Scientific Research Publishing

Journal of Information Security, 2020, 11, 138-148
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Comparative Study of Different Cryptographic Algorithms

Baha Eldin Hamouda Hassan Hamouda

Department of Information Technology, Gulf Colleges, Hafar Al-Batin, KSA
Email: bhh@gulf.edu.sa, bahahamouda@yahoo.com

How to cite this paper: Hamouda, B.E.H.H. (2020) Comparative Study of Different Cryptographic Algorithms. *Journal of Information Security*, **11**, 138-148.
https://doi.org/10.4236/jis.2020.113009

Received: April 20, 2020
Accepted: June 5, 2020
Published: June 8, 2020

Copyright © 2020 by author(s) and Scientific Research Publishing Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/

Open Access

Abstract

With the increasing interconnection of computer networks and sophistication of cyber-attacks, Cryptography is one way to make sure that confidentiality, authentication, integrity, availability, and identification of data user can be maintained as well as security and privacy of data provided to the user. Symmetric key cryptography is a part of the cryptographic technique which ensures high security and confidentiality of data transmitted through the communication channel using a common key for both encryption and decryption. In this paper I have analyzed comparative encryption algorithms in performance, three most useful algorithms: Data Encryption Standard (DES), Triple DES (3DES) also known as Triple Data Encryption Algorithm (TDEA), and Advanced Encryption Standard (AES). They have been analyzed on their ability to secure data, time taken to encrypt data and throughput the algorithm requires. The performance of different algorithms differs according to the inputs.

Keywords

Cryptography, DES, 3DES, AES, Encryption, Decryption, Ciphertext, Plaintext

1. Introduction

In recent years, the world has faced a major challenge in the field of information and communications technology. Computer networks and Internet services are increasing daily, and our life has changed in many applications on the Internet: the growing of e-commerce, online banking services, e-government, payment of bills, and many applications that require a safe environment that serves the private and public sectors.

The vast amount of transactions and applications cannot be left without con-

trol, security and vulnerable to violations, so such transactions and applications, which are carried out over public wired or wireless networks, must require secure and comprehensive communications that secure the network management and monitoring process to make sure data authentication and the integrity, privacy, and integrity of the data.

To transfer data through the internet or any public network, there are many security aspects and applications, from secure commerce and payments to private communications and passwords protection. One of those safest aspects of cryptography is an essential tool for protecting sensitive data. The purpose of using cryptography is privacy during data transfer [1].

Cryptography algorithms play an important role in providing data security against malicious attacks. The cryptography algorithm can classify into a symmetric key (private) and asymmetric (public) key [2] [3]. The public key used to encrypt the message; the private key used to decrypt the message.

Nowadays, there is an urgent need to use cryptography to link the world via open networks, where networks are used to transfer information electronically, between ordinary people or private, public organizations, military and civilian. There must be ways to keep the information confidential.

Cryptography is widely used to convert information into incomprehensible codes by government agencies and intelligence around the world, so, the secure transmission of messages forms online or offline [4].

2. Security Services

ITU-T (X.800) has defined six services related to the security goals and attacks **Figure 1** show the taxonomy of those six common services [5] [6].

It is uncomplicated to relate one or many of these services to one single of the security goals. It is also simple to see that these services have designed to prevent security attacks.

2.1. Data Confidentiality

Data confidentiality designed to ensure the privacy of the data, that no one enters to obtain or know these facts or a specific service through which it prevented to know the contents of the information on all subscribers except the people who have been authorized to know and possess this information. This means that it designed to prevent snooping attacks and traffic analysis.

2.2. Data Integrity

Data integrity designed to protect information from change (delete, add, modify) by unauthorized persons. It may protect the whole message or part of it.

2.3. Authentication

A service or function related to the verification of identification, or a method used to verify a user's identity. Authentication required to access resource system.

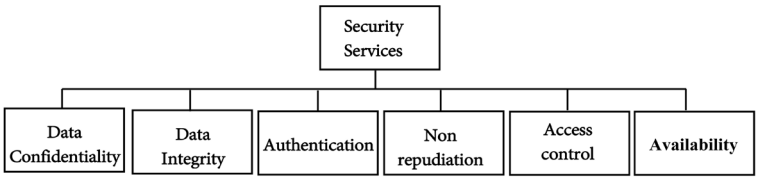

Figure 1. Security services.

2.4. Non-Repudiation

Evidence ensures no agreement or action denied at a later time, the non repudiation service protects against repudiation by the sender or receiver of the data. The sender of data can later prove that data delivered to the intended recipient, for example, digital signature.

2.5. Access Control

Methods used to limit access to a resource system or physical site. Access control used to prevent unauthorized access to systems that encrypt.

2.6. Availability

Means that the data can be accessed at any time continuously without interruption. An availability service is one that protects a system to ensure its availability. This service addresses the security concerns raised by denial-of-service attacks. It depends on proper management and control of system resources and thus depends on access control service and other security services.

3. Techniques

The actual implementation of security goals needs some techniques. Two of them are prevalent today: one is very general (cryptography).

3.1. Cryptography

Cryptography, a word with Greek origins means "secret writing." we use the term refers to the science and art of transforming messages to make them secure and immune to attacks. Although in the past cryptography referred to the encryption and decryption of messages using secret keys, today it is defined as involving three distinct mechanisms: symmetric-key decipherment, asymmetric-key decipherment, and hashing.

3.2. Types of Encryption Algorithms

There are two kinds of key-based encryption algorithms, symmetric encryption algorithms (secret key algorithms) and asymmetric encryption algorithms (or public-key algorithms).

3.3. Differences between Symmetric and Asymmetric Encryption Algorithms

Symmetric encryption algorithms encrypt and decrypt with the same key. The

main advantages of symmetric encryption algorithms are its security and high speed. Asymmetric encryption algorithms encrypt and decrypt with different keys. Data is encrypted with a public key and decrypted with a private key. Asymmetric encryption algorithms (also known as public-key algorithms) need at least a 3000-bit key to achieve the same level of security as a 128-bit symmetric algorithm. Asymmetric algorithms are incredibly slow, and it is impractical to use them to encrypt large amounts of data. Generally, symmetric encryption algorithms are much faster to execute on a computer than asymmetric ones. In practice, they often used together, so that a public-key algorithm used to encrypt a randomly generated encryption key, and the random key used to encrypt the actual message using an asymmetric algorithm. This is sometimes called hybrid encryption [5] [6].

Figure 2 Shows method describes the work of encryption using a single key is used within symmetric cryptography to encrypt the plaintext. Both party encrypting the data and decrypting the data share the key [7].

4. Block Cipher Cryptographic

Symmetric-key block ciphers are the most prominent and important elements in many cryptographic systems. Individually, they provide confidentiality. As a fundamental building block, their versatility allows the construction of pseudo-random number generators, stream ciphers, MACs, and hash functions. They may furthermore serve as a central component in message authentication techniques, data integrity mechanisms, entity authentication protocols, and (symmetric-key) digital signature schemes.

No block cipher is ideally suited for all applications, even one offering a high level of security. This is a result of inevitable tradeoffs required in practical applications, including those arising from, for example, speed requirements and memory limitations (e.g., code size, data size, cache memory), constraints imposed by implementation platforms (e.g., hardware, software, chip cards), and differing tolerances of applications to properties of various modes of operation. Also, efficiency must typically be traded off against security [8].

4.1. Data Encryption Standard (DES)

Data Encryption Standard (DES) was developed by IBM in 1975, and was described by the American National Standards Institute (ANSI) in 1981 under the name ANSI X3.92, and this standard is one of the most common available symmetric key standards these days.

DES encrypts and decrypts data in 64-bit blocks, using a 56-bit key. It takes a 64-bit block of plaintext as input and outputs a 64-bit block of ciphertext. Since it always operates on blocks of equal size and it uses both permutations and substitutions in the algorithm. DES has 16 rounds, meaning the main algorithm is repeated 16 times to produce the ciphertext. It has been found that the number of rounds is exponentially proportional to the amount of time required to find a key using a brute-force attack. So as the number of rounds increases, the security of the algorithm increases exponentially [9].

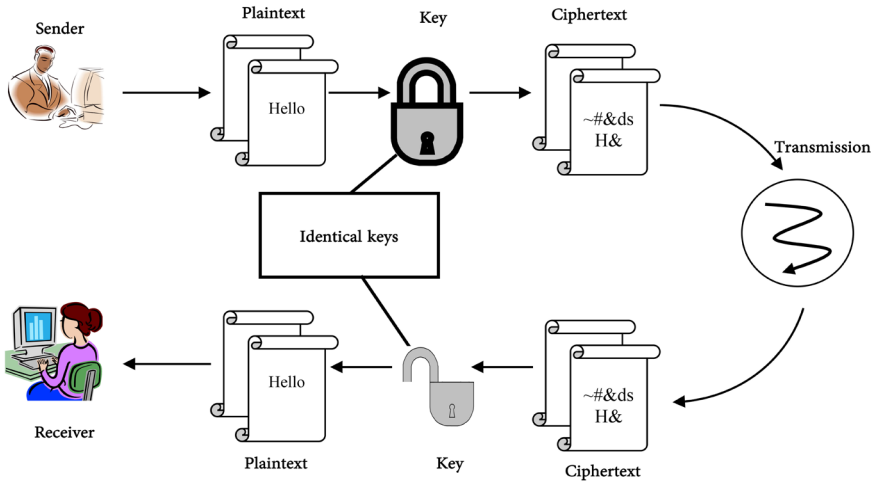

Figure 2. Method describes the work of encryption using a single key.

4.2. Triple DES

Triple DES is a variation of Data Encryption Standard (DES). It uses a 64-bit key consisting of 56 effective key bits and 8 parity bits. The size of the block for Triple-DES is 8 bytes. Triple-DES encrypts the data in 8-byte chunks. The idea behind Triple DES is to improve the security of DES by applying DES encryption three times using three different keys. Triple DES algorithm is very secure (major banks use it to protect valuable transactions), but it is also very slow [10].

Triple-DES encrypts data three times and uses a different key for at least one of the three passes giving it a cumulative key size of 112 - 168 bits. That should produce an expected strength of something like 112 bits, which is more than enough to defeat brute force attacks. Triple DES is much stronger than (single) DES; however, it is rather slow compared to some new block ciphers. However, cryptographers have determined that triple DES is unsatisfactory as a long-term solution, and in 1997, the National Institute of Standards and Technology (NIST) solicited proposals for a cipher to replace DES entirely, the Advanced Encryption Standard (AES) [11].

4.3. Advanced Encryption Standard (AES) Algorithm

AES stands for Advanced Encryption Standard. AES is a symmetric key encryption technique that will replace the commonly used Data Encryption Standard (DES). It was the result of a worldwide call for submissions of encryption algorithms issued by the US Government's National Institute of Standards and Technology (NIST) in 1997 and completed in 2000 [12].

In response to the growing feasibility of attacks against DES, NIST launched a call for proposals for an official successor that meets 21st-century security needs. This successor is called the Advanced Encryption Standard (AES).

Five algorithms were selected into the second round, from which Rijndael was selected to be the final standard. NIST gave as its reasons for selecting Rijndael

that it performs very well in hardware and software across a wide range of environments in all possible modes. It has excellent key setup time and has low memory requirements; also, its operations are easy to defend against power and timing attacks. NIST stated that all five finalists had adequate security and that there was nothing wrong with the other four ciphers.

The winning algorithm, Rijndael, was developed by two Belgian cryptologists, Vincent Rijmen and Joan Daemen [13].

AES provides strong encryption and was selected by NIST as a Federal Information Processing Standard in November 2001 (FIPS-197).

Rijndael follows the tradition of square ciphers. AES algorithm uses three key sizes: a 128-, 192-, or 256-bit encryption key. Each encryption key size causes the algorithm to behave slightly differently, so the increasing key sizes not only offer a larger number of bits with which you can scramble the data but also increase the complexity of the cipher algorithm [14].

4.4. Comparative Analysis of Different Cryptography Algorithms

Table 1 shows the comparative analysis between different cryptography algorithms at different factors such as the key size, block size, cipher type, develop, rounds, and power consumption [15] [16].

5. Simulation Results

In this section, shows the results obtained from running the simulation program using different data like text files, pdf files, word document, and images of different sizes are used to conduct (35) experiments, where a comparison of three algorithms DES, 3DES and AES is performed.

Result for cryptography algorithm DES, 3DES and AES are shown in Table 2.

Figure 3 shows Time consumption of encryption algorithm by DES, 3DES and AES algorithm. It is noticed that AES algorithm time consumption are highest for all sizes.

It indicates the speed of encryption. Throughput of the encryption scheme is calculated by dividing the total plaintext in Megabytes encrypted on the total encryption time for each algorithm.

Figure 4 shows Throughput of each encryption algorithm (Megabyte/Sec) in experiment.

Figure 5 shows Throughput of DES, 3DES, and AES (Megabyte/Sec) in experiment. The result shows AES algorithm Throughput is highest for all sizes.

Figure 6 shows Average Time of each encryption algorithm in experiment.

Simulation results for this compassion shown in Figure 3. It is clear from the graphs that in case the AES algorithm brute force attack takes much more time to find a key therefore AES has better security than DES and Triple DES.

The results show the superiority of the 3DES algorithm over other algorithms in terms of the processing time. That AES has an advantage over other 3DES and DES in terms of time consumption and throughput.

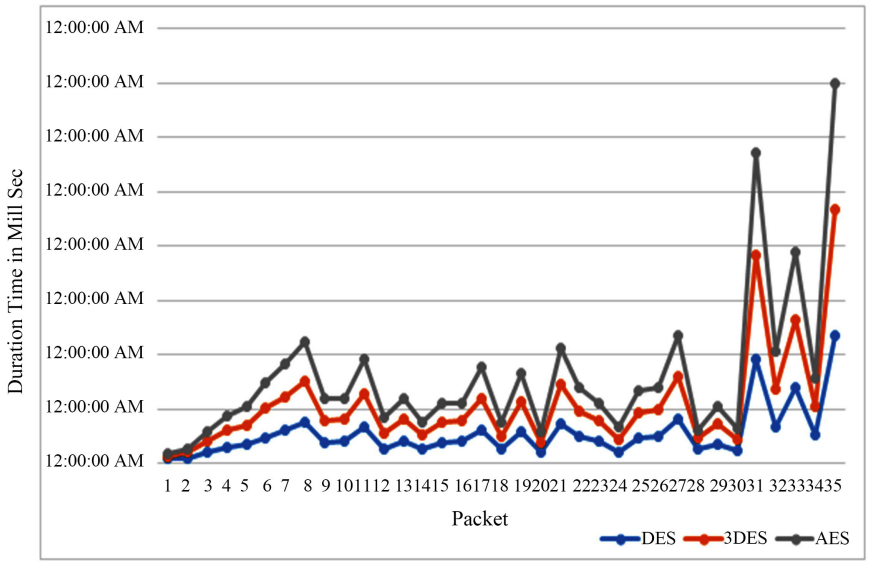

Figure 3. Time consumption of encryption algorithm.

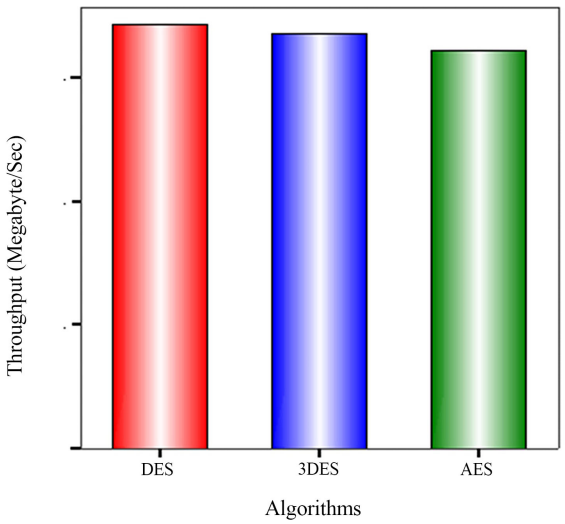

Figure 4. Throughput of each encryption algorithm (Megabyte/Sec).

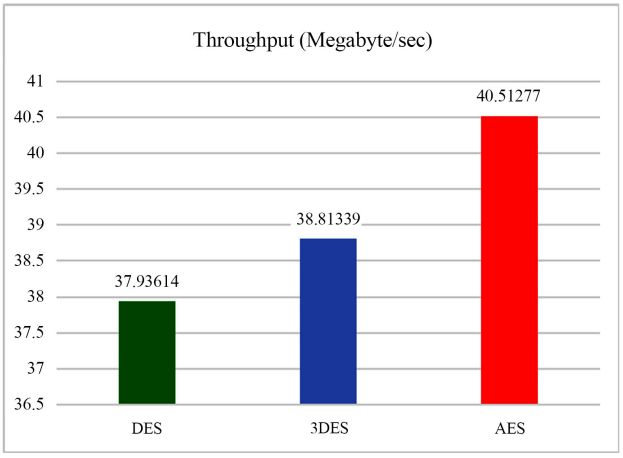

Figure 5. Throughput of DES, 3DES, and AES (Megabyte/Sec).

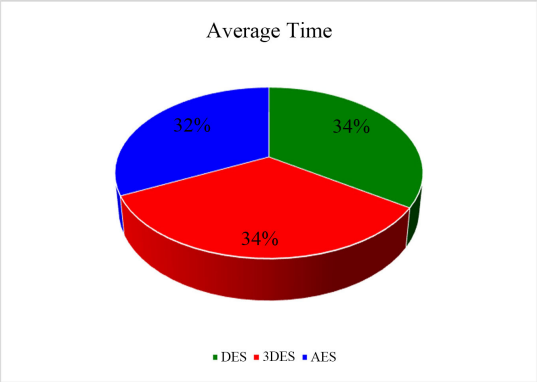

Figure 6. Average Time of each encryption algorithm.

Table 1. Comparative analysis of different cryptography algorithms.

Algorithms Factors	AES	DES	3DES
Cipher Type	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher
Key Size	128,192 or 256 Bits	56 Bits	168,112 or 56 Bits
Block Size	128,192 or 256 Bits	64 Bits	64 Bits
Develop	2000	1977	1978
Rounds	10 (128-bits), 12 (192-bits), 14 (256-bits)	16	48
Power Consumption	Low	Low	Low as compared to DES, AES

Table 2. Comparative execution times (in milliseconds) of encryption algorithms with different packet size.

Input Size (K Bytes)		Algorithms		
		DES	3DES	AES
1	914	15	8	13
2	1508	20	19	13
3	2345	43	38	35
4	3198	59	63	55
5	4038	72	70	68
6	4878	93	108	94
7	5718	121	123	122
8	6558	151	149	145
9	954	77	82	79
10	2730	82	81	78
11	3698	131	126	124
12	2188	55	57	54
13	2706	80	84	75

Continued

14	2062	50	55	49
15	3666	73	76	72
16	3484	81	77	64
17	5198	122	119	115
18	2546	53	46	54
19	4690	114	112	107
20	1836	41	37	37
21	5810	145	143	134
22	4380	97	95	87
23	3720	81	78	63
24	2220	43	46	43
25	4162	95	91	82
26	4348	100	96	80
27	6026	161	158	154
28	2316	54	38	31
29	3246	72	71	64
30	1936	46	44	39
31	10376	384	382	374
32	5810	134	138	139
33	8376	280	246	253
34	4924	107	104	103
35	11782	473	459	464
	Average Time	**108.7143**	**106.2571**	**101.8**
	Throughput (Megabytes/sec)	**37.93614**	**38.81339**	**40.51277**

6. Conclusions

This paper presented the fair comparisons among three commonly used algorithms and the simulated. The selected encryption algorithms DES, 3DES and AES are used for performance evaluation.

For performance evaluation files in different formats like text files, pdf files, word document, and images used and the experimental result based on encrypted file size and encryption time are recorded.

Were presented into (35) factors, in the case of changing packet size, through the presented results under different hardware setting and using different languages. From the comparative analysis, results showed the capability of each algorithm. It concluded that the AES is the best performing algorithm than other common encryption algorithms used. The security has taken into consideration.

Acknowledgements

Open access funding provided by Gulf Colleges.

Funding

Funding of this research was supported by the Gulf Colleges.

Ethical Approval

This article does not contain any studies with human participants or animals performed by any of the authors.

Open Access

This article is licensed under a Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source. Provide a link to the Creative Commons license, and indicate if changes were made.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Kumar, A.Y. (2013) Comparative Study of Different Symmetric Key. *International Journal of Application or Innovation in Engineering & Management*, **2**, 204-206.

[2] Abd Elminaam, D., Abdual Kader, H.M. and Hadhoud, M.M. (2010) Evaluation of the Performance of Symmetric Encryption Algorithms. *International Journal of Network Security*, **10**, 216-222.

[3] Karule, K.P. and Nagrale, N.V. (2016) Comparative Analysis of Encryption Algorithms for Various Types of Data Files for Data Security. *International Journal of Scientific Engineering and Applied Science*, **2**, 495-498.

[4] Pavithra, S. and Ramadevi, E. (2012) Study and Performance Analysis of Cryptography Algorithms. *International Journal of Advanced Research in Computer Engineering & Technology*, **1**, 84.

[5] Stallings, W. (2014) Cryptography and Network Security Principles and Practice. Sixth Edition, Prentice Hall, Upper Saddle River.

[6] Forouzan, B.A. (2007) Cryptography and Network Security. Special Indian Edition, Tata McGraw-Hill Publishing Company Limited, New Delhi.

[7] Mathur, M. and Kesarwani, A. (2013) Comparison between DES, 3DES, RC2, RC6, Blowfish and AES. *Proceedings of National Conference on New Horizons in IT*, *NCNHIT*, Mumbai, September 2013, 143-148.

[8] Alanazi, H.O., Zaidan, A.A., Jalab, H.A., Shabbir, M. and Al-Nabhani, Y. (2010) New Comparative Study between DES, 3DES and AES within Nine Factors. *Journal of Computing*, **2**, 152-157.

[9] Bala, T. and Kumar, Y. (2015) Asymmetric Algorithms and Symmetric Algorithms: A Review. *Proceedings on International Conference on Advancements in Engi-*

neering and Technology ICAET, August 2015, 1-4.

[10] Verma, A., Guha, P. and Mishra, S. (2016) Comparative Study of Different Cryptographic Algorithms. *International Journal of Emerging Trends & Technology in Computer Science*, **5**, 58-63.

[11] Taqa, A., Zaidan, A.A. and Zaidan, B.B. (2009) New Framework for High Secure Data Hidden in the MPEG Using AES Encryption Algorithm. *International Journal of Computer and Electrical Engineering*, **1**, 566-571. https://doi.org/10.7763/IJCEE.2009.V1.87

[12] Abomhara, M., Zakaria, O., Khalifa, O.O., Zaidan, A.A. and Zaidan, B.B. (2010) Enhancing Selective Encryption for H.264/AVC Using Advance Encryption Standard. *International Journal of Computer and Electrical Engineering*, **2**, 223-229. https://doi.org/10.7763/IJCEE.2010.V2.141

[13] Naji, A.W., Hameed, S.A., Zaidan, B.B., Al-Khateeb, W.F., Khalifa, O.O., Zaidan, A.A. and Gunawan, T.S. (2009) Novel Framework for Hidden Data in the Image Page within Executable File Using Computation between Advance Encryption Standard and Distortion Techniques. *International Journal of Computer Science and Information Security*, **3**, 73-78.

[14] Alanazi, H., Jalab, H.A., Zaidan, A.A. and Zaidan, B.B. (2010) New Frame Work of Hidden Data with in Non-Multimedia File. *International Journal of Computer and Network Security*, **2**, 46-54.

[15] Jeeva, A.L., Palanisamy, V. and Kanagaram, K. (2012) Comparative Analysis of Performance Efficiency and Security Measures of Some Encryption Algorithms. *International Journal of Engineering Research and Applications*, **2**, 3033-3037.

[16] Sivakumar, R., Balakumar, B. and Arivu Pandeeswaran, V. (2018) A Study of Encryption Algorithms (DES, 3DES and AES) for Information Security. *International Research Journal of Engineering and Technology*, **5**, 4133-4137.