International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

COMPARATIVE STUDY OF ENCRYPTION ALGORITHMS

P. Rathika[1],Dr. J.GnanaJayanthi[2], Dr. K. Mohan Kumar[3]
[1]Research Scholar, [2&3]Research Supervisors
PG & Research Department of Computer Science, Rajah Serfoji Government College (Autonomous), Thanjavur
Affiliated to Bharathidasan University, Trichirappalli, Tamil Nadu, India

\

ABSTRACT: Exchanging information directly through the network is not safety. The hackers may steal valuable information and misuse that information or alter the information for their convenience. So, before sending the information through the network, they must be encrypted using an algorithm at sender side and decrypted at the receiver side using an effective algorithm to transfer the data securely. Many algorithms invented or evolved over the years for this purpose. This paper analyzes the strength of various cryptographic algorithms with the advantages and disadvantages.

KEYWORDS: Cryptography, Encryption, Decryption, Security, Cipher

I. INTRODUCTION

In this digital world, people depends internet for everything like social media, education, banking, shopping, bill payments. Especially in this pandemic period schools and colleges are running through online only. In this situation, user's information exchanged over the internet are safely handled or not is a big question. To protect user's sensitive information is a crucial task. To provide security to user's information cryptographic algorithms are used.

Cryptography is not a new one it's an ancient encoding technique and it is still being developed.Encryption is one of the technique to provide information security. Encryption algorithms play a vital role in information security against malicious attacks. For information security many encryption algorithms are used. In this research, popular algorithms used for encryption and decryption in various fields are discussed. This paper focus on comparing various encryption algorithms like Triple DES, RSA, AES, Twofish, Blowfish, IDEA, MD5.

II. LITERATURE REVIEW

Dr. Prerna Mahajan & Abhishek Sachdeva (2013), studied three different encryption algorithms namely; AES, DES and RSA. The performance measure of encryption schemes will be conducted in terms of encryption and decryption time such as text or document[1].

Abdalbasit Mohammed Qadir&NurhayatVarol (2019), demonstrated a review of some of the research that has been conducted in the field of cryptography as well as of how the various algorithms used in cryptography for different security purposes work[2].

Omar G. Abood&Shawkat K. Guirguis (2018), discussed several important algorithms used for the encryption and decryption of data in all fields, to make a comparative study for most important algorithms in terms of data security effectiveness, key size, complexity and time, etc. This research focused on different types of cryptography algorithms that are existing, like AES, DES, TDES, DSA, RSA, ECC, EEE and CR4…etc[3].

Dr. Kiramatullah et.al. (2019), considered various encryption algorithms and techniques for improving securing data, information security using encryption. Comparisons of encryption algorithms on the basis of their performance, key size, efficiency in hardware and software, availability, implementation techniques, and speed[4].

Ali Mohammed Ali Argabi&Md Imran Alam (2019), proposed a new cryptographic algorithm AEDS (Advanced Encryption and Decryption Standard) which is developed by combining DES and AES algorithms. AEDS will be more secure and robust as compared to DES and AES[5].

Ms.Vinaya Kulkarni et.al. (2020), described network security on the basis of the services of security. The security services are as confidentiality, authentication and integrity, digital signature, web security, email security, IP security and authentication applications. This paper gives detail study of network security algorithms and their applications. The algorithms are as follows: 1.DES 2.AES 3.RSA 4.MD5 5.SHA512 6.HMAC 7.DIGITAL SIGNATURE 8.SSL 9.SET 10.PGP 11.ESP 12.AH[6].

III. RESEARCH METHODOLOGY

In this research work, the advantages and disadvantages of various kinds of encryption algorithms were tabulated. These advantages and disadvantages and disadvantages were fetched from the resources like text book and from web. For every advantage and disadvantage a point was given and the difference was calculated. The effectiveness of the algorithms measured based on that difference value.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

IV. RESULTS AND DISCUSSION

The following Table 1 shows the advantages and disadvantages of various cryptographic algorithms.

Table 1: Advantages and Disadvantages of Algorithms

S. NO	ALGORITHMS	ADVANTAGES	DISADVANTAGES
1.	**Triple DES**	1.3DES is easy to implement (and accelerate) in both hardware and software. 2. 3DES is ubiquitous: most systems, libraries, and protocols include support for it. 3. 3DES is believed to be secure up to at least "2112" security (which is quite a lot, and quite far in the realm of "not breakable with today's technology").	1. It is slow, especially in software as it was designed for hardware implementations. 2. It is applied three times on the same data so it is such wastage of time.
2.	**RSA Encryption**	1. The primary advantage of public-key cryptography is increased security and convenience. 2. Private keys never need to be transmitted or revealed to anyone. 3. In a secret-key system, by contrast, the secret keys must be transmitted (either manually or through a communication channel) since the same key is used for encryption and decryption. 4. A serious concern is that there may be a chance that an enemy can discover the secret key during transmission.	1. A disadvantage of using public-key cryptography for encryption is speed. There are many secret-key encryption methods that are significantly faster than any currently available public-key encryption method. 2. Nevertheless, public-key cryptography can be used with secret-key cryptography to get the best of both worlds. 3. For encryption, the best solution is to combine public- and secret-key systems in order to get both the security advantages of public-key systems and the speed advantages of secret-key systems. Such a protocol is called a digital envelope.
3.	**Advanced Encryption Standards (AES)**	1. As it is implemented in both hardware and software, it is most robust security protocol. 2. It uses higher length key sizes such as 128, 192 and 256 bits for encryption. Hence it makes AES algorithm more robust against hacking. 3. It is most common security protocol use for wide various of applications such as wireless communication, financial transactions, e-business,	1. It uses too simple algebraic structure. 2. Every block is always encrypted in the same way. 3. Hard to implement with software. 4. AES in counter mode is complex to implement in software taking both performance and security into considerations.

		encrypted storage etc. 4. It is one of the most spread commercial and open source solutions used all over the world. 5. No one can hack your personal information. 6. For 128 bit, about 2^{128} attempts are needed to break. This makes it very difficult to hack it as a result it is very safe protocol.	
4.	**Twofish Encryption Algorithm**	1. Everyone is nervous about the transition of confidential data to the cloud because several businesses consider that the cloud is not as reliable as their own data centre. 2. It is feasible for outsiders to access it while data is in the cloud, but clients' and competitors' data remain stored in the same storage place. 3. Due to the extreme cost and versatility, companies need the benefit of the cloud. 4. The capacity to spin up or decommission servers when market requirements shift is part of this benefit. So, what happens if the service company asks to leave? 5. The virtualized contexts can provide multi-tenancy that includes greater flexibility and reduction in cost. 6. The service providers can access the data if they both contain encrypted data and keys used for encryption. To overcome this issue, processing data encryption in the cloud and preserving the encryption keys at the users' end make sense. 7. Although certain companies, no matter how simple the key security solution is, do not consider handling encryption keys. 8. They have queries about backup, affordability, and rehabilitation from disasters.	1. Dealing with encryption is a well-known technique to keep the data secure from unauthorized individuals and agencies. 2. One of the major benefits of encryption is to provide data access for such an agency that is familiar with the keys and passwords used for the encryption of data. 3. However, below are the few disadvantages of data encryption that require special attention. 4. The user would be unable to explore the encrypted file if the password or key got the loss. 5. However, using simpler keys in data encryption makes the data insecure, and randomly, anyone can access it. 6. Data encryption is a useful data security technique; therefore, it requires plenty of resources like data processing, time consumption, usage of various algorithms for encryption, and decryption. Therefore, it is a bit of an expensive technique. 7. It is possible to establish arbitrary expectations and specifications that might jeopardize data encryption protection if an enterprise may not recognize any of the limitations enforced by encryption techniques.
	Blowfish Encryption Algorithm	1. Blowfish is one of the fastest block ciphers in general use, except when changing keys. 2. Each new key requires pre-processing equivalent to	1. The disadvantages of Blowfish are it must get key to the person out of band specifically not through the unsecured transmission channel.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

5.		encrypting about 4 kilobytes of text, which is very slow compared to other block ciphers. 3. This prevents its use in certain applications, but is not a problem in others, such as SplashID. 4. In an application, it's actually a benefit especially the password-hashing method used in OpenBSD uses an algorithm derived from Blowfish that makes use of the slow key schedule. 5. Blowfish is not subject to any patents and is therefore freely available for anyone to use. This has contributed to its popularity in cryptographic software.	2. Each pair of user's needs a unique, so as number of users increase, key management becomes complicated. For example N(N-1)/2 keys required. Blowfish can't provide authentication and non-repudiation as two people have same key. 3. It also has weakness in decryption process over other algorithms in terms of time consumption and serially in throughput
6.	**IDEA Encryption Algorithm.**	1. Keys of encryption and decryption are small. Using these there is a chance of generating stronger ciphers, with simple transformations. 2. These are used to have a higher rate of data throughput i.e. in a range of hundreds of megabytes/sec in hardware implementations. 3. Whereas the implementation is software generates a throughput of megabytes/sec.	1. Being a single key at both ends, it should be kept secret at both ends. 2. As the number of keys depends on the number of communicating parties, key stack in larger networks will be more which affects the maintenance.
7.	**MD5 Encryption Algorithm**	1. MD5 Algorithms are useful because it is easier to compare and store these smaller hashes than store a large variable length text.	1. Moreover, it is very easy to generate a message digest of the original message using this algorithm.

The above Table 1 shows the advantages and disadvantages of the Triple DES, RSA, AES, Twofish, Blowfish, IDEA, MD5 encryption algorithms. It clearly shows that AES algorithm has more advantages over other algorithms and it has limited disadvantages only. The following Table 2 shows the weightage of various algorithms.

Table 2: Weightage of various Algorithms

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

Algorithm	Advantage	Disadvantage	Weight
Triple DES	3	2	1
RSA Encryption	4	3	1
Advanced Encryption Standard(AES)	6	4	2
Twofish Encryption Algorithm	8	7	1
Idea Encryption Algorithm	5	3	2
MD5 Encryption Algorithm	3	2	1
Blowfish Encryption Algorithm	1	1	0

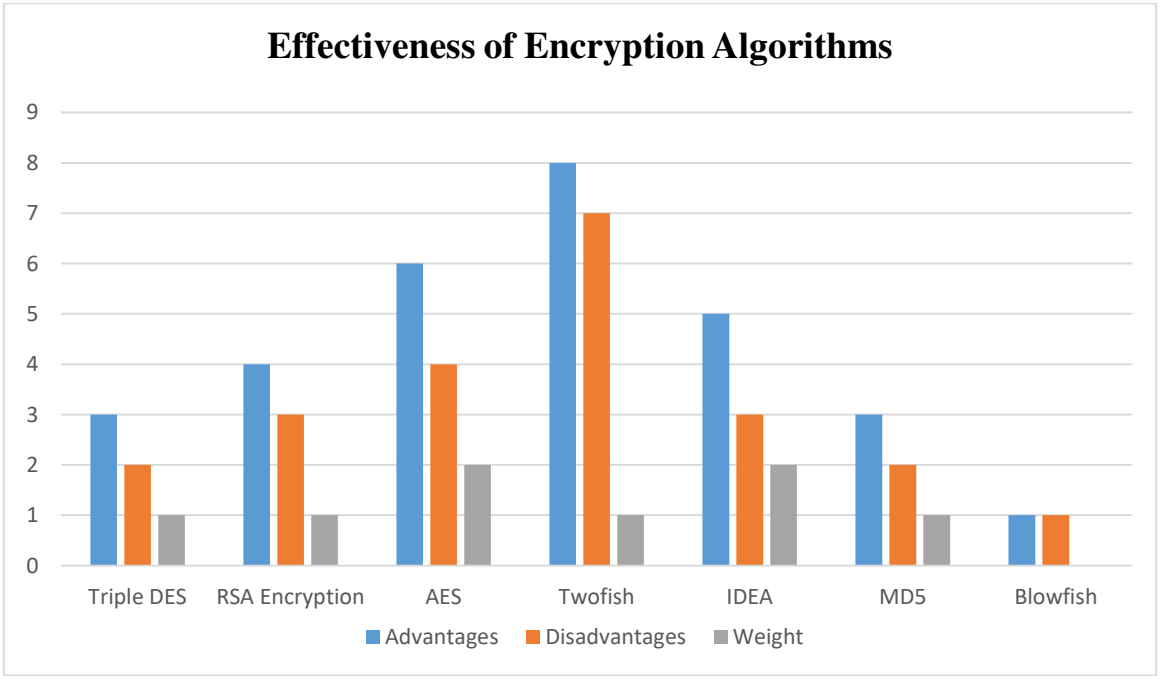

Figure 1:Effectiveness of various Algorithms

The above Figure -1 shows the graphical representation of the above Table -2.This results clearly shows that AES algorithm is more efficient than other algorithms.

V. CONCLUSION

This methodology surveyed the different types of encryption algorithms like Triple DES, RSA, AES, Twofish, Blowfish, IDEA, MD5and HMAC. This comparative study of various encryption algorithms shows that the strength of the algorithm depends upon the advantages and disadvantages of the algorithm. Based on this research it was concluded that AES algorithm has much better than other algorithms.

REFERENCES

[1] Dr. Prerna Mahajan, Abhishek Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security",Global Journal of Computer Science and Technology, Volume 13, Issue 15, 2013.

[2] AbdalbasitMohammed Qadir, NurhayatVarol, "A Review Paper on Cryptography",ResearchGate, 2019.
[3] Omar G. Abood, Shawkat K. Guirguis, "A Survey on Cryptography Algorithms",International Journal of Scientific and Research Publications, Volume 8, Issue 7, 2018.
[4] Dr. Kiramatullah, BibiAyisha, Farrukh Irfan, InaamIllahi, Zeeshan Tahir, "Comparison of Various Encryption Algorithms for Securing Data" , 2019.
[5] Ali Mohammed Ali Argabi, Md Imran Alam, "A new Cryptographic Algorithm AEDS (Advanced Encryption and Decryption Standard) for data security",International Advanced Research Journal in Science, Engineering and Technology,Volume 6, Issue 10, 2019.
[6] Ms.Vinaya Kulkarni,Ms. ShivaliKirdat,Ms. SnehaPatil,Dr. C.H.Patil, "Study on Network Security Algorithm",International Journal of Engineering Research & Technology (IJERT),Volume 8, Issue 05, 2020.