Performance Evaluation of Hybrid Cryptography Algorithm for Secure Sharing of Text & Images

Pooja Patil[1], Dr. Rajesh Bansode[2]

[1]*ME Student, Dept. of Information Technology, Thakur College of Engineering & Technology, Maharashtra, India*
[2]*Professor, Dept. of Information Technology, Thakur College of Engineering & Technology, Maharashtra, India*

Abstract - *Nowadays, the networks have gone global and information has taken the digital form. Since, large amount of data transferred over the internet, data security becomes challenging issue. Symmetric & asymmetric cryptographic techniques used today for hiding any confidential information from an intruder. Cryptography provides integrity, confidentiality, non-repudiation and authenticity to the secret data. A hybrid cryptography is a mixture which focuses primarily on blending together the facilities of asymmetric cryptography with the effectiveness of symmetric cryptography which enhances the security level. The proposed hybrid method is the combination of symmetric algorithm (AES), asymmetric algorithm (ECC) & hash function (SHA256). Here, SHA-256 is a mathematical function that is run on digital data. It is used to verify the integrity of data. Proposed hybrid method is compared with existing method which uses AES algorithm for text and image encryption. The proposed method is more efficient in case of text encryption if compared with above existing method. Image encryption of proposed method is less efficient than above existing method. Encryption and decryption time for image can be reduced in future work.*

Key Words: **AES, Cryptography, Decryption, ECC, Encryption, SHA256**

1. INTRODUCTION

The high growth in the networking technology leads a common culture for interchanging of the data very drastically. Since, large amount of data transferred over the internet, data security becomes challenging issue. There is a need of security to guard such data which communicates on unsecure channel.

Cryptography, a word with Greek origins, means "secret writing". The message to be sent through an unreliable medium is known as plaintext, which is encrypted before sending over the medium. The encrypted message is known as cipher text, which is received at the other end of the medium and decrypted to get back the original plaintext message [1]. The working of encryption and decryption is shown in figure 1 [2]. The figure 1 states that sender encrypts the message using secret key and send it through the communication channel. Receiver decrypt the message using the secret key. Cryptography provides a number of security goals to ensure the privacy of data, non-alteration of data and so on. Due to the great security advantages of cryptography it is widely used today [3].

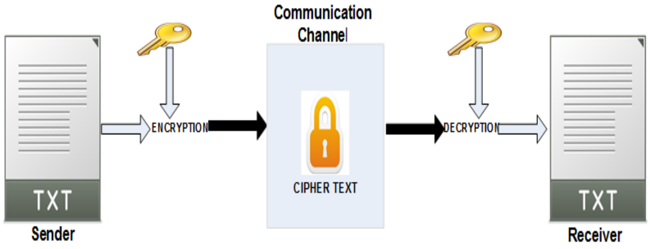

Fig-1: Working of encryption and decryption

Cryptography algorithms can be divided into two broad categorizes: Symmetric key cryptography and Asymmetric key cryptography [1].

1.1 Classification of cryptography

A. Symmetric Key Cryptography

Symmetric algorithm is also called shared key cryptography. During data transmission, the sender and the receiver share the same key for encryption and decryption [4]. There are different types of symmetric algorithms like Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), Advanced Encryption Standard (AES) and Blowfish [5].

B. Asymmetric Key Cryptography

Asymmetric Algorithm is also called public key cryptography. It uses two keys 'Private key' and 'Public key'. During data transmission, the sender encrypts the plain text with the help of public key known as the cipher text and the receiver decrypts this cipher text with the help of its private key [4]. The different types of asymmetric algorithms are Rivest Shamir Adlemen (RSA), Diffie Hellman (DH) and Digital Signature Algorithm (DSA), ECC [5].

1.2 Hybrid Cryptography

The concept which combines the both symmetric and asymmetric cryptographic techniques is known as hybrid cryptography. A hybrid cryptosystem is a protocol using symmetric and asymmetric cryptographic technics together, each to it's best advantage. Hybrid encryption is considered a highly secure type of encryption as long as the public and private keys are fully secure. Hybrid cryptography is achieved through data transfer using unique session keys along with symmetrical encryption. Public key encryption is implemented for random symmetric key encryption. The recipient then uses the public key encryption method to decrypt the symmetric key. Once the symmetric key is recovered, it is then used to decrypt the message [6].

1.3 Hash Function

Cryptographic hash function is a mathematical function which maps data of arbitrary size to data of fixed size. The values returned by hash function are called as hash values, hash codes, hash sums or simply hashes. Only two families of hash functions came to be used widely (namely the MD and SHA families). These functions provide certain security properties and play a key role in building various security applications related to digital signatures, authentication and message integrity [7].

2. LITERATURE SURVEY

In paper [1], A comparative study of encryption techniques in terms of symmetric key and asymmetric key algorithms analyzed. In the symmetric key encryption AES algorithm is found to be better in terms of cost, security and implementation. In asymmetric key encryption RSA algorithm is better in terms of speed and security.

In paper [2], different types of symmetric and asymmetric algorithms are explained. Symmetric algorithms include DES, 3DES, AES. Asymmetric algorithms include RSA & Elgamal. The performance results show that the symmetric schemes are computationally inexpensive when compared with asymmetric schemes.

In paper [3], the existing encryption techniques are studied and analyzed to promote the performance of the encryption methods also to ensure the security proceedings. All the techniques are useful for real-time encryption. Each technique is unique in its own way, which might be suitable for different applications.

In Paper [4], a comparative study of different key algorithms like, AES, DES, 3DES, Blowfish and RSA are analyzed and compared. From the results it has been found that among the symmetric encryption algorithm, AES and Blowfish are the most secure and efficient algorithms. The speed and power consumption of these algorithms are better compared to the others. In case of asymmetric encryption algorithm, RSA is secure and can be used for application in wireless network because of its good speed and security.

In paper [5], the traditional algorithms are discussed. Symmetric cryptography utilizes a single key to achieve encryption and decryption which could rise security issues. Asymmetric Key Cryptography uses two separate keys to prevent any unethical access to the data. One key remains private while the other is available in the public key repository. The latter provides more security than the former. Still symmetric cryptographic techniques are preferred for their simpler description and less requirement of resources.

In paper [6], Hybrid encryption system is proposed. This is the one which combines convenience of public key cryptosystem with the efficiency of symmetric key cryptosystem. The proposed hybrid encryption algorithm provides more secure and convenient technique for secure data transmission for all kind application.

In paper [7], cryptographic hash functions are discussed. These functions provide certain security properties and play a key role in building various security applications related to digital signatures, authentication. And message integrity. This paper emphasizes on cryptographic hash function families, compression functions and formal terminology.

In paper [8], the main objectives of cryptography are explained such as Confidentiality, Integrity, Non-repudiation, Authentication, Access Control. Various cryptographic algorithms analysed such as DES, 3DES, ECC, RSA, BLOWFISH, AES on the basis of performance parameters. It is concluded that ECC & BLOWFISH provides better security with high speed.

In paper [9], AES based text encryption is explained. AES is a symmetric block cipher system which uses replaces or exchange network. The data block length and key length of AES can be varied according to the requirement. Three key lengths: 128, 192, 256, whose iteration cycle number is 10, 12 and 14 round respectively, are used.

In paper [10], encryption and decryption of text using AES is explained. The proposed algorithm offers high encryption quality rather than other standards. There is currently no evidence that AES has any weaknesses making any attack other than exhaustive search, i.e. brute force. It provides security to multiple accounts, multiple files which have confidential data.

In paper [11], Image encryption and decryption is performed using AES algorithm. It is implemented to secure the image data from an unauthorized access. The original images can also be completely reconstructed without any distortion. It is concluded that it has extremely large security key space & can withstand with attacks like the brute force attack, cipher attacks and plaintext attacks.

In paper [12], AES algorithm to encrypt and decrypt the image and text. It makes use of 128 bit key for encryption which makes AES secure and faster than DES. As the key size is larger, it helps to overcome several attacks such as brute force attack and man in the middle attack.

In paper [13], ECC is explained in detail. Elliptic curve cryptography (ECC) is a relatively newer form of public key cryptography that provides more security per bit than other forms of cryptography still being used today.

In paper [14], encryption and decryption of text using ECC is explained with mapping technique. It is concluded that ECC has low power consumption, less memory requirement, small key size and high security.

In paper [15], Image encryption and decryption using ECC algorithm is implemented to encrypt, decrypt and digitally sign the cipher image to provide authenticity and integrity.

In paper [16], the ECC algorithm is proposed to compute secret key value without sharing in network. Encryption and decryption operation is performing based on block cipher of coordinate system. The proposed system can avoid chosen plaintext attacks, man-in-the-middle attacks etc.

In paper [17], hybrid cryptography technique using AES and ECC is proposed. The system is intended to provide security to a variety of multimedia data ranging from text documents, images, audio, video. Proposed hybrid system capable of encrypting and decrypting the sensitive data to protect it from unauthorized access and attacks.

In paper [18], hybrid cryptography approach implemented using AES and ECC. This system provides encryption to the multimedia data such as text, image, audio, video which resulted in an output with 100 percent accuracy without any loss of information.

In paper [19], Different text files are taken as input and encrypted using AES-ECC hybrid approach. Analysis of AES encryption with ECC is done on the basis of different parameters like storage requirement, encryption time, decryption time.

In paper [20], hybrid approach for encryption technique is implemented over a binary image, which provides more accuracy to the encryption process. The ECC and AES are combined in such a way that differentiates them from the usual manner of encryption. These days with the increasing trend of security it becomes essential to protect the data and information in a better way.

In paper [21], SHA1 and MD5 algorithms are explained in detail. It is concluded that SHA1 is more faster than MD5, and SHA2 is even more secure than SHA1 and MD5. Hash functions can be implemented with hybrid cryptography to improve performance & security in future.

In paper [22], review is written about various cryptographic hash algorithms and the fundamental rationale behind them. Hash value is maintained by using different hashing algorithm in different situation to check whether the message is modified or not. Which algorithm is more suitable for the particular message is discussed.

In paper [23], the detailed design of hash function MD5, SHA1, SHA2, SHA3 is provided. Different parameters are Hash functions are analysed by comparing with each other.

In paper [24], working of SHA-256 is explained. SHA-256 is a mathematical function that is run on digital data. Computed hash is compared to an expected hash value to verify the data's integrity.

3. PROBLEM DEFINITION

Cryptographic techniques provides the secure data transmission, but there are some complexities in existing systems. Most of the cryptographic techniques are time consuming processes. Some techniques does not includes the integrity checks on transmitted data. Another issue is lack of security during key exchange. In order to implement an effective cryptographic algorithm all these aspects has to be considered in order to make it robust. There is need to implement the technique which helps to overcome such complexities in such existing system.

The Proposed hybrid cryptographic technique which uses the best features of symmetric (AES) and asymmetric (ECC) cryptographic technique with hash function (SHA256). So that, this technique helps to reduce the time complexity. Also, provides authentication and the validation of data integrity.

4. DESCRIPTION OF ALGORITHMS

4.1 Advanced Encryption Standard (AES)

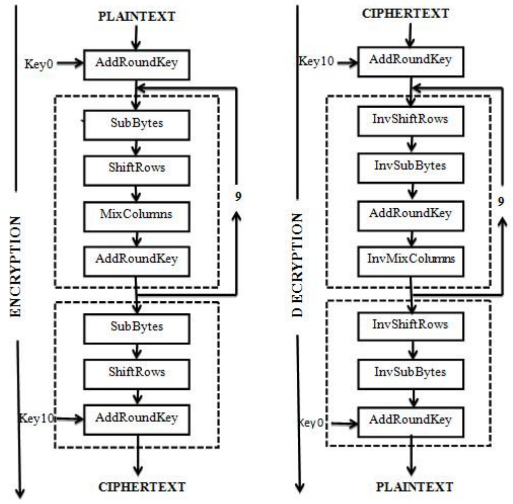

Fig-2: AES encryption & decryption process

AES is a symmetric block cipher system which uses replaces or exchange network. The data block length and key length of AES can be varied according to the requirement. Three key lengths: 128, 192, 256, whose iteration cycle number is 10, 12 and 14 round respectively, are used. The AES algorithm mainly has three aspects: round change, turns and key expand. Every transformation of round is a collection of a non-linear layer, the linear mixture layer and add round key layer. AES encryption process is shown in Figure 2 [9].

4.2 Elliptic Curve Cryptography (ECC)

Elliptic curve cryptography (ECC) is a relatively newer form of public key cryptography that provides more security per bit than other forms of cryptography still being used today. Mathematically, elliptic curves are cubic curves that are equivalent to tori, topologically. Despite their name, they are not closely related to the ellipse, however they get their name from the elliptic integral. The Weierstrass normal form, the basic general elliptic curve used for cryptography, is of the form $y^2 = x^3 + ax + b$ which is visualised in figure 3. Curves of this form are defined by different values for a and b. By modifying these values, the visualization of the curve can expand, contract, or pinch off to be two separate pieces. Curves used for cryptography, in practice, are often defined with very large integer values for a and b [13].

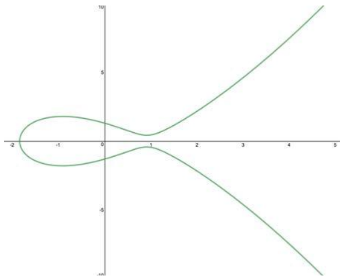

Fig-3: Simple elliptic curve visuallization

4.3 Secure Hash Algorithm (SHA256)

SHA-2 is a set of cryptographic hash functions the variants of SHA-2 are SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256. SHA-2 includes a significant number of changes from its predecessor, SHA-1. SHA-2 currently consists of a set of six hash functions with digests that are 224, 256, 384 or 512 bits.SHA-256 is a mathematical function that is run on digital data. Computed hash is compared to an expected hash value to verify the data's integrity [24].

5. METHODOLOGY

The proposed system consists of two processes such as encryption process and decryption process. It uses symmetric algorithm AES and asymmetric algorithm ECC along with hash function SHA256. All the essential features of these algorithms are made available in proposed hybrid algorithm. Better encryption of AES, most efficient key management by ECC along with the digital signature by making use of SHA-256 are included in a single hybrid system.

5.1 Encryption Process

1. An AES key 'K' of 128-bit, 192-bit or 256-bit is chosen.
2. Encrypt message (M) using AES algorithm and above selected key K.
eM = AES-encryption(M)
3. AES key K is encrypted by making use of ECC algorithm.
eK = ECC-encryption (K)
4. The cipher text (eM) is fed to SHA256 algorithm which generates a message digest of 256-bit.
mD = SHA256 (eM)
5. The encrypted message (eM) and AES encrypted key (eK) is transmitted to the user over a network.
Figure 4 shows the encryption process of proposed algorithm.

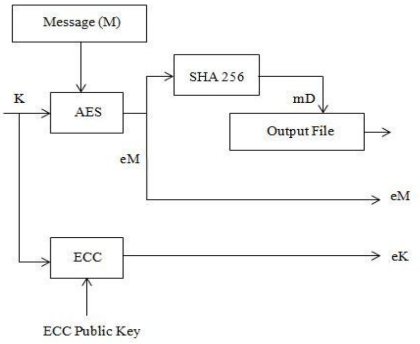

Fig-4: Encryption Process

5.2 Decryption Process

This process is the reverse of encryption process and is having following steps:
1. The encrypted AES key (eK) is decrypted with ECC algorithm.
K = ECC-decryption (eK)
2. Similarly the encrypted message (eM) is decrypted by AES algorithm using key K
M = AES-decryption (eM)
3. The message digest of encrypted message (eM) is computed using SHA256.
mD = SHA256 (eM)
4. Thus we get message (M) of sender.
Figure 5 shows the decryption process of proposed algorithm.

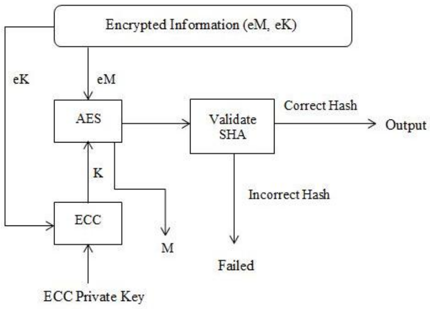

Fig-5: Decryption Process

Proposed hybrid cryptography method is implemented for secure sharing of patient healthcare information on website. Encryption and decryption time taken for different text and image files are calculated. Also, hash matching is performed.

There are following steps:

1. File is uploaded by admin and encryption time is calculated.
2. File is successfully shared with user.
3. User enters the secret key which is sent by the admin to decrypt the file which is received and then decryption time is calculated.
4. After successful decryption, file can be downloaded.

5. To perform hash matching, hash is generated for that file to check whether it is matching with its hash value or not.

6. RESULT AND DISCUSSION

The result obtained from proposed method and is compared with existing algorithm. Different file size of text and image are taken as input to calculate encryption and decryption time. Comparative result is shown in tabular form. Average time for encryption and decryption of given file size is calculated for both existing and proposed method.

6.1 Text Files

The comparisons of text files are done between the existing algorithm and proposed hybrid algorithm. Average time is calculated for both systems. The same data sets are used as inputs for the comparison purpose. This is shown in Table 1 as below.

Table 1 states that average time of encryption and decryption of text files of proposed hybrid method is less than the existing system.

Table -1: Encryption & decryption time of text

File Size (KB)	Reference [12]		Hybrid Method	
	Encryption Time (ms)	Decryption Time (ms)	Encryption Time (ms)	Decryption Time (ms)
20	838	917	49	80
25	911	989	50	82
50	941	1128	57	83
75	1154	1454	65	88
100	1704	2117	71	92
150	1815	2305	88	113
Average Time	1227.16	1484.83	63.33	89.66

6.2 Image Files

The comparison is of image files are done between the existing algorithm and proposed hybrid algorithm. Average time is calculated for both systems. The same data sets are used as inputs for the comparison purpose. This is shown in Table 2 as below.

Table 2 states that average time of encryption and decryption of image files of proposed hybrid method is little bit more than the existing system.

Table -2: Encryption & decryption time of image

File Size (KB)	Reference [12]		Hybrid Method	
	Encryption Time (ms)	Decryption Time (ms)	Encryption Time (ms)	Decryption Time (ms)
20	17	25	51	82
25	21	34	52	85
55	40	58	59	96
75	57	98	66	102
100	77	132	81	113
150	108	188	113	135
Average Time	53.33	89.16	70.33	102.16

7. CONCLUSION

The limitations of various cryptographic techniques are analyzed and hybrid system with hash function is proposed which is the combination of the AES, ECC and SHA256. This methodology implemented for secure sharing of healthcare data. Text and images with different file size are taken as input. Encryption is performed on original file and it sent to the intended receiver. Receiver decrypted that file using secret key and then matching of hash is performed. The successful hash matching indicates that data is not altered. This system performs encryption and decryption for better security of confidential data. It protects the sensitive data from unauthorised access and attacks. It provides authentication, enhanced time and validation of data integrity. So, using this hybrid approach sharing and accessing the data is secure.

REFERENCES

[1] N. Bisht and S. Singh, “A Comparative Study of Some Symmetric and Asymmetric Key Cryptography Algorithms”, Int. J. Innovative Res. Sci. Eng. Technol., Vol. 4, no. 3, pp.1028-1031, Mar. 2015.

[2] F. Maqsood, M. Ahmed, M. M. Ali, and M. A. Shah, “Cryptography: A Comparative Analysis for Modern Techniques”, Int. J. Adv. Comput. Sci. Appl., Vol. 8, no. 6, pp.442-448, 2017.

[3] P. Verma, J. Shekhar, Preety, and A. Asthana, “A Survey for Performance Analysis Various Cryptography Techniques Digital Contents”, Int. J. Comput. Sci. Mobile Comput., Vol.4, no.1, pp. 522-531, Jan. 2015.

[4] Verma, P. Guha, and S. Mishra, “Comparative Study of Different Cryptographic Algorithms”, Int. J. Emerg. Trends Technol. Comput. Sci., Vol. 5, no. 2, pp. 58-63, Mar-Apr 2016.

[5] K. Uma, G. Karthik, and R. V. Prasath, “A comparative analysis of Symmetric and Asymmetric key cryptography”, J. Chem. Pharm. Sci., Vol. 10, no. 1, pp.324-326, Jan-Mar 2017.

[6] P. Kuppuswamy and S. Q. Y. Al-Khalidi, “Hybrid Encryption/Decryption Technique Using New Public Key and Symmetric Key Algorithm”, Manage. Inf. Syst. Rev., Vol. 19, no. 2, pp.1-13, Mar. 2014.

[7] E. Swathi, G. Vivek, and G. S. Rani, “Role of Hash Function in Cryptography”, in National Conference on Computer Security, Image Processing, Graphics, Mobility and Analytics, India, 2016, pp.10-13.

[8] H. Zope and S. Sangam, “Comparative Analysis of Various Encryption Algorithms and Techniques”, Int. J. Res. Appl. Sci. Eng. Technol., Vol. 5, no. 12, pp. 422-427, Dec. 2017.

[9] N. Mathur and R. Bansode, “AES Based Text Encryption Using 12 Rounds with Dynamic Key Selection”, in 7th International Conference on Communication, Computing and Virtualization, 2016, Vol. 79, pp. 1036-1043.

[10] K. K. Saraf, N. Goyal, S. Raokhande, and A. Takale, “Text Encryption and Decryption using AES Algorithm”, Int. J. Electron., Elect. Comput. Syst., Vol. 7, no. 3, pp.638-643, Mar. 2018.

[11] P. Deshmukh, “An Image Encryption and Decryption Using AES Algorithm”, Int. J. Sci. Eng. Res., Vol.7, no.2, pp.210-213, Feb. 2016.

[12] N. S. Rani, A. N. M. Juliet, and K. R. Devi, “An Image Encryption & Decryption And Comparison With Text - AES Algorithm”, Int. J. Sci. Technol. Res., Vol. 8, no.7, pp.668-673, Jul. 2019.

[13] R. Harkanson and Y. Kim, “Applications of Elliptic Curve Cryptography: A Light Introduction to Elliptic Curves and a Survey of Their Applications”, in 12th Annual Cyber and Information Security Research Conference, USA, Apr. 2017, pp.1-7.

[14] K. Keerthi and B. Surendiran, “Elliptic Curve Cryptography for Secured Text Encryption”, in International Conference on Circuits Power and Computing Technologies, India, 2017.

[15] L. D. Singh and K. M. Singh, “Image encryption using elliptic curve cryptography”, in 11th International Multi-Conference on Information Processing, 2015, Vol. 54, pp. 472-481.

[16] S. Banerjee and A. Patil, “ECC Based Encryption Algorithm for Lightweight Cryptography”, in 18th International Conference on Intelligent Systems Design and Applications, India, 2018, Vol.1, pp. 600-609.

[17] S. C. Iyer, R. R. Sedamkar, and S. Gupta, “A Novel Idea on Multimedia Encryption Using Hybrid Crypto Approach”, in 7th International Conference on Communication, Computing and Virtualization, 2016, Vol. 79, pp.293-298.

[18] S. C. Iyer, R. R. Sedamkar, and S. Gupta, “An Efficient Multimedia Encryption using Hybrid Crypto Approaches”, Int. J. Recent Trends Eng. Res., Vol. 2, pp. 442-452, 2016.

[19] S. Sharma and V. Chopra, “Analysis of AES Encryption with ECC,” in International Interdisciplinary Conference On Engineering Science & Management, India, Dec. 2016, pp. 195-201.

[20] Ameta and S. Upadhyay, “A Hybrid Approach for Image Encryption using Different Number Iterations in ECC and AES Techniques”, Int. J. Comput. Appl., Vol. 175, no.3, pp.10-12, Oct. 2017.

[21] S. Aggarwal, N. Goyal, and K. Aggarwal, “A review of Comparative Study of MD5 and SHA Security Algorithm”, Int. J. Comput. Appl., Vol.104, no.14, pp.1-4, Oct. 2014.

[22] M. A. Kale and S. Dhamdhere, “Survey Paper on Different Type of Hashing Algorithm”, Int. J. Adv. Sci. Res. Eng. Trends, Vol. 3, no. 2, pp.14-16, Feb. 2018.

[23] P. P. Pittalia, “A Comparative Study of Hash Algorithms in Cryptography”, Int. J. Comput. Sci. Mobile Comput., Vol. 8, no. 6, pp.147-152, Jun. 2019.

[24] Use cases for hash functions or what is SHA-256? Available:https://medium.com/@makhmud.islamov/use-cases-for-hash-functions-or-what-is-sha-256-83036de048b4, accessed Jan.2020.