Empirical Research Press Ltd.
London, United Kingdom

International Journal of
Engineering and Applied Computer Science

Volume: 04, Issue: 02, March 2022 ISBN: 9780995707542

# Analysis of Most Common Encryption Algorithms

*Attique Ahmed[1], Muhammad Naeem[2]*

[1,2] Department of Computer Science, Abbottabad University of Science and Technology, Pakistan

10.24032/IJEACS/0402/003

*© 2022 by the author(s); licensee Empirical Research Press Ltd. United Kingdom. This is an open access article distributed under the terms and conditions of the Creative Commons by Attribution (CC-BY) license. (http://creativecommons.org/licenses/by/4.0/).*

Volume: 04, Issue: 02, ISBN: 9780995707542, March 2022

# Analysis of Most Common Encryption Algorithms

***Abstract*—As the things are settled down after the emergence of technology, and this is the decade of professionalism as far as technology is concerned, security of data is the major hurdle in this race. This is the era in which data is one click away from the users, so data needs to be more secured so that it can be avoided unauthorized access. For this purpose, different data security fields have also emerged to ensure data security and confidentiality. In this survey paper we will look up all the techniques used for data encryption and after that, we compare those techniques to provide the best algorithm to ensure that data is secured. We go categorically, as in most of the cases, symmetric encryption technique is applicable and, in a few cases, asymmetric is recommended. Firstly, in our study, we compare both the techniques with each other and then compare all the algorithms working under the above-mentioned categories concerning their time, efficiency, memory usage, latency, key size, and several rounds which will result in showing the best algorithm according to input data.**

***Keywords- Encryption, Cryptography, Symmetric, Asymmetric, data security, algorithm.***

## I. INTRODUCTION

The settlement of technology and software programs used these days has facilitated malicious customers to intercept information at some stage in data transmission [2]. As a result, it's far extraordinarily crucial for any corporation or person to guard their touchy and treasured records. Security frequently looks up retaining the information secure from unauthorized access to maintain the quality line of defense [9]. Encryption is a method to save data so that the information stays unchanged and guarded at some stage in the information transmission from the sender to the meant recipient [26]. Encryption is described as the procedure of concealing records from intruders or unauthorized persons [14]. Conversely, decryption is the procedure of changing records again into the record's regular layout [14].

People and organizations are being subjected to protection incidents including breaches of privacy and identity theft. As a result, people's monetary facts were stolen, online debts were given illegally accessed, and to a degree person names and passwords were given posted to the public. In 2021, there were 1291 protection incidents and forty-four million data were compromised amongst exceptional businesses. The hike of security breaches was up to 17% as compared to the year 2020 [28]. Moreover, those affected businesses incur large quantities of losses in phrases of stolen budgets and different costs in the aftermath of the incidents [20].

To mitigate the security threats as far as data is concerned; encryption techniques and algorithms were designed right from the emergence of new technology. There are two types of Encryption algorithms which are named Symmetric and Asymmetric algorithms which have their pros and cons respectively. An in-depth study reveals that it varies from case to case in selecting the optimal encryption algorithm [18].

## II. FUNDAMENTALS OF STUDY

Data Security has become a crucial factor nowadays, mainly with current exchange networks, which have drawbacks that might be leveraged to devastating effects. In our study, we afford a few dialogues on famous encryption algorithms that may be used to tighten data protection in Symmetric/ Asymmetric Encryption. The best manner to start this debate is to begin from the fundamentals first. Thus, we study definitions of algorithms and basic cryptographic standards after which dive into the center part of the dialogue in which we give an evaluation of two techniques [3][16].

### *A. Algorithm*

The algorithm is a set of rules, a method, or a system for fixing a problem. An encrypted set of rules is a fixed mathematical method for acting encryption on facts. Through using such a set of rules, data is made inside cipher textual content and calls for using a key to remodeling facts into their unique shape [15]. This brings us to the idea of cryptography that has been lengthy and has been utilized in data protection in data communication.

### *B. Cryptography*

Cryptography is a way of the use of superior mathematical concepts in storing and transmitting data in a specific shape so that is understood by the ones whom it's supposed can examine and the method it. Encryption is key idea in cryptography [13][17]. It is the method in which a message is encoded in a layout that can't be examined or understood without the aid of using a key. A simple content from a person may be encrypted to ciphertext, and then processed through a data exchange channel so no one can intrude with obvious textual content. When it hits the receiver end, the ciphertext is decrypted to the original simple content [22].

### *C. Encryption*

It is the method of locking up data with the use of cryptography. The data that has been protected in this manner is encrypted [1].

### *D. Decryption*

The method of opening the encrypted data by using cryptographic methods [1].

### *E. Key*

A piece of hidden information like a password is used to encrypt and decrypt data. There are some distinct kinds of keys utilized in cryptography [4].

### *F. Steganography*

It is truly the technological know-how of hiding data from hackers and unknown people that could harm you. The distinction between steganography and encryption is that the snoopers won't have the ability to comprehend there are any hidden data in the picture, text, or any other media [26].

### *G. Symmetric Encryption*

This is the most effective type of encryption that provides one hidden key to cipher and decrypt data [22]. Symmetric encryption is an ancient and well-known method. In this method, the mystery key is used which may be a number, a phrase, or a string of arbitrary letters. It is mixed with the obvious textual data or a message to enclose the content material in a specific manner. The sender and recipient must know the name of the key which is used to encrypt and decrypt all of the messages. Blowfish, Twofish, AES, DES, 3DES, and RCG are examples of symmetric encryption. The broadly used symmetric set of rules is AES-128, AES-256, and blowfish. See Figure 1.

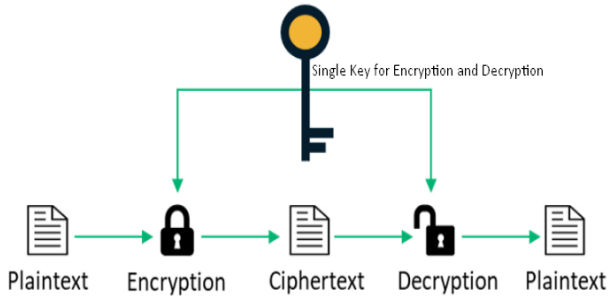


Figure 1. Symmetric Key Encryption

### *H. Asymmetric Encryption*

Asymmetric encryption can also be named public-key encryption which is comparatively a new method, as compared to symmetric encryption. Asymmetric encryption makes use of two keys to encrypt simple textual content namely a public key and a private key [29]. Secret keys are then exchanged over the Internet or a massive network. It guarantees that hackers/snoopers cannot misuse the keys. It is critical to observe that absolutely anyone with this key can decrypt the message and that is why such encryption makes use of associated keys to enhance protection [2]. A public key is made generously had to absolutely everyone who would possibly need to send or receive a message.

A message encrypted with the use of a public key can best be decrypted using a private key; a message encrypted by the use of a personal key may be decrypted by the use of a public key. Security of general public key is not always required because it's far from publicly to be had and may be surpassed over the internet [38].

Asymmetric encryption is typically utilized in everyday communication channels, mainly over the Internet. The most popular asymmetric encryption algorithms are EIgamal, RSA, DSA, elliptic curve technique and hyperelliptic curve techniques, etc. See Figure 2.

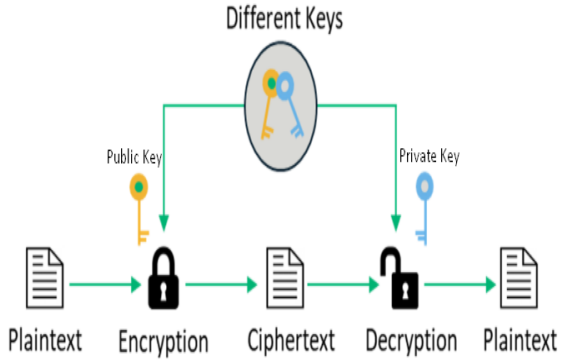


Figure 2. Asymmetric Key Encryption

Upon detailed investigation, we found differences between symmetric and asymmetric encryption techniques. All of them are given in the table below:

TABLE I. DIFFERENCE BETWEEN SYMMETRIC AND ASYMMETRIC TECHNIQUES

| No | Symmetric Encryption | Asymmetric Encryption |
|---|---|---|
| 1. | A single key is used to both encrypt and decrypt data. | Alternate keys are used to encrypt and decrypt data. The public key for encryption and the private key for decryption. |
| 2. | The size of ciphertext is comparatively the same or smaller than the size of the original content. | The size of ciphertext is comparatively the same or larger than the size of the original content. |
| 3. | The process of encryption is faster than asymmetric. | The process of encryption is slower than symmetric. |
| 4. | Used when a large amount of data is required to be transferred. | Used when data is small. |
| 5. | Largely used for confidentiality. | Used for confidentiality, authenticity, and non-repudiation. |
| 6. | Resource utilization is low. | Resource utilization is high. |

## III. ANALYSIS OF POPULAR ALGORITHMS

In this section, we compare different algorithm techniques. Firstly, we consider symmetric algorithms, and then we compare asymmetric algorithms. At the end of the study, we compare both symmetric and asymmetric algorithms in order to suggest the best algorithm which can compensate for all types of encryption tasks with great reliability.

### A. *Symmetric Algorithms Comparison*

After complete analysis, it is clear that blowfish and AES are the best among all other algorithms [4]. As these are invented after DES and 3DES so all the complications and drawbacks present in the aforementioned algorithms were mitigated in AES and blowfish techniques [23]. By comparing the key size of all the algorithms, it is observed that the AES and blowfish have bigger key sizes as compared to other techniques.

Blowfish is based on a Feistel network [11]. Feistel network uses a series of consecutive ciphers on a block of given data and is designed for a block of ciphers that encrypt a large amount of data [3]. A Feistel network works on a division basis, by splitting the block of data into 2 equal pieces and then applying encryption in multiple rounds [12].

TABLE II. SYMMETRIC ALGORITHMS COMPARISON

| Parameters for Comparison | DES | 3DES | AES | Blowfish | Twofish |
|---|---|---|---|---|---|
| **Developers** | IBM | IBM | NIST | Bruce Schneire | Bruce Schneire |
| **Emerging Year** | 1974 | 1978 | 2001 | 1993 | 1972 |
| **Size of Key** | 56 bits | 192 bits | 128, 192, 256 bits | Up to 448 bits | Up to 256 bits |
| **Size of Block** | 64 bits | 64 bits | 64 bits | 64 bits | 128 bits |
| **No. of Rounds** | 16 | 48 | 10, 12, 14 | 16 | 16 |
| **Algorithm Type** | Feistel N/W | Feistel N/W | Substitution & Permutation Network | Feistel N/W | Feistel N/W |
| **Encryption Time (ms) (25kb file size)** | 0.89 | 1.391 | 0.48,0.67, 0.95 | 0.59 | 0.99 |

AES is based on substitution and permutation networks [15]. The substitution and permutation network works on mathematical calculation and formulae to substitute and flip flop the date from one place to another [11]. In this way, the data can be made non-understandable by a common person until it is decrypted by the person who knows the key for decryption [22].

### B. *Asymmetric Algorithms Comparison*

By comparing the data fetched from Table III, it can be examined that RSA and ECC are in the race [5]. To filter one out of two, we need to understand the basic working and specifications of both algorithms thoroughly.

The key size in RSA can proceed up to a thousand bits, but the problem is that, if we use the larger key, greater will be the time of encryption and decryption, which is not our desire from this technique [27].

TABLE III. ASYMMETRIC ALGORITHMS COMPARISON

| Parameters for Comparison | Elliptic Curve | Elgamal | RSA |
|---|---|---|---|
| **Developers** | Neal Koblitz, Victor S. Miller | Taher Elgamal | Rivest, Shamir, and Adleman |
| **Emerging Year** | 1985 | 1985 | 1977 |
| **Size of Key** | Up to 512 bits | 521 bits | Up to 15360 bits |
| **Algorithm Type** | Algebraic Structure of elliptic curve over a finite field | Diffie Hellman key exchange | Exponentiation is a finite field over integers including prime numbers |
| **Encryption Time (ms)** | 390 | 297 | 531 |

On the other hand, ECC can do the specific task of encryption with the least bits of the key [9]. This can be shown in Table IV.

TABLE IV. RSA VS ECC (BORROWED FROM [13])

| Bits Level | RSA | ECC |
|---|---|---|
| **80 bits** | 1024 | 160 |
| **112 bits** | 2048 | 224 |
| **128 bits** | 3072 | 256 |
| **192 bits** | 7680 | 386 |
| **256 bits** | 15360 | 512 |

ECC is a very promising asymmetric cryptography technique that was presented by Miller and his fellow Koblitz during the late 1980s [1]. This kind of algorithm is suitable for devices using memory constraints such as Palmtop computers, Smartphones, Smartcards, etc [16]. As compared to RSA and ECC requires few parameters to encrypt and decrypt the desired data or content, keeping the security level equivalent to all other sibling algorithms [13].

RSA uses the technique of exponentiation over finite fields including prime numbers [17]. On the other hand, ECC uses algebraic expressions which can also be used to encrypt and decrypt data more conveniently. ECC shows great results in respect of performance so this can be recommended as far as asymmetric techniques are concerned [13].

## IV. DISCUSSION

To conclude the discussion, we have a specific kind of distribution as shown in Figure 3.

We can easily comprehend the fact from the figure that if the input size is less than 512 bits then we go for symmetric algorithms. The reason behind this observation is that symmetric key encryption seems faster than asymmetric

encryption concerning processing time. Another reason for using symmetric key encryption is that resource utilization is very low in this technique so it is best suited to content with lesser size.

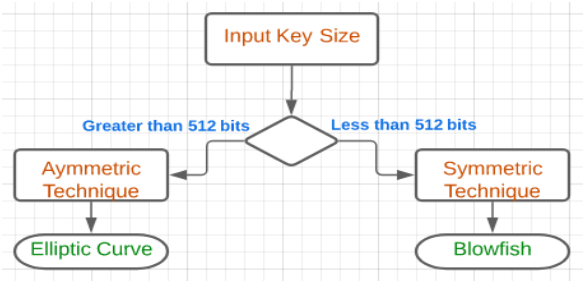


Figure 3. Suggested Best Encryption Technique

If in such cases where input data is greater than 512 bits then as a drawback of symmetric algorithm it can't handle large size of input data. So, in this case, we use the asymmetric technique.

By Deep looking at asymmetric encryption techniques, we also recommended that the ECC algorithm is the best among all older techniques and has criteria of factorization which has diverse variations to solve complex issues.

In the case of the symmetric approach, we conclude that blowfish is the best available amongst all. The reason behind this fact is that AES is also in the race, but as far as brute force attacks are concerned, AES can't handle these attacks. On the other hand, blowfish have the ability to mitigate and almost resist brute force attacks. So, in the case of security and performance, our study shows that blowfish is the best among all symmetric techniques.

## V. Conclusion and Future Work

This analysis and study did not only help us to find the best algorithm among the cluster of techniques being used in the world, but also provides us with the future aspects in which we can also work on the techniques which are free of symmetric and asymmetric approaches. Those techniques may be named hybrid encryption techniques. Hybrid techniques are also present in the market. But the problem is that these are at the initial stage and have various limitations and deficiencies which are yet to be removed.

## References

[1] Mota, Aquino Valentim, et al. "Comparative analysis of different techniques of encryption for secured data transmission." 2017 IEEE International Conference on Power, Control, Signals & Instrumentation Engineering (ICPCSI). IEEE, 2017.

[2] Sharma, Apoorva, and Gitika Kushwaha. "Comparative Analysis of Different Encryption Techniques in Mobile Ad-Hoc Networks (MANETs)." IITM Journal of Management & IT 10.1 (2019): 55-64.

[3] Bhanot, Rajdeep, and Rahul Hans. "A review and comparative analysis of various encryption algorithms." International Journal of Security & Its Applications 9.4 (2015): 289-306.

[4] Jeeva, A. L., Dr V. Palanisamy, and K. Kanagaram. "Comparative analysis of performance efficiency and security measures of some encryption algorithms." International Journal of Engineering Research & Applications (IJERA) 2.3 (2012): 3033-3037.

[5] Prajapati, Priteshkumar, et al. "Comparative analysis of DES, AES, RSA encryption algorithms." International Journal of Engineering & Management Research (IJEMR) 4.1 (2014): 132-134.

[6] Smekal, David, Jan Hajny, and Zdenek Martinasek. "Comparative analysis of different implementations of encryption algorithms on FPGA network cards." IFAC-PapersOnLine 51.6 (2018): 312-317.

[7] Riman, Chadi, and Pierre E. Abi-Char. "Comparative analysis of block cipher-based encryption algorithms: A survey." Information Security and Computer Fraud 3.1 (2015): 1-7.

[8] Marwaha, Mohit, et al. "Comparative analysis of cryptographic algorithms." Int. J. Adv. Eng. Tech/IV/III/July-Sept 16 (2013): 18.

[9] Maqsood, Faiqa, et al. "Cryptography: a comparative analysis for modern techniques." International Journal of Advanced Computer Science & Applications 8.6 (2017): 442-448.

[10] Hercigonja, Zoran. "Comparative analysis of cryptographic algorithms." International Journal of Digital Technology & Economy 1.2 (2016): 127-134.

[11] Long, Sihan. "A Comparative Analysis of the Application of Hashing Encryption Algorithms for MD5, SHA-1, and SHA-512." Journal of Physics: Conference Series. Vol. 1314. No. 1. IOP Publishing, 2019.

[12] Panda, Madhumita. "Performance analysis of encryption algorithms for security." 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES). IEEE, 2016.

[13] Farah, Shahzadi, et al. "An experimental study on performance evaluation of asymmetric encryption algorithms." Recent Advances in Information Science, Proceeding of the 3rd European Conf. of Computer Science,(EECS-12). 2012.

[14] Singh, Gurpreet. "A study of encryption algorithms (RSA, DES, 3DES, and AES) for information security." International Journal of Computer Applications 67.19 (2013).

[15] Yegireddi, Ramesh, and R. Kiran Kumar. "A survey on conventional encryption algorithms of Cryptography." 2016 International Conference on ICT in Business Industry & Government (ICTBIG). IEEE, 2016.

[16] Mushtaq, Muhammad Faheem, et al. "A survey on the cryptographic encryption algorithms." International Journal of Advanced Computer Science and Applications 8.11 (2017): 333-344.

[17] Jaryal, Shikha, and Chetan Marwaha. "Comparative analysis of various image encryption techniques." International Journal of Computational Intelligence Research 13.2 (2017): 273-284.

[18] Dakate, Deepak Kumar, and Pawan Dubey. "Performance comparison of symmetric data encryption techniques." IDEA 128 (2012): 58.

[19] Ebrahim, Mansoor, Shujaat Khan, and Umer Bin Khalid. "Symmetric algorithm survey: a comparative analysis." arXiv preprint arXiv: 1405.0398 (2014).

[20] Jang, Shin Woo. "Comparative analysis of AES, Blowfish, Twofish and Threefish encryption algorithms." Anal. Appl. Math. 10 (2017): 5.

[21] Liu, Fuwen, and Hartmut Koenig. "A survey of video encryption algorithms." computers & security 29.1 (2010): 3-15.

[22] Kumar, Anuj, Sapna Sinha, and Rahul Chaudhary. "A comparative analysis of encryption algorithms for better utilization." International Journal of Computer Applications 71.14 (2013).

[23] Hamouda, Baha Eldin Hamouda Hassan. "Comparative study of different cryptographic algorithms." Journal of Information Security 11.3 (2020): 138-148.

[24] Innokentievich, Tutubalin Pavel, and Mokshin Vladimir Vasilevich. "The Evaluation of the cryptographic strength of asymmetric encryption algorithms." 2017 Second Russia and Pacific Conference on Computer Technology and Applications (RPC). IEEE, 2017.

[25] Saleh, Mohammed A., et al. "An analysis and comparison for popular video encryption algorithms." 2015 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE). IEEE, 2015.

[26] Mahajan, Prerna, and Abhishek Sachdeva. "A study of encryption algorithms AES, DES and RSA for security." Global Journal of Computer Science and Technology (2013).

[27] Afolabi, A. O., and O. G. Atanda. "Comparative analysis of some selected cryptographic algorithms." Computing, Information Systems, Development Informatics & Allied Research Journal 7.2 (2016): 41-52.

[28] https://www.securitymagazine.com/articles/96667-the-top-data-breaches-of-2021

## AUTHORS PROFILE

**Mr. Attique Ahmed** has completed his BS degree in Computer Science from Hazara University, Mansehra, Pakistan. Presently, He is pursuing M.Phil. degree in Computer Science from Abbottabad University of Science and Technology, Abbottabad, Pakistan.

**Dr. Muhammad Naeem** is an Associate Professor and Head of the Department of Computer Science at Abbottabad University of Science and Technology, Abbottabad, Pakistan. He has completed his Ph.D. from Leicester University, United Kingdom.