Cryptography: A Comparative Analysis for Modern Techniques

Faiqa Maqsood[1]
Dept. Computer Science & Information Technology
Superior University
Lahore, Pakistan

Muhammad Mumtaz Ali[3]
Dept. Computer Science & Information Technology
Superior University
Lahore, Pakistan

Muhammad Ahmed [2]
Dept. Computer Science & Information Technology
Superior University
Lahore, Pakistan

Munam Ali Shah[4]
Dept. Computer Science
COMSATS Institute of Information Technology
Islamabad, Pakistan

***Abstract*—Cryptography plays a vital role for ensuring secure communication between multiple entities. In many contemporary studies, researchers contributed towards identifying best cryptography mechanisms in terms of their performance results. Selection of cryptographic technique according to a particular context is a big question; to answer this question, many existing studies have claimed that technique selection is purely dependent on desired quality attributes such as efficiency and security. It has been identified that existing reviews are either focused only towards symmetric or asymmetric encryption types. Another limitation is found that a criterion for performance comparisons only covers common parameters. In this paper, we have evaluated the performance of different symmetric and asymmetric algorithms by covering multiple parameters such as encryption/decryption time, key generation time and file size. For evaluation purpose, we have performed simulations in a sample context in which multiple cryptography algorithms have been compared. Simulation results are visualized in a way that clearly depicts which algorithm is most suitable while achieving a particular quality attribute.**

***Keywords*—Cryptography; symmetric; asymmetric; encryption; decryption**

I. Introduction

Cryptography is the art of secret writing which is used since Roman times to hide information secret or keeping message secure. To keep information secret, a widely-used method is an encryption/decryption. Basically, encryption/decryption are the fundamental functions of cryptography. In encryption, a simple message (plain text) is converted into unreadable form called ciphertext. While in decryption, a ciphertext is converted into the original text (plaintext). Both of these functions are used to secure message against who is not authorized to view the message contents [1]-[3]. The simple working of encryption and decryption functions is shown in Fig. 1.

Symmetric and asymmetric are widely accepted types of cryptography [4] in which symmetric (also called symmetric key cryptography) is focused towards ensuring secure communication between sender and receiver by using same secret key, whereas asymmetric cryptography (also called public key cryptography) secures communication by using public and private keys [5], [6]. Private key is hold individually in communication while public key is known to everyone due to public nature. Fig. 2 and 3 shows the symmetric and asymmetric cryptography, respectively.

To secure the communication, key size is the most important parameter in symmetric and symmetric cryptography. The key size of symmetric cryptography is less than the asymmetric cryptography which make symmetric cryptography less secure for more sensitive data [7], [8].

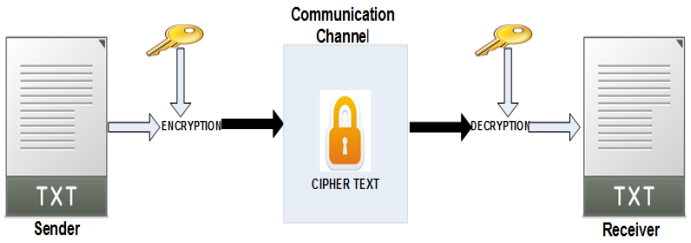

Fig. 1. Working of encryption and decryption.

The computational time of asymmetric cryptography is greater than the symmetric cryptography which makes encryption/decryption more complex for a large amount of data [9], [10]. Due to larger key size and greater computational time of asymmetric cryptography, public key cryptography is used once for key exchange only and further encryption/ decryption is done by symmetric key cryptography [11], [12].

The computational time of cryptography techniques is further classified as encryption/decryption time, key generation, and key exchange time. Encryption/decryption time is calculated by converting a plaintext (message) into ciphertext and vice versa [13], [14]. Key generation time is depending on the size of key length which is different for symmetric and asymmetric cryptography. Key exchange time is depending on the communication channel between sender and receiver [15], [16].

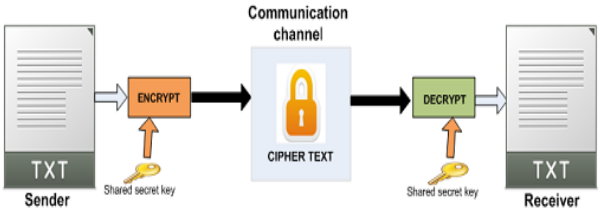

Fig. 2. Symmetric Cryptography

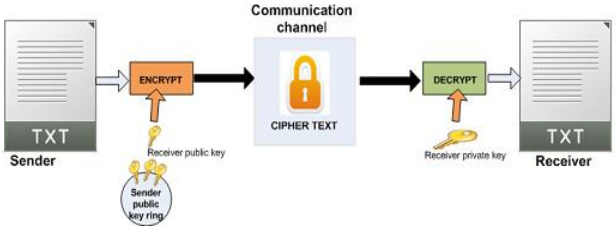

Fig. 3. Asymmetric cryptography.

There are designed many cryptographic algorithms used for encryption and decryption [17], [18]. As we already described, the cryptography schemes are classified as symmetric and asymmetric algorithms. In our paper, symmetric algorithms include but not limited; DES (Data Encryption Standard), 3DES (Triple Data Encryption Standard), AES (Advanced Encryption Standard). Asymmetric algorithms include RSA (Rivest, Shamir and Adleman), Elgamal, and ECC (Elliptic Curve Cryptography) [19]. Fig. 4 describes the taxonomy of cryptography techniques.

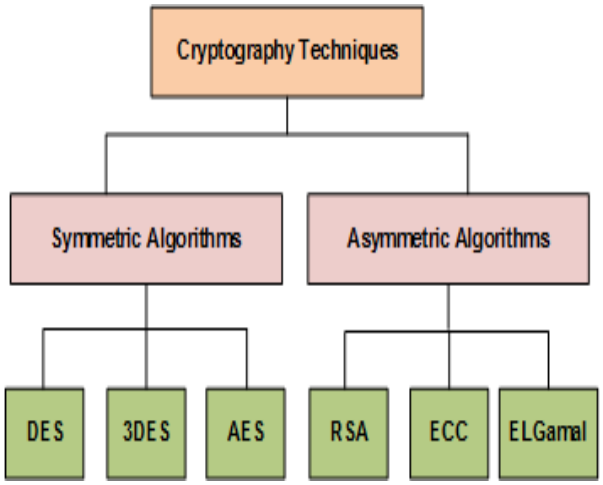

Fig. 4. Taxonomy of cryptography techniques.

In this paper, we describe the literature review of the cryptographic schemes including symmetric and asymmetric. We also evaluate the performance of described cryptographic systems on different file sizes. Performance analysis shows that the asymmetric algorithms take much time for encryption and decryption as compare to symmetric algorithms.

The main objective of this paper is to provide the performance evaluation of cryptographic schemes including symmetric and asymmetric algorithms. We use different evaluation parameters such as encryption/decryption time, and key generation time.

The rest of the paper is organized as: Section II discussed existing state of the art cryptographic schemes. Performance evaluation and results discussion of cryptographic schemes is presented in Section III. Section IV concludes the paper and future work.

II. Literature Review

There are many cryptography algorithms used to secure information such as DES, 3DES, Blowfish, AES, RSA, ElGamal and Paillier [2]. All of these algorithms are unique on it's way. However, the problem is that how to find the best security algorithm which provides the high security and also take less time for a key generation, encryption, and decryption of information. Security algorithms will depend on pros and cons of each algorithm, requirement and suitable for different application [25], [32], [33].

In paper [7], it has been evaluated that performance of two algorithms DES and Blowfish on basis of certain parameters such as encryption speed, power consumption, and security analysis. Experiment result showed that performance of Blowfish is fastest than DES and AES algorithm [34]. However, in [35] results showed that AES performance is good than Blowfish.

In [18] some of the cryptography algorithms details are given such as AES, DES, 3DES, RC6, Blowfish and RC2. Furthermore, the performance of these security algorithms is also evaluated and experiment is performed on text file and image. The result is showed that all algorithms slow in performance as compare to Blowfish as increased the packet size. However, selecting the image as the type of data instead of text file then Blowfish, RC6, and RC2 the algorithm has consumed more time than AES, DES and 3DES algorithms. The result showed that DES is still faster in performance than 3DES [18].

In this paper, [36] take the different size of a file for performance evaluation of cryptography algorithm. The experiment is performed on single processor and cloud computing. The result is proved that cryptography algorithm works faster in cloud computing than a single processor computer. AES with small input file has highest Speed up ratio, MD5 the least while RSA is the most time-consuming [36]. In author [37] evaluated the performance of different cryptography algorithms such as DES, AES, and 3DES to find the encryption and decryption time and throughput for different hardware. These algorithms are used to calculate the time of encryption. Encryption time is increasing as when the size of data increases. Therefore, the speed of encryption increase depends on file (in bytes) not on the data type of a file [38]. The throughput of 3DES has less as compare to AES, text files and images used for performance evaluation [39]. Dot net frame used for implementation of DES 3DES that take more processing time as compare to AES algorithm [37]. Only a single parameter is used to measure the encryption time. For future work of this paper is measure the encryption time by using the different parameter.

DES performance is not faster for software use. However, the performance of DES is faster on hardware [40] [12]. The performance of AES, DES, and Blowfish has been evaluated by using different size of text file in term of encryption and decryption speed. Future work of this paper shows better result by using the better simulator for implementation [41]. In this paper [42], RSA, DES and AES are discussed. Analyses are performed on the basis of some parameter such as usage of memory, computation time and output byte. Text file used for evaluation and implementation of result which showed that DES and AES are the minor difference for file encryption time while encryption time of RSA is longest and also consumed the high memory.

Mobile client and server used for evaluating the performance of RSA and ECC cryptography algorithm [43]. WTLS (Wireless Transport Layer Security) security protocol is used for performance evaluation. In experiment, the result showed that RSA is faster for client side but performance is slow at the server side as compare to ECC (Elliptic Curve Cryptosystem) performance. RSA, ElGamal and Paillier have been used for performance evaluation based on a parameter such as the encrypted file size, decrypted file size, encryption time, decryption time and throughput. Experimental result showed that encryption time of RSA is better than ElGamal but decryption time of ElGamal is better as compared to RSA. Result also showed that throughput of RSA encryption process is better and throughput in the decryption process of ElGamal performance is better than RSA. Overall performance according to the chosen parameter RSA is better than all other two algorithms paillier and ElGamal [29].

In [44] paper analysis is performed and RSA with different key size and word length variable in term of encryption and decryption process require memory size and execution time. Experiment result showed that RSA execution time is slow and need more memory requirement as compare to ECC. Key agreement and key distribution is the main problem in DES algorithm but in RSA encryption and decryption, both operations consume more time. The result showed in a simulation that RSA is slower in performance than DES and evaluated that RSA algorithm throughput of is not better than DES algorithm. In this paper, simulation result showed that power consumption and throughput of DES algorithm is much better than another algorithm [45].

III. State of the Art of Cryptography Schemes

A. Symmetric Cryptography

Symmetric cryptography is placed in the category of cryptography schemes in which a shared key is used to convert a plaintext into cipher text. A same secret key is shared by both sender and receiver. Followings are the symmetric cryptography schemes.

- DES (Data Encryption Standard): DES stands for Data Encryption Standard. DES introduced in early 1970 at IBM. The early design of DES is based on Horst Feistel. DES is a symmetric cryptographic algorithm used for encryption and decryption of message [20]. In DES, only one secret key is used for both encryption and decryption. The key size of DES is 56-bit. To perform encryption/decryption, the sender and receiver must have the same key. The DES performs encryption on a block of 64-bit [13]. The DES algorithm is most widely used in many applications [21] and some popular use in military, commercial, and security of communication system [7], same as DES but key size is different from DES. The key size of 3DES is 168 bit. The 3DES algorithm performs operation three times on each block of data. It is slower than DES [22].
- AES (Advanced Encryption Standard): AES stands for Advanced Encryption Standard which is the advancement of 3DES algorithm [23]. It was introduced in 1997 by the NIST (National Institute of Standards and Technology). Basically, AES is based on the Rijndael cipher developed by two cryptographers, Joan Daemen and Vincent Rijmen. AES is different from DES and 3DES due to variables key sizes such as 128, 192, and 256 bits [21]. Same like DES and 3DES, AES also performs encryption on blocks which are 128-bit [13]. AES algorithm use in small devices for encrypting a message to send over a network. Some other applications are monetary transaction [24] and security applications [15] [25].

B. Asymmetric Cryptography

Asymmetric cryptography is also in the category of cryptography schemes. Unlike symmetric cryptography, two keys are used: one is public and second is private. The public key is shared by anyone in the cryptographic system while the private key is kept secret by authenticated user. Followings are the asymmetric cryptography algorithms.

- RSA (Rivest, Shamir and Adleman): RSA stands for Rivest, Shamir and Adleman who introduced the RSA algorithm in 1977 [26]. RSA is an asymmetric cryptographic algorithm [2] which is also used for encryption and decryption of the message. RSA is widely used in transferring of keys over an insecure channel. Due to asymmetric nature, there are two keys used in the algorithm. One is public key and second is a private key. The public key is openly accessible to everyone in the cryptosystem and the private key is kept secret by authorized person. RSA provides confidentiality, integrity, authenticity, and non-repudiation of data [27] [23]. RSA is more commonly used in electronic industry for online money transfer [19]. In future, RSA can be used in Java cards [28].
- ElGamal: ElGamal algorithm was introduced in 1985 by Taher ElGamal [29]. ElGamal is an asymmetric key encryption algorithm that is based on the Diffie-Helman key exchange as an alternative to RSA for public key encryption. ElGamal is also used in digital signature generation algorithm called ElGamal signature scheme [20][30][31]. A homomorphic algorithm named paillier used for its semantic security [6].
- ECC (Elliptic Curve Cryptography): ECC stands for Elliptic Curve Cryptography. ECC introduced in 1985 by Neal Koblitz and Victor S. Miller. ECC lies in the category of the asymmetric scheme that is based on

elliptic curves. The applications of ECC are encryption, digital signatures and pseudo-random generators [32].

IV. Performance Evaluation

In this section, we present experimental setup and experimental results of symmetric and asymmetric algorithms.

A. Experimental Setup

The algorithms are implemented using the Java (Eclipse Platform Version: 3.3.1.1) Experiments are performed on Intel Pentium processor with a 2.34 GHz and 1 GB of memory. We used different size of text files in our experiments such as 32 KB, 126 KB, 200 KB, 246 KB and 280 KB.

B. Experimental Result

We evaluate the performance of symmetric and asymmetric algorithms by using parameters such as encryption time, decryption time and key generation time. Symmetric algorithms include DES and AES while asymmetric algorithms include RSA and ElGamal.

Encryption time is the time required by any encryption function to convert plaintext into ciphertext [44]. Decryption time is the time required to convert again cipher text into plain text. Similarly, key generation time is the time taken by key generation function to generate keys. All these functions generate different times according to the size of text files and key length in any algorithm. Table 1 shows the generation time of symmetric and asymmetric keys.

TABLE. I. Key Sizes with their Generation Time

Cryptography Algorithms		***Key Size (bits)***	***Generation Time (milliseconds)***
Symmetric	DES	56	29 ms
	AES	128	75 ms
Asymmetric	RSA	1024	287 ms
	ElGamal	160	86 ms

C. Symmetric Cryptography

In this section, we analyzed the encryption and decryption time of symmetric algorithms. Fig. 5 shows the encryption time of DES and AES algorithms performed on different file sizes. It is obvious from the Fig.5 that the encryption time of AES algorithm is lower than comparing to DES algorithm.

In Fig. 6, the performance results show that the decryption time of AES is also lower than the decryption time of DES. To conclude, the performance of AES algorithm in the context of encryption/decryption time is much better than the DES algorithm.

Table 2 shows the encryption and decryption time of symmetric and asymmetric algorithms with their different file sizes. Performance results show that when we increase the size of text files, the encryption and decryption time is also increased.

TABLE. II. File Size with their Encryption and Decryption Times

Cryptography Algorithms	***File size (kilo bytes)***	***Encryption Time (in Seconds)***	***Decryption Time (in Seconds)***
DES	32	0.27	0.44
	126	0.83	0.65
	200	1.19	0.85
	246	1.44	1.23
	280	1.67	1.45
AES	32	0.15	0.15
	126	0.46	0.44
	200	0.72	0.63
	246	0.95	0.83
	280	1.12	1.10
RSA	32	0.13	0.15
	126	0.52	0.43
	200	0.74	0.66
	246	1.11	0.93
	280	1.39	1.23
ElGamal	32	0.45	0.43
	126	1.03	0.85
	200	1.41	1.13
	246	1.75	1.30
	280	1.83	1.64

D. Asymmetric Algorithms

In this section, we analyzed the performance of asymmetric algorithms in term of encryption and decryption time. Fig. 7 shows the encryption time of RSA and ElGamal algorithms performed on different file sizes. It is obvious from the Fig. 7 that the encryption time of RSA algorithm is lower than comparing to ElGamal algorithm.

In Fig. 8, the performance results show that the decryption time of RSA is also lower than the decryption time of ElGamal. To conclude, the performance of RSA algorithm in the context of encryption/decryption time is much better than the ElGamal algorithm.

E. Symmetric and Asymmetric Algorithms

In this section, we analyzed the performance of symmetric and asymmetric cryptographic algorithms in term of encryption/decryption time and key generation time.

- *Encryption Time:* Fig. 9 shows the encryption time of DES, AES, RSA, ElGamal on different file sizes. It is clear from the figure that encryption time of DES algorithm is more than all other schemes such as AES, RSA, and ElGamal. The RSA encryption time is less than all other schemes. To conclude that, the encryption time of asymmetric algorithms is less than the symmetric algorithms.

- *Decryption Time:* Fig. 10 shows the decryption time of DES, AES, RSA, ElGamal on different file sizes. The decryption time of RSA algorithm is much than all other schemes such as DES, AES, and ElGamal.
- *Key Generation Time*: Fig. 11 shows the key generation time of symmetric and asymmetric algorithms. Key generation time is depending on the bit length of a key. The more in length, the increase in time. The RSA algorithm takes more time to generate the key because of key length 1024 bits while DES algorithm takes less time because of key length 56 bits.

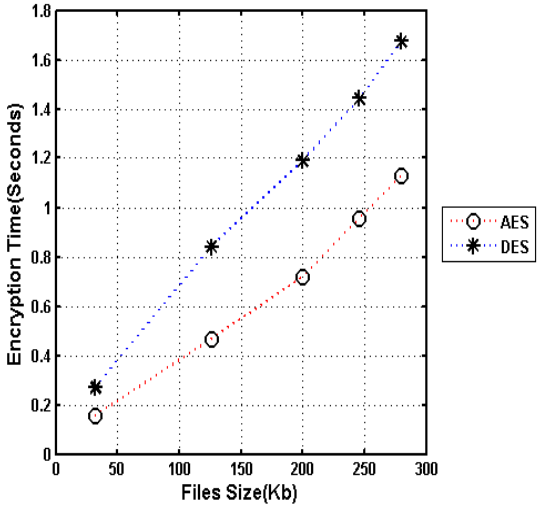

Fig. 5. Encryption Time (AES and DES).

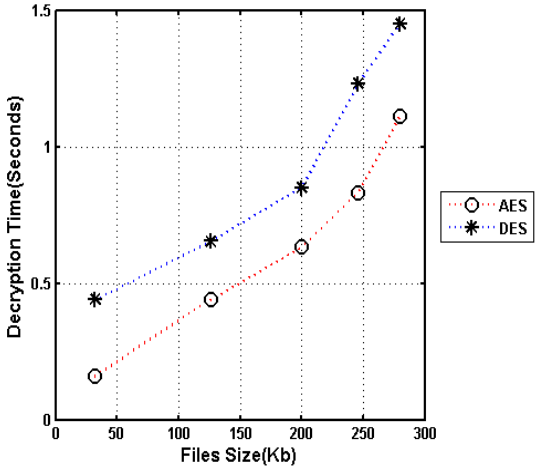

Fig. 6. Decryption Time (AES and DES).

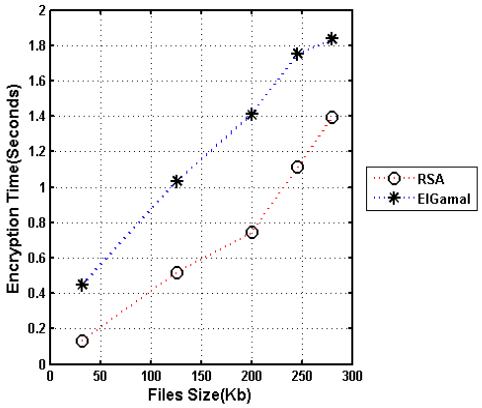

Fig. 7. Encryption Time (RSA and ElGmal).

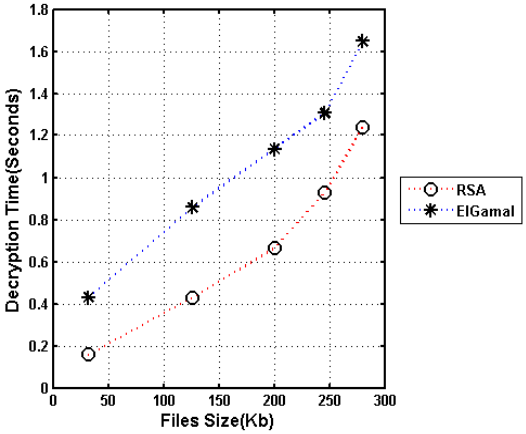

Fig. 8. Decryption Time (RSA and ElGmal).

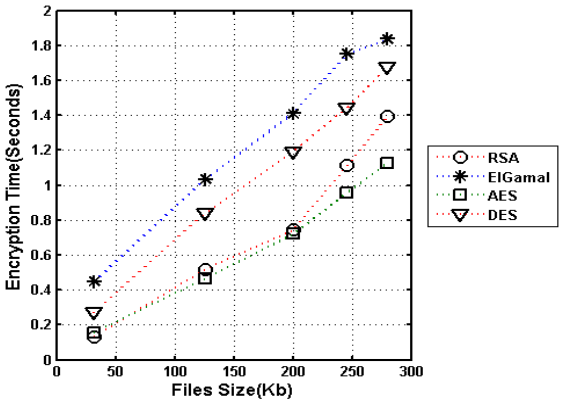

Fig. 9. Encryption Time (DES, AES, ElGmal and RSA).

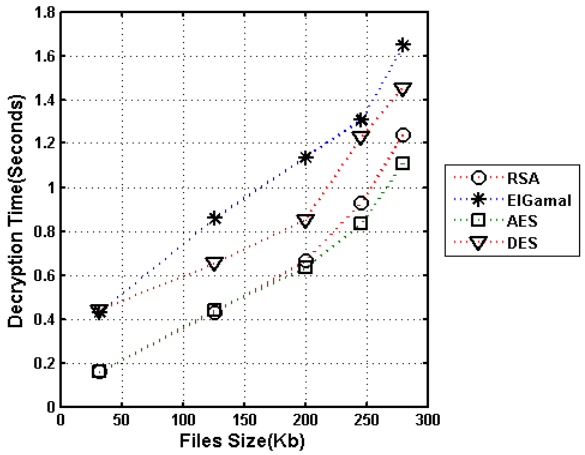

Fig. 10. Decryption Time (DES, AES, ElGmal and RSA).

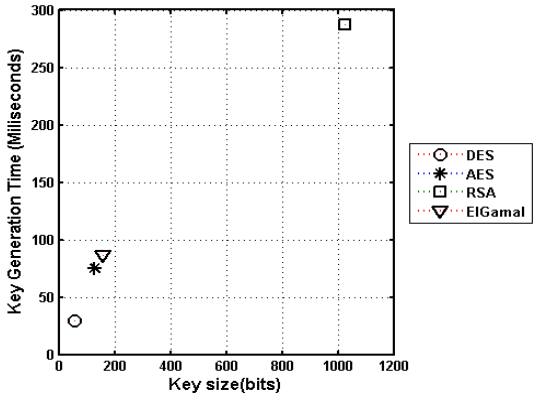

Fig. 11. Key Generation Key (DES, AES, ElGmal and RSA).

V. CONCLUSION

In this work, we analyzed the performance of symmetric and asymmetric cryptography schemes. We used encryption time, decryption time and key generation time to evaluate the cryptographic schemes. The performance results show that the symmetric schemes are computationally inexpensive when compared with asymmetric schemes. The key generation time is depending on the key length of bits. In future, we plan to elaborate more symmetric and asymmetric schemes and extend our performance analysis results.

REFERENCES

[1] Jitendra Singh Chauhan and S. K. Sharma, "A Comparative Study of Cryptographic Algorithms," Int. J. Innov. Res., pp. 24–28, 2015.

[2] A. Al Hasib and A. A. M. M. Haque, "A comparative study of the performance and security issues of AES and RSA cryptography," Proc. - 3rd Int. Conf. Converg. Hybrid Inf. Technol. ICCIT 2008, vol. 2, no. November 2001, pp. 505–510, 2008.

[3] C. Narasimham and J. Pradhan, "Evaluation of Performance Characteristics of Cryptosystem Using Text Files.," J. Theor. Appl. Inf. Technol., vol. 4, no. 1, 2008.

[4] M. Mikhail, Y. Abouelseoud, and G. Elkobrosy, "Extension and Application of El-Gamal Encryption Scheme," 2014.

[5] A. Naureen, A. Akram, T. Maqsood, R. Riaz, K. H. Kim, and H. F. Ahmed, "Performance and security assessment of a PKC based key management scheme for hierarchical sensor networks," IEEE Veh. Technol. Conf., pp. 163–167, 2008.

[6] S. Farah, M. Y. Javed, A. Shamim, and T. Nawaz, "An experimental study on Performance Evaluation of Asymmetric Encryption Algorithms," Recent advaces Inf. Sci., vol. 8, pp. 121–124, 2012.

[7] R. Tripathi and S. Agrawal, "Comparative Study of Symmetric and Asymmetric Cryptography Techniques," Int. J. Adv. Found. Res. Comput., vol. 1, no. 6, pp. 68–76, 2014.

[8] B. Padmavathi and S. R. Kumari, "A Survey on Performance Analysis of DES , AES and RSA Algorithm along with LSB Substitution Technique," Int. J. Sci. Res., vol. 2, no. 4, pp. 170–174, 2013.

[9] G. Singh, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security," *Int. J. Comput. Appl.*, vol. 67, no. 19, pp. 975–8887, 2013.

[10] A. Patil and R. Goudar, "A Comparative Survey Of Symmetric Encryption Techniques For Wireless Devices," *Int. J. Sci. Technol. Res.*, vol. 2, no. 8, pp. 61–65, 2013.

[11] C. Science and M. Studies, "An Efficient Password Security Mechanism Using Two Server Authentication and Key Exchange," pp. 50–53, 2015.

[12] A. Levi and E. Savas, "Performance evaluation of public-key cryptosystem operations in WTLS protocol," *Proc. - IEEE Symp. Comput. Commun.*, pp. 1245–1250, 2003.

[13] S. S. and K. Annapoorna Shetty, "A Review on Asymmetric Cryptography – RSA and ElGamal Algorithm," *Int. J. Innov. Res. Comput. Commun. Eng.*, vol. 2, no. Special issue 5, p. 98, 2014.

[14] T. Nie, C. Song, and X. Zhi, "Performance evaluation of DES and Blowfish algorithms," *2010 Int. Conf. Biomed. Eng. Comput. Sci. ICBECS 2010*, 2010.

[15] D. Elminaam, "Performance evaluation of symmetric encryption algorithms," *Int. J. Comput. Networks*, vol. 8, no. 12, pp. 280–286, 2008.

[16] A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, "Energy Analysis of Public-Key Cryptography on Small Wireless Devices," *Third IEEE Int. Conf. Pervasive Comput. Commun.*, p. 3, 2005.

[17] S. Singh and R. Maini, "Comparison of data encryption algorithms," *Int. J. Comput. Sci. …*, vol. 2, no. 1, pp. 125–127, 2011.

[18] D. Li, Y. Wang, and H. Chen, "The research on key generation in RSA public-key cryptosystem," *Proc. - 4th Int. Conf. Comput. Inf. Sci. ICCIS 2012*, pp. 578–580, 2012.

[19] H. Mathur and P. Z. Alam, "Cryptology Algorithm," *Int. J. Elmerging Trends Technol. Comput. Sci.*, vol. 4, no. 1, pp. 4–6, 2015.

[20] D. Sukhija, "Performance Evaluation of Cryptographic Algorithms : AES and DES," vol. 3, no. 9, pp. 582–585, 2014.

[21] M. Panda, "Performance Analysis of Encryption Algorithms for Security," pp. 840–844, 2016.

[22] E. Barker, A. Roginsky, G. Locke, and P. Gallagher, "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths," *NIST Spec. Publ.*, no. January, pp. 800–131, 2011.

[23] H. O. Alanazi, B. B. Zaidan, a. a. Zaidan, H. a. Jalab, M. Shabbir, and Y. Al-Nabhani, "New Comparative Study Between DES, 3DES and AES within Nine Factors," *J. Comput.*, vol. 2, no. 3, pp. 2151–9617, 2010.

[24] A. K. Mandal and C. Parakash, "Performance Evaluation of Cryptographic Algorithms : DES and AES," 2012.

[25] A. Sterbenz and P. Lipp, "Performance of the {AES} Candidate Algorithms in {Java}," *Third {Advanced Encryption Stand. Candidate Conf. April 13--14, 2000, New York, NY, USA*, pp. 161–168, 2000.

[26] R. L. Rivest, A. Shamir, and L. Adleman "A Method for Obtaining Digital Signatures and Public- Key Cryptosystems." Communications of the ACM, vol. 26, no. 1, pp. 96–99, 1983.

[27] M. E. Student, "Algorithms for Secure Cloud," vol. 3, no. 6, pp. 1–9, 2014.

[28] G. Bernabé and N. Clarke "Study of RSA Performance in Java Cards," 2013 .

[29] P. Nalwaya, V. P. Saxena, and P. Nalwaya, "A cryptographic approach based on integrating running key in feedback mode of elgamal system," *Proc. - 2014 6th Int. Conf. Comput. Intell. Commun. Networks, CICN 2014*, pp. 719–724, 2014.

[30] X. Li, X. Shen, and H. Chen, "ElGamal digital signature algorithm of adding a random number," *J. Networks*, vol. 6, no. 5, pp. 774–782, 2011.

[31] H. Chen and J. Lin, "Digital Signature Scheme," 2009.

[32] M. S. Anoop, "Elliptic Curve Cryptography," *Infosecwriters*, pp. 1–11, 2015.

[33] R. H. Rathod and C. Dhote, "Comparison of symmetric key encryption algorithms," International Journal of Research in Information Technology (IJRIT), 2014.

[34] O. Verma, R. Agarwal, D. Dafouti, and S. Tyagi, "Peformance analysis of data encryption algorithms," in Electronics Computer Technology (ICECT), 2011 3rd International Conference on, vol. 5. IEEE, 2011, pp. 399–403.

[35] A. Jeeva, D. V. Palanisamy, and K. Kanagaram, "Comparative analysis of performance efficiency and security measures of some encryptionalgorithms," International Journal of Engineering Research and Applications (IJERA) ISSN, pp. 2248–9622, 2012.

[36] P. Arora, A. Singh, and H. Tyagi, "Evaluation and comparison of security issues on cloud computing environment," World of Computer Science and Information Technology Journal (WCSIT), vol. 2, no. 5, pp. 179–183, 2012.

[37] M. Mittal, "Performance evaluation of cryptographic algorithms," International Journal of Computer Applications, vol. 41, no. 7, pp. 1–6, 2012.

[38] R. Masram, V. Shahare, J. Abraham, and R. Moona, "Analysis and comparison of symmetric key cryptographic algorithms based on various file features," International Journal of Network Security & Its Applications, vol. 6, no. 4, 2014.

[39] S. Kansal and M. Mittal, "Performance evaluation of various symmetric encryption algorithms," in Parallel, Distributed and Grid Computing (PDGC), 2014 International Conference on. IEEE, 2014, pp. 105–109.

[40] S. Soni, H. Agrawal, and M. Sharma, "Analysis and comparison between aes and des cryptographic algorithm," International Journal of Engineering and Innovative Technology, vol. 2, no. 6, pp. 362–365, 2012.

[41] J Thakur and N. Kumar, "Des, aes and blowfish: Symmetric key cryptography algorithms simulation based performance analysis," International journal of emerging technology and advanced engineering, vol. 1, no. 2, pp. 6–12, 2011.

[42] S. M. Seth and R. Mishra, "Comparative analysis of encryption algorithms for data communication 1," IJCST, vol. 2, 2011.

[43] A. Levi and E. Savas, "Performance evaluation of public-key cryptosystem operations in wtls protocol," in Computers and Communication, 2003.(ISCC 2003). Proceedings. Eighth IEEE International Symposium on. IEEE, 2003, pp. 1245–1250.

[44] K. B. R. P.R.Vijayalakshmi, "Performance analysis of rsa and ecc in identity-based authenticated new multiparty key agreement protocol," International Conference on Computing, Communication and Applications (ICCCA), 2012.

[45] A. Aman, J. Attri, A. Devi, and P. Sharma, "Comparative analysis between des and rsa algorithms," International Journal of Advanced Research in Computer Science and Software Engineering, 2012.