International Journal of Research in Engineering, Science and Management
Volume 4, Issue 11, November 2021
https://www.ijresm.com | ISSN (Online): 2581-5792

Cryptographic Techniques on Network Security

Dhruti Patel[1*], Darsh Patel[2], Vatsal Patel[3], Amit Ganatra[4]
[1,2,3]*UG Student, Department of Computer Science and Engineering, Devang Patel Institute of Advance Technology and Research, Charotar University of Science and Technology, Changa, India*
[4]*Principal, Devang Patel Institute of Advance Technology and Research, Charotar University of Science and Technology, Changa, India*

***Abstract*: In modern world with the advance of technology, Information Security becomes a top priority for everybody who uses the internet. The data security in that it can be linked safely and quickly across the internet via digital file transmission. Encryption is the process of transforming plain information into decrypted material that is difficult for unintended receivers to decipher. To secure data, a variety of encryption algorithms are accessible, each with different degrees of intensity, performance, and consumption of resources. Thus, selecting the appropriate algorithm for specific application is challenging task. This paper is a study review of some symmetric and asymmetric cryptographic techniques.**

***Keywords*: encryption, cipher, symmetric algorithms, asymmetric algorithms, information security.**

1. Introduction

The research and art of changing communications to make them safe and resistant to assaults by unauthorized users is known as cryptography. Encryption process refers to the actual information before it is altered. Encryption is the method of converting plain text to cipher text, while decryption is the way of transforming cipher text back to its original form. The transmitter converts plain text to cipher text, while the receiver converts cipher text back to plain text using a decryption method. As a result, it aids in data transfer security and protection from unauthorized users [5], [7].

For certain purposes, data security is a critical concern. Have the highest importance, such as digital commerce, e-mail, health records, and many others, all of which necessitate the transmission of personal information. Improving the work's privacy, legitimacy, and dependability necessitates a significant amount of effort to reinforce present techniques in the face of continual attempts to breach them and to develop models that are immune to the majority, if not all, types of assaults.

Symmetric key cryptography and Asymmetric key cryptography are the two major types of cryptography. The only key is used to transfer data from the sender to the receiver in symmetric key cryptography. It employs a private key and a secret key, which might be a number, a word, or a string. To use this strategy, both the sender and the recipient must have the same key. In this form of encryption, block ciphers and stream ciphers are the two most prevalent modes of operation. Block ciphers deal with groupings of bits known as blocks, which are processed several times. The blocks are transformed into fixed-length blocks of plain text in block chippers. Each round, the key is placed in a different way. Stream ciphers, unlike block chippers, work on one step at a time, encrypting data by splitting it into tiny single bits. This is accomplished by the use of a bitwise XOR technique [8], [9].

Two different types of keys are used in Asymmetric key cryptography: one is used to encrypt the plain text and the other is used to decode the cipher text. The key used for encryption is known as an open key, and it may be broadcast by the owner to others, whereas the key used for decryption is called as the private key, and that is only accessible by the legitimate user.

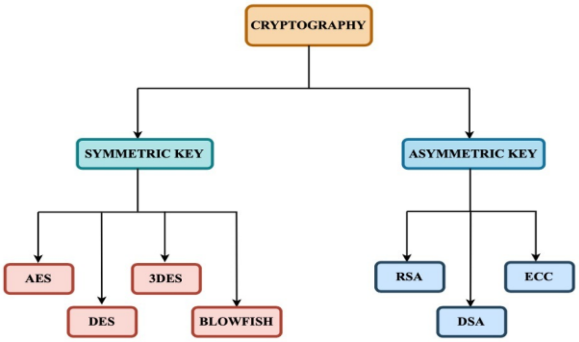

Fig. 1. Classification of encryption algorithms

The cryptography purpose is Authentication systems aid in the verification of identities. This procedure guarantees that the message's source is appropriately recognized. Only the originator and the intended receiver must be able to handle the data of a communication, according to the concept of secrecy. The allocation principle argues that assets should always be accessible to authorized parties. The security mechanism assures that the message's components are the same as they were when it was transmitted to the intended receiver who can contact the operation is specified and controlled by access control.

2. Literature Survey

[1] Omar G. Abood, Shawkat K. Guirguis they mainly discussed on various key in order to undertake a comparative

*Corresponding author: dhrutipatel0111@gmail.com analysis of the most common algorithms in terms of information security efficacy, key size, complexity, and length, among other characteristics, researchers looked at algorithms used for data encryption and decryption in a number of fields. This study looked into a variety of encryption algorithms, including AES, TDES, RSA, DSA, DES, ECC, EEE, and CR4, among others.

[2] Yahia Alemami, Mohamad Afendee Mohamed, Saleh Atiewi classified on security is essential for maintaining information privacy and confidentiality. To safeguard data while storage or transmission, a variety of encryption algorithms are accessible. The strength, speed, and consumption of resources of several encryption algorithms varies. The goal of this research is to offer the most prominent and fascinating algorithms in use today.

[3] A. Joseph amalraj, J. John Raybin Jose, most email services use Public Key Infrastructure (PKI) as the method for implementing security to increase effectiveness and safety, although PKI-based systems have costly certificate administration and scalability issues. The major goal of this strategy is to raise knowledge of email security and its needs among standard computer users. For encrypted communication, a variety of cryptographic approaches have been developed. The suggested mailing system is secure according to industry standards.

[4] Sujatha K, D. Ramya Devi Kala Rathinam D, certain networks might be private because they actually occur within an organization. Compression is a method of lowering the number of bytes or bits used to describe information. Network security is utilized in a variety of industries, including govt agencies, organizations, businesses, banks, and other businesses. Certain techniques have been used in cryptography continue providing information security. The spoke about cryptographic concepts, cryptosystem types, and cryptographic models and algorithms in this article. It's all about maintaining the confidentiality, verification, and consistency while accessing sensitive information.

[6] Mahmud Hasan, Md. Navid Bin Anwar, Jafrin Zafar Loren, Md. Mahade Hasan, and S. M. Tanjim Hossain, cryptographic techniques are vulnerable to a variety of assaults, including brute force, man-in-the-middle, and cycle attacks, all of which are still treated as threads. This study evaluates the role of several cryptographic algorithmic by using performance measures and threads, and determines the best algorithms for several sorts of activities.

3. Cryptography Algorithms

A. *Symmetric Cryptography Algorithms*

To convey data from transmitter to the receiver, symmetrical cryptography techniques employ just one key. It makes use of a private key and a secret key number that might be a value, a character, or a string. In this part, several types of symmetric algorithms are described separately in respect of their functional blocks, benefits, and drawbacks. The below Figure 2 shows about the working of the symmetric cryptosystem. There are four types of algorithms namely AES, DES, 3DES, BLOWFISH [11].

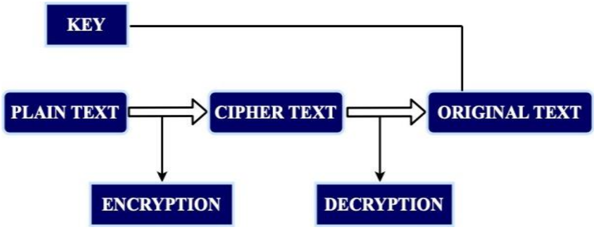

Fig. 2. Block diagram of symmetric cryptosystem

1) *Advanced encryption standard algorithm*

The Advanced Encryption Standard (AES) is the most powerful and widely used symmetric encryption algorithm currently available. In terms of discovering, it is at least six times quicker than triple DES. A replacement was required because the key size of DES was too tiny. It was assumed that as processing power rose, it would be vulnerable to a massive relevant search onslaught. Triple DES was created to address this problem. However, it was discovered to be sluggish. Some of AES's qualities are as follows: Block cipher with symmetrical blocks, symmetric key, 128-bit data, 128-192-256-bit keys. Triple-DES is a more powerful and quicker encryption algorithm. The whole set of requirements as well as design specifications should be provided. Software written in Java and C [12].

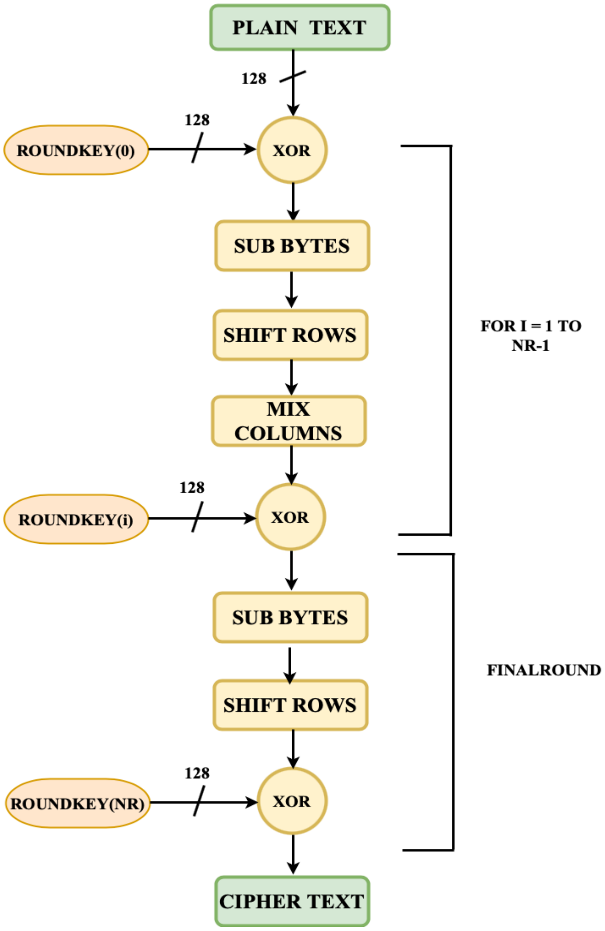

Fig. 3. AES algorithm flowchart

AES is an adaptable cipher instead of a Feistel cipher. A modification network is used. It is made up of a series of interconnected operations, some of which involve the substitution of defined outcomes for had before and others which involve shifting bits about. Interestingly, instead of bits, AES executes all of its operations in bytes. As an outcome, 128-bits of plaintext are treated as 16 bytes by AES. For matrix computing, these 16 bytes are partitioned into four columns & four rows. Unlike DES, the number of repetitions in AES may be customized and is determined by the key size. AES uses 10-128-bit keys, 12-192-bit keys, and 14-256-bit keys. The work flow of the AES algorithm shows in below Figure 3.

2) Data Encryption Standard Algorithm

The Data Encryption Standard's credibility has decreased since it was proven to be vulnerable to incredibly powerful attacks. DES is a block cipher that encrypts 64-bit frame of data. This implies DES takes 64-bits of plain data and converts it to 64-bits of encrypted text. With minor differences, encryption and decryption use the same technology and key. The key has a length of 56-bits.

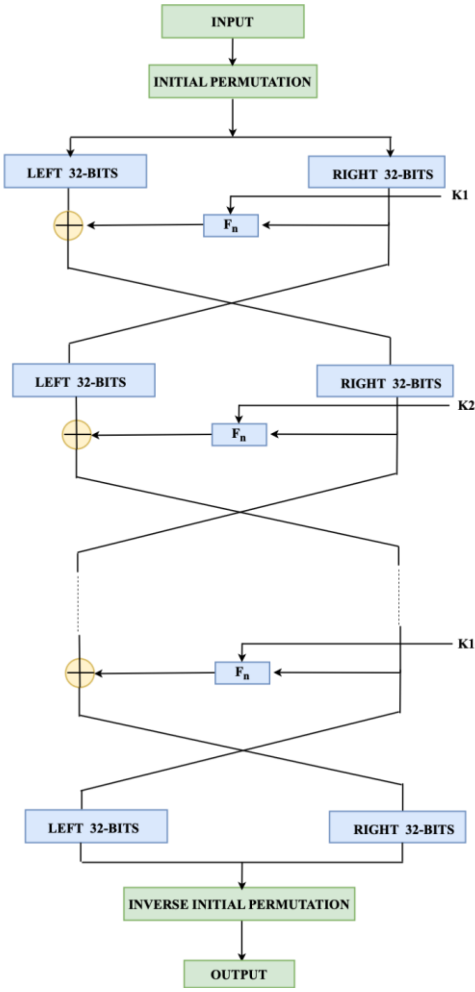

Fig. 4. DES algorithm flowchart

As a result, taking away the eighth-bit of a 64-bit key yields a 56-bit key. Replacement and permutation are two cryptographic basics that DES is founded on. The DES algorithm is divided into 16 phases, each of which is referred to as a round. Each round involves replacement and re-organization.

The plain 64-bit text block is given over to a permutation function at the starting stage. The first variation is done with simple text. Following that, the permutation first generates half of the subset block, represented as Right Plain Text, Left Plain Text. Each LPT and RPT now through a 16-round method of encryption. Finally, LPT and RPT are reconnected, and the united a final permutation is applied to the block. As a consequence of this procedure, 64-bit encrypted text is generated. The work flow of the DES algorithm shows in below Figure 4.

3) Triple Data Encryption Standard Algorithm (TDES)

Triple DES is a type of encryption that uses three DES copies to encrypt the same data. It uses many key selection methods: in first, all keys are unique, in the second, 2 keys are same and one is distinct, and in the third, all keys are almost same. Despite the fact that Triple DES is vulnerable to an encounter attack, it employs a 21112 full security grade instead of a 168-bit key. A block smash technique is also viable due to the evident tiny block size and the usage of the very same key to encrypt large quantities of data. It's also prone to a sweet32 attack.

Before employing TDES, users first step to produce and share a key, which is made up of three DES keys. This indicates the real TDES key is 168-bits long. The following is an illustration of the encryption technique: With one DES to encrypt the textual chunks. Decrypt the result of step-1 and by single DES uses K2. Furthermore, with single DES, secure the output of step-2 with key K3. The output of step-3 is the cipher text. Decryption is the second method of decrypting a cipher text. K3 is used to decrypt, followed by K2 to encrypt, and finally K1 to decrypt. The work flow of the 3DES algorithm shows in below Figure 5.

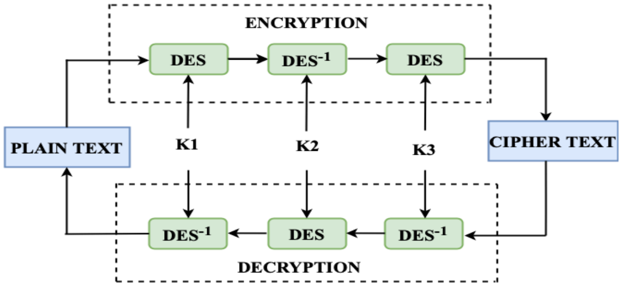

Fig. 5. 3DES algorithm flowchart

4) BLOWFISH Algorithm

Blowfish is a cryptographic algorithm created by Bruce Schneier in 1993 as a replacement for the DES Encryption Method. It is substantially quicker than DES and has a decent encryption efficiency, despite the fact that no viable cryptanalysis approach has been discovered too far. It's one of the earliest secured block ciphers that isn't subject to any copyrights and hence may be used by anybody [17].

There are few steps involved in this algorithm. Firstly, the generation of subkeys in encryption, encryption and decryption processes are both performed. need 18 subkeys, and it utilized with same subkeys for both. Each array member is a 32-bit entry, and these 18 subkeys are kept in a P-array. The figures of pi(Π) are used to start it. P [0] = "24sd48re", P [1] = "58gb1g4t5" is the hexadecimal expression of every one of the subkeys. Each subkey is now altered in relation to the input key. The resulting P-array has 18 subkeys, which are used around the encryption process. Secondly, initialization of substitution boxes, in both the encryption and decryption processes, 4 replacement S-boxes are needed, each containing 256 entries, where each item is 32-bit. The installation of P-array completes, it is populated with the numbers of pi(Π).

Finally, there are two parts to the encryption function: Rounds, the encryption is separated into 16 rounds, each uses the plaintext from the previous round as well as the subkey that matches it (Pi). The coming one's are quick rundown of each round. The function F is described here. Addition mod 232 is the expression "add" in this case. Post-processing: Just after 16 cycles, the output is analyzed. The work flow of the Blowfish algorithm shows in below Figure 6.

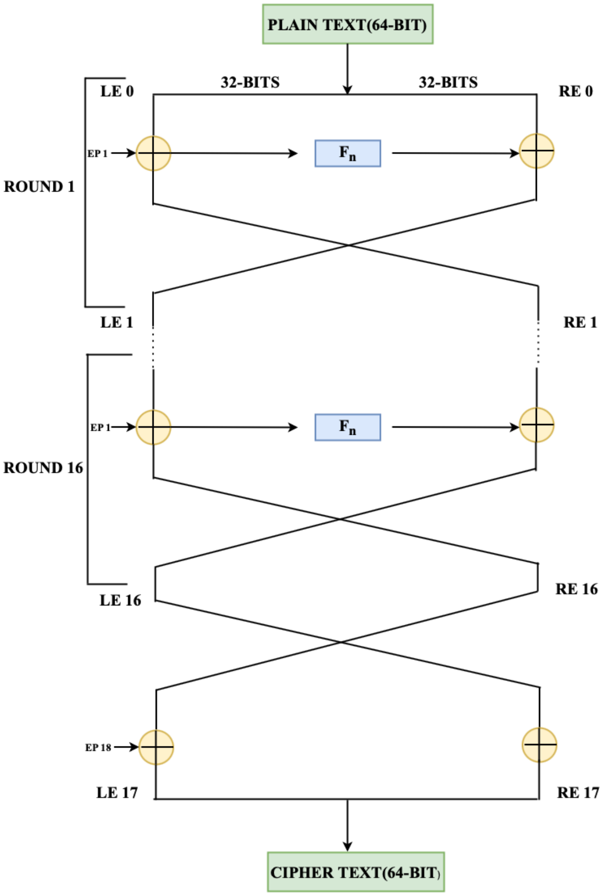

Fig. 6. Blowfish algorithm flowchart

B. *Asymmetric Cryptography Algorithms*

Two different types of keys are being used in asymmetric key cryptography: the first is used to encrypt the plain text and the other is used to decipher the cipher text. The information used for encryption is known as the public key, and it may be broadcast by the proprietor to others, whereas the key used for decryption is referred as the private key, and it is only known by the legitimate user. Examples Asymmetric cryptography are bob sends the server to the public key and asks certain information. The host encrypts data and delivers to the customer using the public key of the client. This signal is obtained by Bob, who decrypts it. Even if a third party has access to the address bar public key, no one else can decode the data. The below Figure 7 shows about the working of the symmetric cryptosystem. There are three types of algorithms namely RSA, DSA, ECC [10].

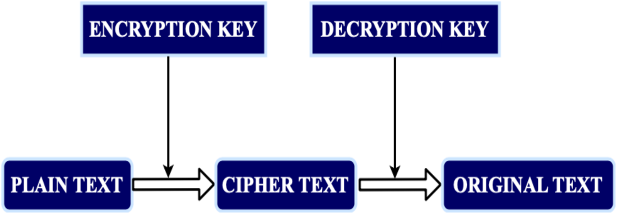

Fig. 7. Block diagram of asymmetric cryptosystem

1) *RSA Algorithm*

RSA is an acronym for Rivest-Shamir-Adleman. It's a type of cryptosystem that allows for safe data transfer. The encryption key is known in the RSA algorithm, while the decryption key is confidential. The notion that factoring the product of the two huge prime integers is difficult is the basis for this approach. Adi Shamir, Ron Rivest, and Leonard Adleman created it in 1977 [16].

Asymmetric encryption is a kind of encryption that uses the Cryptographic algorithms. Because it employs two independent keys: A Private Key and a Public Key it is asymmetric. The Public Key is shared with everyone, but the Secret Key, as the name propose, is kept private. The RSA principle is found on the notion that scaling a large integer is hard. Two integers make up the public key, one being the product of simply multiplying extremely large prime numbers. Private key is also made up of same prime numbers. As a result, the secret key is disclosed if the big number can be factoring. When a result, encryption intensity is solely reliant on key size, and encryption strength keeps growing as key size is roughly doubled. RSA keys are typically 1024 or 2048-bits long, although they can be longer analysts agree that 1024-bit keys will be cracked shortly. Unfortunately, at this movement, it looks to be an impossibility.

Either sector and allow and digital signatures may be done using RSA. The effectiveness of encryption is entirely dependent on key size, this might result in a doubling or triple of the key size. improves encryption strength significantly. The work flow of RSA algorithm shows in below Figure 8.

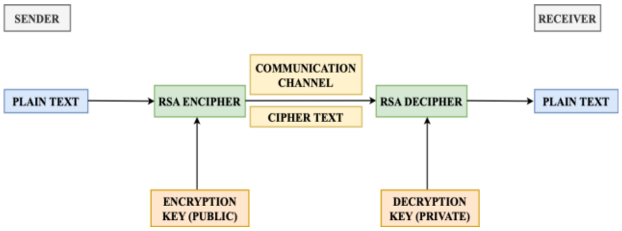

Fig. 8. RSA algorithm flowchart

2) *Digital Signature Algorithm (DSA)*

DSA is the abbreviation for Digital Signature Algorithm. It is used to verify and create digital signatures. It is based on the modular exponentiation and discrete logarithm mathematical concepts. The NIST created it in 1991. It entails four procedures: Generation of keys, distribution of keys, signing, and verification of signatures [15].

The following are three advantages of the DSA Algorithm: Message Authentication: Using the correct key combination, you may authenticate the user's origin. Authenticity Verification: Tampering with the signal will prohibit the package from being encrypted in the first place. Non-repudiation: If the transmitter confirms the signatures, they cannot argue they didn't send the communication. The DSA algorithm's whole method is depicted in the graphic above. Here, you'll need two separate functions: one for signing and one for verifying. The encryption and decryption component of a common digital signature authentication method differs.

Steps involved in this algorithm is key generation, Signature generation, and Signature Verification. The work flow of the DSA algorithm shows in below Figure 9.

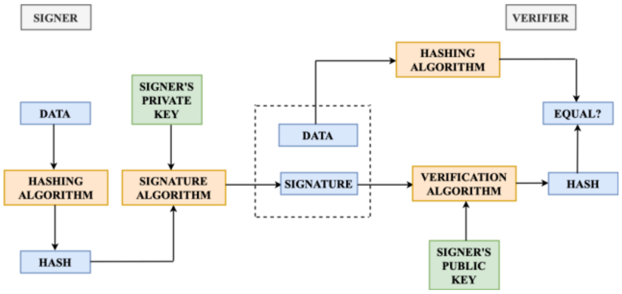

Fig. 9. DSA algorithm flowchart

3) *Elliptic Curve Cryptography Algorithm*

Elliptic Curve Cryptography is a new public-key encryption system that is lighter, quicker, and more effective than its predecessors. Because ECC is so lightweight, Bitcoin, for instance, employs it as its asymmetric cryptosystem. The elliptic curve is the mathematical structure that enables all of this feasible, so keep reading to understand how well these curves allow a few of the world's most powerful encryption. Encrypting data so that only authorized entities may decrypt it is a popular application of ECC. This has a variety of applications, although it is most typically used to encrypt Online communication. In the Qvault web app, for instance, I could use ECC to encrypt an email confirmation because only the receiver could access it [14].

ECC is one of several different kinds of public-key cryptography. RSA, Diffie-Helman, and other techniques are examples. Let's begin with a high-level summary of public-key cryptography as a foundation for discussing ECC and building on these concepts. When you have the opportunity, go into public-key cryptography in deeper level. We can do the following using public-key cryptography: A public key and a private key are generated. The public key is made available to the general audience., and anybody may use it to encrypt data. The private key, on the other hand, is shrouded in secrecy, but only those who possess it will be able to decode data.

It is centered on the elliptical curve theory, which may be used to construct cryptographic keys that are quicker, less, and much more efficient. The elliptic equation is used to generate the key. Mobile apps make extensive use of this technology. In 2004, elliptic encryption methods were widely used. y2=x3+ax+b is the equation for an elliptic curve. It achieves the same amount of safety by using smaller keys. Smaller keys are crucial, especially in an environment where enough encryption is performed on less capable devices such as smartphones. Elliptic curve cryptography is presently employed in a range of applications, including the US government's internal documents and the Tor program's invisibility.

4. Performance Analysis

On the basis of numerous performance indicators, the

Table 1
Performance analysis of symmetric cryptography algorithms

Algorithm	Proposed by	Year	Key Size (bits)	Block Size (bits)	Round	Security	Efficiency	Features
AES	Joan Daeman and Incent Rijmen	1998	128, 192, 256	128	10, 12, 14	Mostly secure	Fast	The level of security is outstanding. It performs the best in terms of security and encryption.
DES	IBM	1975	64	64	16	Inadequate	Slow	Not Strong Enough
3DES	NIST	1977	112, 16, 8	64	48	Adequate security	Fast - hardware Slow - software	Symmetric-key block cipher
BLOWFISH	Bruce Schneier	1993	32-448	64	16	Royalty free	Fast	Fast Cipher in SSL

Table 2
Performance analysis of asymmetric cryptography algorithms

Algorithm	Proposed by	Year	Key Size (bits)	Block Size (bits)	Round	Security	Efficiency	Features
RSA	Rivest Shamir Adleman	1977	1024-4096	128	1	Medium level	Slow-hardware (decryption)	Low Speed with Excellent Security
DSA	NIST	1997	56	64	-	Mostly	Slow	Good Security and fast speed
ECC	Neal Koblitz and Victor Miller	1985	More than symmetric and variable	Variable	1	Mostly	Slow	Excellent security and fast speed

execution results of various symmetric and asymmetric algorithms are analyzed. These measures are used to determine which approach outperforms the others. The Table 1 shows the comparison among all algorithms in Symmetric Cryptography, Table 2 illustrates the differentiation of three algorithms in Symmetric Cryptography which was explained in this paper. The performance parameters listed below are examined are Key size, block size, round, security, efficiency, features.

From the above tables, it showcases the AES, TDES, Blowfish are swiftly in speed, encryption, flexibility. The findings also suggest that the AES method is the most secure, flexible, and effective in terms of encryption. When compared to alternative, this is the most effective.

5. Conclusion

In this work, a thorough examination of the effectiveness of several cryptographic techniques is carried out in order to decide which approach is optimal for a certain area of practice. Cryptography is one of the most important components to provide security to data communication between networks. From our study we cannot conclude which particular cryptography technique or algorithm is most efficient because it depends on various parameters and applications, but we may infer that symmetric cryptography algorithms like AES, BLOWFISH, DES, and 3DES are better ideal for applications like wireless technology, J-File, image recognition, smart cards, and e-commerce. Asymmetric encryption schemes like RSA, DSA, and ECC, on either hand, are the ideal choice for developing like Online banking, online apps, email authentication, and key distribution over the mobile and web. Cryptography will continue to be employed in IT and corporate strategy to protect individual, commercial, healthcare, and retail data while retaining a fair level of anonymity.

References

[1] Omar G. Abood, Shawkat K. Guirguis, "Survey on Cryptography Algorithms," in International Journal of Scientific and Research Publications, vol. 8, no. 7, pp. 495-516, July 2018.

[2] Yahia Alemami and Mohamad Afendee Mohamed, Saleh Atiewi, "Research on Various Cryptography Techniques, in International Journal of Recent Technology and Engineering, July 2019.

[3] A. Joseph Amalraj and J. John Raybin Jose, "A Survey Paper on Cryptography Techniques," International Journal of Computer Science and mobile computing, July 2016.

[4] K. Sujatha and D. Ramya Devi Kala Rathinam, "A Review Paper on Cryptography and Network Security," in International Journal of Pure and Applied Mathematics, vol. 119, no. 17, pp. 1279-1284, 2018.

[5] A. M. Qadir and N. Varol, "A Review Paper on Cryptography," 2019 7th International Symposium on Digital Forensics and Security (ISDFS), 2019, pp. 1-6.

[6] Md. Navid Bin Anwar, Mahmud Hasan, Md. Mahade Hasan, Jafrin Zafar Loren and S. M. Tanjim Hossain, "Comparative Study of Cryptography Algorithms and it's Applications," in International Journal of Computer Networks and Communications Security, vol. 7, no. 5, pp. 96-103, May 2019.

[7] K. Vanitha, K. Anitha, A. M. J. Md. Zubair Rahaman, M. Mohamed Musthafa, "Analysis of Cryptographic Techniques in Network Security," in Journal of Applied Science and Computations (JASC), August 2018.

[8] Biryukov, A., & Perrin, L. P. (2017). State of the art in lightweight symmetric cryptography.

[9] Szerwinski, R., & Güneysu, T. (2008, August). Exploiting the power of GPUs for asymmetric cryptography. n *International Workshop on Cryptographic hardware and embedded systems* (pp. 79-99). Springer, Berlin, Heidelberg.

[10] Patarin, J. (1996, August). Asymmetric cryptography with a hidden monomial. In *Annual International Cryptology Conference* (pp. 45-60). Springer, Berlin, Heidelberg.

[11] Thakur, J., & Kumar, N. (2011). DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis. *International journal of emerging technology and advanced engineering*, *1*(2), 6-12.

[12] Mahajan, P., & Sachdeva, A. (2013). A study of encryption algorithms AES, DES and RSA for security. *Global Journal of Computer Science and Technology*.

[13] Han, S. J., Oh, H. S., & Park, J. (1996, September). The improved data encryption standard (DES) algorithm. In *Proceedings of ISSSTA'95 International Symposium on Spread Spectrum Techniques and Applications* (Vol. 3, pp. 1310-1314). IEEE.

[14] Shankar, K., & Eswaran, P. (2016). An efficient image encryption technique based on optimized key generation in ECC using genetic algorithm. In *Artificial intelligence and evolutionary computations in engineering systems* (pp. 705-714). Springer, New Delhi.

[15] Gennaro, R., Goldfeder, S., & Narayanan, A. (2016, June). Threshold-optimal DSA/ECDSA signatures and an application to Bitcoin wallet security. In *International Conference on Applied Cryptography and Network Security* (pp. 156-174). Springer, Cham.

[16] Zhao, G., Yang, X., Zhou, B., & Wei, W. (2010, July). RSA-based digital image encryption algorithm in wireless sensor networks. In *2010 2nd International Conference on Signal Processing Systems* (Vol. 2, pp. V2-640). IEEE.

[17] Abdul Kareem Nasser, M., & Abduljaleel, I. Q. (2013). Speech encryption using chaotic map and blowfish algorithms. *Journal of Basrah Researches (Sciences)*, *39*(2A).