A Review of Cryptographic Techniques Used in Wireless Network Security

Zeeshan Pasha[1] and Muhammad Awais Chheena[2]
[1,2]Department of Computer Science and Engineering, UET, Lahore, Pakistan
[1]zeeshanpasha783@gmail.com, [2]chaudhry176@gmail.com

***Abstract*– The study of secret writing is known as Cryptography. It is basically science and art. For network security cryptography is basically now a day's most popular approach which are using in industry. There is two parts of cryptography, one is encryption and other one is decryption. The process of converting the plain text into cipher text with the help of some keys is known as Encryption. The process of converting back the cipher text into plain text with the help of some keys is known as Decryption. Cryptography is playing main role in providing security for the networks and in Internet security it is main part like Emails. Public key, symmetric key and hash function cryptography are used for the encryption and decryption for secure communication. In this review paper, among the various existing encryption decryption algorithms like DES, 3DES, BLOWFISH, IDEA, AES, RC6, MD5 and RSA are chosen and compared on the premise of size, block size, round, structure, security, flexibility to expand in future and limitations.**

***Keywords*– Network Security, Encryption, Decryption, Symmetric Key, Public Key and Cipher Text**

I. INTRODUCTION

Cryptography assumes a noteworthy part in an art of mystery composing. It is the specialty of securing data by changing and innovation application. The primary purpose behind utilizing email is likely the comfort and speed with which it can be transmitted, regardless of topographical separation. Presently a day's our whole globe is relying upon web and its application to ensuring national security. Cryptography is utilized to guarantee that the substance of a message is exceptionally privacy transmitted and would not be changed. The possibility of encryption and encryption calculation by which we can encode our information in mystery code and not to be capable discernable by programmers or unapproved individual even it is hacked [3]. As it is difficult to quit hacking, we can secure our touchy information even it is hacked utilizing encryption strategies and which ensuring the data security; since World War-I and the coming of the PC, the strategies used to complete cryptology have turned out to be progressively mind boggling and its application more across the board.

A) Wireless Networks

Wireless networks are system networks that aren't connected by cables of any kind. The utilization of a wireless network permits enterprises to avoid the expensive method of introducing cables into buildings or as an association between totally different instrumentation locations. The idea of wireless systems is radio waves, associate degree of implementation that takes place at the physical level of network structure.

B) Cipher Text

Cipher text is encrypted text. Plaintext is what you have got before cryptography, and cipher text is that the encrypted result. The term cipher is usually used as a word for cipher text, however it a lot of properly means that the strategy of cryptography instead of the result.

Safety measures should be incorporated into pc systems whenever they're potential targets for malicious or mischievous hacks. This can be particularly for systems that handle financial transactions, confidential, classified or different data whose secrecy and integrity are crucial. With the necessity to guard the integrity and privacy of data belonging to individuals and organizations, we've developed this technique.

II. ENCRYPTION AND DECRYPTION ALGORITHMS

Encryption is a procedure of coding data which could either be a record or mail message into figure message a shape indistinguishable without a deciphering key. Keeping in mind the end goal to counteract anybody aside from the expected beneficiary from perusing that information. Decoding is the turnaround procedure of changing over encoded information to its unique and un-encoded shape of plaintext [2]. Encryption Decryption process is explained in Fig. 1.

A key in cryptography is a long grouping of bits utilized by encryption/unscrambling calculations.

A given encryption calculation takes the first message, and a key, and modifies the first message numerically in light of the key's bits to make another encoded message. In like manner, a decoding calculation takes a scrambled message and re-establishes it to its unique frame utilizing at least one key. To encode plaintext, an encryption key is utilized to force an encryption calculation onto the information. To interpret, a client must have the fitting unscrambling key. An unscrambling key comprises of an arbitrary series of numbers, from 40 through 2,000 bits long. The key forces a decoding

Fig. 1: Encryption Decryption Process

calculation onto the information. This decoding calculation switches the encryption calculation, restoring the information to plaintext. More extended the encryption key, more troublesome to translate it. For a 40-bit encryption key, more than one trillion conceivable decoding keys exist.

A) Need of Cryptographic Algorithms

Authentication: Verification systems help to set up confirmation of characters. This procedure guarantees that the birthplace of the message is accurately recognized.

Confidentiality: The rule of classification determines that lone the sender and the planned beneficiary ought to have the capacity to process the substance of a message.

Availability: The standard of accessibility expresses that assets ought to be accessible to approved gatherings every one of the circumstances.

Integrity: The respectability instrument guarantees that the substance of the message continue as before when it achieves the proposed beneficiary as sent by the sender.

Access Control: Access Control indicates and controls who can get to the procedure [1].

III. TYPES OF CRYPTOGRAPHIC ALGORITHMS

There are a few methods for ordering cryptographic calculations. They will be sorted in view of the quantity of keys that are utilized for encryption and decoding and further characterized by their application and utilization. The accompanying are the three sorts of algorithms that are talked about [2].

Symmetric Key Cryptography (SKC): Utilizations a solitary key for both encryption and unscrambling.

Public Key Cryptography (PKC): Utilizations one key for encryption and another for unscrambling.

Hash Functions: Utilizations numerical changes to irreversibly "encode" data.

A) Symmetric Key Cryptography

The most broadly utilized symmetric key cryptographic strategy is the Data Encryption Standard (DES). It is the most generally utilized symmetric-key approach. It utilizes a settled length of 56-bit key and an effective calculation to rapidly encode and unscramble messages. It can be effectively actualized in equipment, influencing the encryption and unscrambling to process significantly speedier. When all is said in done, expanding the key size, makes the framework more secure. A variety of DES called Triple-DES or DES-EDE (scramble decode encode), utilizes three uses of DES and two free DES keys to deliver a successful key length of 168 bits [2].

Regardless of the proficiency of symmetric key cryptography, it has a major frail spot-key administration. Since a similar key is utilized for encryption and unscrambling, it must be kept secure. On the off chance that an enemy knows the key, at that point the message can be unscrambled. In the meantime, the key must be accessible to the sender and the collector and these two gatherings might be physically isolated. Symmetric key cryptography changes the issue of transmitting messages safely into that of transmitting keys safely. This is a change on the grounds that keys are considerably littler than messages and keys can be created in advance. By and by, guaranteeing that the sender and recipient are utilizing a similar key that potential enemies don't have the foggiest idea about these key remains a noteworthy hindrance. This is alluded to as the key administration issue. This process explained in Fig. 2.

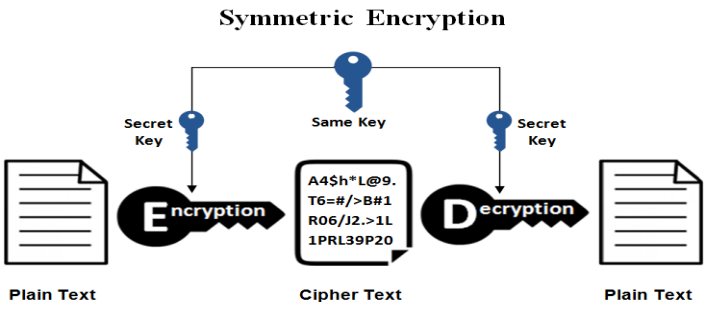

Fig. 2: Symmetric Encryption Decryption Process

B) Public/Private Key Cryptography

Asymmetric key cryptography beats the key administration issue by utilizing diverse encryption and decoding key sets. Knowing about one key, say the encryption key, isn't sufficiently adequate to decide the other key - the decoding key. In this manner, the encryption key can be made open gave the unscrambling key is held just by the gathering wishing to get scrambled messages (henceforth the name public/private key cryptography). Anybody can utilize the general population key to scramble a message, however just the beneficiary can decode it.

The scientific connection between people in public/private key match allows a general run: any message encoded with one key of the combine can be effectively unscrambled just with that key's partner. To encode with general society key means you can unscramble just with the private key. The opposite is additionally evident - to scramble with the private key means you can decode just with general society key [3]. This process explained in Fig. 3.

C) Hash Functions

Hash works (a kind of one-way work) are essential for quite a bit of cryptography. In this application, capacities are portrayed and assessed as far as their capacity to withstand assault by an enemy. All the more particularly, given a message x, on the off chance that it is computationally infeasible to discover a message y not equivalent to x with the end goal that H(x) = H(y) at that point H is said to be a feebly impact free hash work. An emphatically impact free hash work H is one for which it is computationally infeasible to locate any two messages x and y with the end goal that H(x) = H(y) [6].

The necessities for a decent cryptographic hash work are more grounded than those in numerous different applications (mistake remedy and sound ID excluded). Consequently, cryptographic hash capacities make great stock hash capacities - even capacities whose cryptographic security is traded off. For example MD5 and SHA-1. The SHA-2 calculation, however, has no known bargains. This process explained in Fig. 4.

IV. LITERATURE SURVEY

B. Nithya et. al [3] a portion of the current calculations like DES, 3DES, AES, Blowfish, RC4, RSA and MD5 calculations. In any case, IDEA, TEA, CAST, RC2, RC5, RC6, Serpent, Twofish, Threefish, Mars, ECC, DHA, SHA are looked at and perused less. The correlations of calculations are in the premise of security, adaptability, encryption execution, speed and memory use. The near outcomes said that the calculations AES, Blowfish, RC4, DES, TDES are most quick in encryption time, speed, memory when contrasted with others. The everyday enhancing web innovation needs more and quick security for the correspondence channel, through which the data is passing.

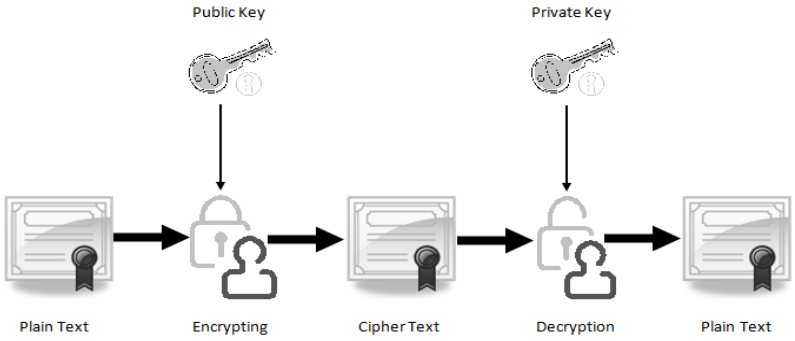

Fig. 3: Public/Private Encryption Decryption Process

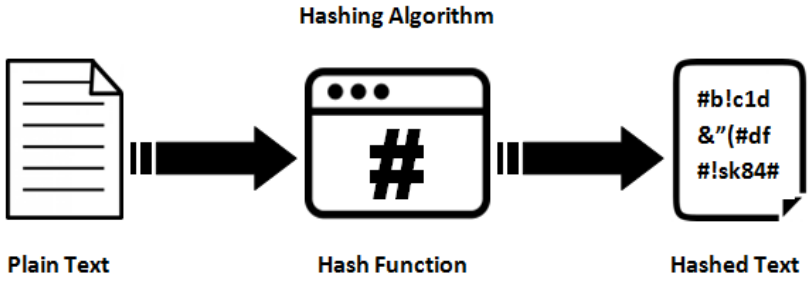

Fig. 4: Hashing Encryption Decryption Process

A. Joseph Amalraj et. al [1] gives a detailed study of Cryptography Techniques like AES, DES, 3DES, Blowfish, RSA, CL-PKC. Among those algorithms and concepts the security for the data has become highly important since the selling and buying of products over the open network occur very frequently. They surveyed about the existing works on the encryption techniques. The selected algorithms are AES, 3DES, Blowfish and DES. It was concluded that Blowfish has the better performing than other algorithms.

Anjula Gupta et. al [4] the current encryption strategies are examined and investigated to advance the execution of the encryption techniques additionally to guarantee the security procedures. To total up, all systems are one of a kind in its own particular manner, which may be appropriate for various applications. By Surveying numerous papers, established that throughput estimation of BLOWFISH is more noteworthy than every symmetric calculation. Power Consumption estimation of BLOWFISH is minimum. The trial consequences of numerous papers demonstrated that BLOWFISH has preferable execution and productivity over all other piece figures. The following method that is broadly used to ensure our data is RSA. I have perused numerous papers on Cryptography that primarily utilized RSA calculation for data security. RSA is the most secure and broadly utilized by specialists. RSA can be utilized with numerous strategies like RSA and DES, RSA and AES, RSA and DIffie Hellman, RSA and IDEA, RSA and Blowfish, RSA and Twofish by consolidating cryptography calculations to enhance security.

Zoran Hercigonja et.al [5] gives a scientific examination on different symmetric encryption calculations, for example, DES, 3DES, CAST-128, BLOWFISH, IDEA, AES, RC6 and unbalanced RSA algorithm. The investigation depends on the engineering of the calculations, the security perspectives and the constraints they have. The examination plainly expresses that however Asymmetric algorithms are prevalent in security, they set aside more opportunity for handling and requires more memory. For all intents and purposes, Asymmetric calculations like RSA are utilized for the key trade and symmetric calculations are utilized for encryption/unscrambling.

V. COMPARISON OF CRYPTOGRAPHY ALGORITHMS

Among various existing encryption decryption algorithms, DES, 3DES, BLOWFISH, IDEA, AES, RC6, MD5 and RSA are chosen and compared on the premise of size, block size, round, structure, security, flexibility to expand in future and limitations. Table I illustrates the comparative study on chosen algorithms.

Table I: Comparative Analysis of Existing Algorithms

Author	Algorithm Studied	Description	Conclusion
B. Nithya et.al [3]	DES TDES AES RSA RC4 MD5 SHA	Compared Algorithms – Key • Size • Block Size	Calculations AES, Blowfish, RC4, DES, TDES are most quick in Encryption time, speed, memory when contrasted with others.
A. Joseph Amalraj et. al [1]	DES 3DES AES Blowfish RSA	Compared Algorithms – Key • Size • Block Size • Round • Structure • Flexibility	Best performance is given by blowfish algorithm as compared to other algorithms.
Anjula Gupta et. al [4]	DES 3DES AES Blowfish IDEA RC4 RC6 Serpent Twofish TEA CAST RSA Diffie-Hellman MD5	Compared Algorithms – Key • Size • Block Size • Round • Structure • Flexibility • Features	Throughput value of BLOWFISH is greater. Power Consumption value of BLOWFISH is least.
Zoran Hercigonja et. al [5]	DES 3DES CAST-128 BLOWFISH IDEA AES RC6 RSA	Compared Algorithms – Key • Structure • Flexibility • Modification • Known Attacks	Basically Symmetric algorithms are used encryption decryption method and RSA algorithms used key exchange method.

From the above comparative analysis on existing algorithms, it will be mentioned that what proportion the study created on every algorithms. Authors have taken more than once, some of the existing algorithms like DES, 3DES, AES, Blowfish, RC4, RSA and MD5 algorithms. But IDEA, RC5, RC6, TEA, CAST, ECC, DHA, SHA, RC2, Serpent, Twofish, Threefish, Mars are compared and perused less. The comparisons of algorithms are within the basis of security, flexibility, structure, performance, size, block size, round and memory usage. The comparative outcomes said that the algorithms AES, Blowfish, RC4, DES, TDES are most quick in encoding time, speed, memory in comparison to others.

VI. CONCLUSION

System Security is the most crucial part in data security. The everyday enhancing web innovation needs more and quick security for the correspondence channel, through which the data is passing. Cryptography is a developing innovation which is essential for organize security. Symmetric calculations have quickest than unbalanced calculations. In this paper, we have presented the comparative study of the different encryption methods and their calculation mechanisms. The current encryption strategies are contemplated and dissected to advance the execution of the encryption techniques additionally to guarantee the security procedures.

REFERENCES

[1] A. J. Amalraj and J. J. R. Jose, "A survey paper on cryptography techniques," *International Journal of Computer Science and Mobile Computing,* vol. 5, pp. 55-59, 2016.

[2] V. Agrawal, S. Agrawal, and R. Deshmukh, "Analysis and review of encryption and decryption for secure communication," *International Journal of Scientific Engineering and Research (IJSER),* Vol. 2, 2014.

[3] B. Nithya and D. P. Sripriya, "A review of cryptographic algorithms in network security, "*International Journal of Engineering And Technology (Ijet) Vol*, vol. 8, 2016.

[4] A. G. N. K. Walia, "Cryptography Algorithms: A Review, "*International Journal of Engineering Development and Research*, 2014.

[5] Z. Hercigonja, "Comparative Analysis of Cryptographic Algorithms," *International Journal of Digital Technology & Economy, V*ol. 1, pp. 127-134, 2016.

[6] https://www.manomayasoft.com/blog/item/163-encryption-and-decryption-algorithm (Accessed on, Apr 15, 2018).