5]

Comparison table shows us the difference between DES and RSA algorithm based on four different parameters: type of cryptography, key used, throughput, confidentiality.

Table 1: Comparison between Des and Rsa Algorithm [5]



S.N	FEATURE	DES	RSA
1	Type of cryptography	Symmetric	Asymmetric
2	Key used	Same key for encryption and decryption	Different key is used for encryption and decryption
3	Throughput	Very high	Low
4	Confidentiality	High	Low

Annapoorna Shetty et. al. (2014) in this paper [4] a detail about cryptography is studied. Cryptography is the art and science of protecting information from unwanted person and converting it into a form which is not easily breakable. The main aim of cryptography is keeping data secure form unauthorized persons. Data cryptography mostly is the combination of the content of data, such as text data, image related data and audio, video related data. To convert that data into code form (cipher text) is called data encryption. The reverse of data encryption process is called data Decryption.

The paper first discusses about different goals of the cryptography. Different goals like Confidentiality, Authentication, Integrity, Non Repudiation, Access control are discussed. Different type of attacks that may damage your data is mentioned. In the paper nine different attacks are discussed including Cipher text-only attack, Known-plaintext attack, Chosen-plaintext attack etc.

Two types of cryptography are discussed. This paper gives detail about two asymmetric algorithm RSA and Elgamal algorithm. Summary table give the detail of the two algorithms based on different factor analyzed. In this paper the summary table reports the key length value, type of algorithm, security attacks, simulation speed, scalability, key used, power consumption, and hardware/ software implementation difference between RSA and EL-Gamal.

Bryce D. Allen (2008) in this paper [5] two previous cryptography techniques Asymmetric and Symmetric cryptography are combined into one know as Hybrid Cryptosystems. Hybrid cryptosystems combine them to gain the advantages of both. This paper implements the two attacks, basic meet-in-the-middle attack and the two-table attack. Several variations in basic meet-in-middle attack are implemented and all these implementations are done in c++. Table 1.1 shows Splitting probability of the experiment. Elgamal cryptography algorithm with Discrete Log Problem was discussed. This paper discuss meet-in-middle attack in detail with different parameters like its Requirements and Assumptions, problem Solution, its implementation, its Running Time and Memory Usage. Then second attack “two table attacks” was discussed with same parameters.

Implementing a cryptosystem securely requires far more than an understanding of the basic algorithm. The implementer must be aware of possible attacks on the system, and choose keys and parameters to make those attacks infeasible. This paper discussed attacks which rely on the underlying mathematics - however timing attacks have been discovered against various cryptosystem which gain information based on how long the computer takes to perform encryption or decryption operations.

Franck Lin (2010) [6] explain the cryptography book. He divides this book into two parts; first part contains the description of Symmetric and Asymmetric key algorithm with examples. A stream cipher attempts to imitate a one-time pad. Since it is impractical to have a key that is at least the same size as the plaintext, stream ciphers take a smaller 128 bit key. Block ciphers represent a major advancement in cryptography and have little vulnerability. Most block ciphers rely on substitution-permutation rounds. In each round, data is broken up into 8-bit sections, substituted according to a key, recombined, and then rearranged according to a key. Second part contains the description of digital Age and cryptography. This report confirms the feasibility and strength of quantum cryptography, highlighting an almost certain legal battle and information technology revolution.

Sombir Singh et. al. (2013) in this paper [7] “DES” Symmetric algorithm was explained. Data encryption standard (DES) is a private key cryptography system that provides the security in communication system but DES has the problem of brute force attacks. To improve the security of DES algorithm the transposition technique is added before the DES algorithm to perform its process. If the transposition technique is used before the original DES algorithm then the user required first to break the original DES algorithm and then transposition technique. So the security is approximately double as compared to a simple DES algorithm.

This paper includes four techniques to provide security. First is DES, Double DES (2DES), Its process is the same as DES but repeated same process 2 times using two keys K1 and K2, Triple DES is DES -three times, last one is the transposition technique, this does not replace the one alphabet with another like the substitution technique but perform the permutation on the plain text to convert it into cipher text.

The Designed system improved the security power of original DES. The only drawback of Enhanced DES is extra computation is needed but the today’s computer have parallel and high speed computation power so the drawback of the Enhanced DES algorithm is neglected because our main aim is to enhance the security of a system.

3. DETAIL ABOUT DIFFERENT CRYPTOGRAPHIC ALGORITHM

Data Encryption Standard (DES): DES algorithm is secret key based algorithm in which same key is used for encryption and decryption. Des is a symmetric key algorithm. DES is the block cipher — an algorithm that takes a fixed-length string of plaintext bits. In the case of DES, the block size is 64 bits. The key originally consists of 64 bits; however, only 56 of these are actually used by the algorithm. Eight bits are used for checking parity, and are thereafter discarded. Hence the effective key length is 56 bits. [2] DES when implemented with hardware and software it give better performance in hardware rather than in software [8]. DES consumes low power as compare to any other cryptography algorithm (RSA).

Advanced Encryption Standard (AES): AES is the advance encryption algorithm which is proposed to provide very strong security and to overcome the problem of DES algorithm. AES is the block cipher. In the case of AES, the block size is 128 bits. Size of a key is depends upon the plain text. Standard size of the key is 128 bit but if for some reasons more security is required then it may increase upto 256 bits (192 and 256). Number of rounds are depend upon key size: if key is of 128 bit then 10 rounds are there, if 192 key size is used then 12 rounds are there and if key size is 256 then 14 no. of rounds are there. AES is now used worldwide.[6]

Rivest Shamir Aldeman (RSA): RSA algorithm is the most commonly used and secure public key encryption and authentication algorithm. It can be used to encrypt a message without the need to exchange a secret key separately. It is included as part of the Web browsers from Microsoft and Netscape. It's also part of Lotus Notes, Intuit's Quicken, and many other products. The encryption system is owned by RSA Security. The company licenses the algorithm technologies and also sells development kits. The technologies are part of existing or proposed Web, Internet, and computing standards. RSA security depends on the difficulty of factoring the large integers. It is generally considered to be secure when sufficiently long keys are used (512 bits is insecure, 768 bits is moderately secure and 1024 bits is good, for now).

RSA computation occurs with integers modulo n = p*q. It requires keys of at least 1024 bits for good security. Keys of size 2048 bit provide best security. Widely used for secure communication channel and for authentication to identity service provider. RSA is too slow for encrypting large volumes of data but it is widely used for key distribution. [9] RSA has the disadvantage that it is not efficient for both hardware and software implementation. The principle of RSA algorithm is „it is easy to multiply two prime numbers but difficult to factor them‟. As RSA is asymmetric key cryptographic algorithm so there are different keys for encryption and decryption. [1]

Elgamal Algorithm: ElGamal encryption/decryption is based on the difficulty of the discrete algorithm problem where it is straight forward to raise numbers of large powers but it is much harder to do the inverse computation of the discrete logarithm. The ElGamal algorithm depends on certain parameters which are affecting the performance, speed and security of the algorithm. ElGamal encryption is one of many encryption schemes which utilizes randomization in the encryption process. [9]

The ElGamal algorithm can be use as RSA algorithm for public key encryption because:

• RSA encryption depends on the difficulty of factoring large integers while

• ElGamal encryption depends on on the difficulty of computing dicrete logs in a large prime modulus.

ElGamal is nothing but the advance version of Diffie- Hellmen key exchange protocol. But, ElGamal is not good because its cipher text is two times longer than the plain text. ElGamal is good because it gives different cipher text for same plain text each time. For image data, the size of the cipher text is very huge & reshaping the encrypted data was not under-stood. ElGamal‘s encryption is very simple because it is multiplication of message and symmetric key

4. CONCLUSION

Security is playing a very important and powerful role in the field of networking, Internet and various communication systems. In this paper we compare various symmetric algorithms (DES and AES) and asymmetric algorithms (RSA and Elgamal). Based on this research we conclude that in symmetric algorithm AES is better and in asymmetric algorithm Elgamal is better to provide security. For future, algorithms will be enhanced to get more powerful security system.

5. REFERENCES

[1] Gambhir, Ankit. "RSA Algorithm or DES Algorithm?" Journal of Engineering Computers & Applied Sciences 3.4 (2014).

[2] Bhardwaj, CR S. "Modification of Des Algorithm." International Journal of Innovative Research and Development 1.9 (2012).

[3] Thakur, Jawahar, and Nagesh Kumar. "DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis."International journal of emerging technology and advanced engineering 1.2 (2011).

[4] Annapoorna Shetty, Shravya Shetty and Krithika. “A Review on Asymmetric Cryptography –RSA and ElGamal Algorithm” International Journal of Innovative Research in Computer and Communication Engineering 2014.

[5] Allen, Bryce. Implementing several attacks on plain ElGamal encryption. ProQuest, 2008.

[6] Lin, Franck. "Cryptography’s Past, Present, and Future Role in Society”.

[7] Singh, Sombir, Sunil K. Maakar, and Sudesh Kumar. "A Performance Analysis of DES and RSA Cryptography." International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), ISSN: 2278-6856.

[8] Padmavathi, B., and S. Ranjitha Kumari. "A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique."International Journal of Science and Research 2.4 (2013).

[9] Singh, Rashmi, and Shiv Kumar. "Elgamal’s Algorithm in Cryptography."International Journal of Scientific & Engineering Research 3 (2012).

[10] Menezes, Alfred J., Paul C. Van Oorschot, and Scott A. Vanstone. Handbook of applied cryptography. CRC press, 1996.

[11] Li, Xiaofei, Xuanjing Shen, and Haipeng Chen. "ElGamal Digital Signature Algorithm of Adding a Random Number." Journal of Networks 6.5 (2011): 774-782.

[12] Sison, Ariel M., et al. "Implementation of Improved DES Algorithm in Securing Smart Card Data." Computer Applications for Software Engineering, Disaster Recovery, and Business Continuity. Springer Berlin Heidelberg, 2012. 252-263.

[13] Mahajan, Prerna, and Abhishek Sachdeva. "A study of Encryption Algorithms AES, DES and RSA for Security." Global Journal of Computer Science and Technology 13.15 (2013).

[14] William Stallings, " Cryptography and Network Security Principles and Practices", Prentice Hall, November 16, 2005.

[15] Elminaam, Diaa Salama Abd, Hatem Mohamed Abdual-Kader, and Mohiy Mohamed Hadhoud. "Evaluating The Performance of Symmetric Encryption Algorithms." IJ Network Security 10.3 (2010): 216-222.