IJCSE International Journal of Computer Sciences and Engineering Open Access

Review Paper Vol.-6, Issue-5, May 2018 E-ISSN: 2347-2693

Secure and Authenticated Cryptographic Techniques: "A Review"

S. Srivastav[1*], V. Pal[2], V. Gupta [3], K.K. Gola[4]

[1,2,3]Department of Mathematics, Faculty of Engineering, TMU, Moradabad, 244001 India
[4]Department of Computer Science and Engineering, Faculty of Engineering, TMU, Moradabad, 244001 India

**Corresponding Author: shwetashona121@gmail.com*

Available online at: www.ijcseonline.org

Accepted: 17/May/2018, Published: 31/May/2018

Abstract— In the world of the high technology networking system, it is very important to ensure the security of the data. To make our data secure during communications, Cryptography is the best method in networking security to provide the confidentiality or authentication. There are two main methods which are used to achieve these two things (i.e. confidentiality and authentication) in cryptography that are public key cryptosystem and digital signatures. Here this work shows a survey on the existing techniques and also presents a comparison that helps the researches to find the gaps in the existing techniques.

Keywords— Encryption, Decryption, Symmetric key, Public Key, Cryptographic algorithms, Digital Signature

I. Introduction

The network security and cryptography are the two very important in terms of cyber world because without these two things our data is not secure. There are mainly two types of data the one is authenticated and the other is confidential data. If we talk about the symmetric cryptography then it includes confidential data and not the authentication while on the other hand the "digital signature" includes authenticated data and is not confidential one, we are working on the cryptography and algorithms which will generate a particular algorithm which will be authenticated as well as confidential both and which will make our network secure [10].

The digital signature can be understood by an example that if two persons are talking and the hacker or the third person wants the message to be decoded in the middle of the conversation then he must know both the keys of the sender and user without it the message cannot be decoded or encrypted and for this we need a security cross check whether it is confidential and authenticated or not. There are some requirements of digital signature that are mentioned below-

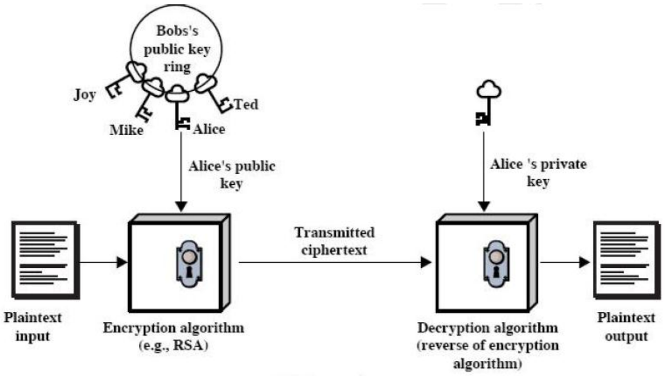
i) It depends on the matter that is send by the sender.

ii) The information that is to be send or receive must be different and unique.

iii) The authentication of date and time is must for digital signature.

iv) In digital signature the message to not be leaked it is necessary that the third person should not know the contents that are send or receive.

Mathematical and computer science are the major parts of the cryptography. The theory of cry of public key is mostly number theory .for the proper knowledge of public key of cryptosystem number theory should be known properly .the public key algorithm is more reliable on mathematics than on permutation, the public key cryptosystem is based on mathematical function more than substitution method. As we know that public key cryptosystem is based on the method of cryptography that is asymmetric rather than symmetric cryptography [3].



(a) Encryption

Figure 1. Encryption Decryption Process

Security is one of the most important and essential thing in daily life. Whenever we talk about the online things or the internet issues we talk about the network security. Security is the very first barrier or we can say a very useful need in terms of cyber world. The day to day thefts are increasing day by day and are producing a very bad impact on the youth people as we know that without security a network is not valid and authenticated and also not useful in cyber world[18].

II. KEY POINTS OF CRYPTOGRAPHY

Cryptography is usually referred to as “the study of secret”. Cryptography is a process to attain the security by encodes the data to make it incompressible. It stores and transmits the data in such manner so that only those people can access the data for which it has been planned. We can transmit the data over internet safely by using some cryptographic algorithm so that it will be difficult to attacker to encode our confidential or private information. The terms are most often associated with cryptography are:-

1. Plain Text: A simple text that an individual wants to share with other is referred to a plain text. For example Celia wants to send "hello" to her friend aliena. Here "hello" is a plain text.

2. Cipher Text: A text which is incomprehensible by anyone or a meaningless text is referred to a cipher text. Suppose "w8ehd98" is a Cipher Text obtained for "hello" after encryption. Decoding the Cipher Text by decryption, we again get a Plain Text.

3. Encryption: It is a phenomenon by which a Plain Text converts into a Cipher Text. It converts meaningful information into garbage information.

4. Decryption: It is a phenomenon by which a Cipher Text converts into a Plain Text. It converts garbage information into meaningful information.

5. Key: A numeric or mathematical value by which we can encrypt a Plain Text or decrypted a Cipher Text. A key is needed for both encryption and decryption. In this section, the author describes the previous research works in the form of title, problem statement, objectives, not repeat the information discussed in Introduction.

III. SECURITY SERVICES

There are some basic goals of cryptography. All security system must contain a various number of the security function that can assure the secrecy of the system. These functions are specified as the goal of the security system. These main goals of cryptography are explained below:

Authentication: It is the process that provides one's identity i.e. before sending and receiving the message, receiver and sender identity should be verified. In Authentication, the user or system has to be proving its singleness to the assistant or client. It is used by an assistant when it needs to know who is accessing their data or site. Authentication does not want to know what task a particular person can do or what information a particular person can see. Authentication usually identifies and verifies who the person or system is.

Data Confidentiality: It means the protection of data or information against unconstitutional revelation of data i.e. only the authenticated people are able to read the message content and no one else. It may be applied to whole data, some portion of data and even existence of data. The main component which makes the information confidential would be encryption. It keeps the client's information between you and a client and not telling others like co-workers, family member, friends etc.

Data Integrity: It includes an assurity that data has not been altered or recreated in such an unconstitutional manner after it was made, transmitted or stored. It means that there has been no deletion, addition or recreation done with the data. Digital signatures or data authentication codes are the cryptographic mechanism that can be used to analyze to both accidental alteration and deliberate alteration. The accidental alteration that might happen because of transmission problem or hardware failure while deliberate alteration that might happen by an attacker. Although non-cryptographic mechanism can be used to analyze accidental alteration, they are not suitable for investigating the deliberate alteration.

Non-repudiation: A mechanism to prove that the sender truly sends the message i.e. neither the sender nor the receiver can falsely deny that they have sent a certain message. It is the declaration that an individual cannot refuse something. Non-repudiation can be obtained through the use of digital signatures, confirmation services, and timestamps. It gives the assurance of transmitting the message between parties and digital signatures or encryption.

IV. RELATED WORK

In the various section of literature review, we will discuss the different cryptography and network security under the given section and the reviews of so many researchers are present in this section.

Dhawan [8] has discussed the different algorithms of encryption under the.NET. According to the author different algorithms were compared with others like DES, 3DES, RC2, and AES. This mainly concludes that AES is better in comparison to the other algorithms of cryptography.

Thakur et al [26] have discussed the comparison between the symmetric keys DES, AES and Blowfish. The comparison was made between the size (key, block) and speed. These were the parameters on which the algorithms worked. It was concluded that Blowfish has better performance than any other algorithm of cryptography.

M. Chanda Mona et al [11] have discussed a survey on various encryption and decryption techniques and algorithms. This paper provides a review and survey of some symmetric and asymmetric techniques. DES, AES, Symmetric and asymmetric each technique is unique in its own way and thus beneficial in its own way.

Muhammad Faheem Mushtaq et al [14] have discussed that cryptography is an essential, effective, efficient technique for security. It was based on DES, 3DES, Blowfish, AES and Hybrid cubes encryption algorithm (Hisea). The author concluded that they contain evaluation parameter like encryption and decryption time, memory, avalanche effect, entropy, correlation assessment and the results show that Blowfish, AES, Hisea are more secure and Blowfish is best among them for encryption and decryption while AES is good for avalanche effect and for entropy.

Harpreet Kaur et al [9] have discussed in the research paper that encryption, AES, DES, 3DES, Blowfish-based on the authentication and confidentiality of the data so that the hackers can't decode it easily. It concluded that the more reliable algorithm is AES and more efficient and good for security purposes. The author also concluded that the algorithms provide more security in data storage and transmission.

Saranya K et al [21] on 3 March 2014 have discussed that in today's era it is very important to secure data and uses all the cryptographic techniques and algorithm to make the data more secure. This research paper focuses on cryptography, symmetric keys, asymmetric keys, and cryptanalysis. It concluded that some techniques succeeded and some techniques failed due to the security issue. The main purpose of this paper is to get the proper knowledge of cryptographic algorithms and some parameters like a liability to attacks, the uniqueness of the parameters and techniques etc.

Monika Agrawal and Pradeep Mishra [13] have discussed the detailed study of the symmetric encryption techniques with their advantages and limitations mainly focuses on symmetric and asymmetric encryption techniques, cipher text, plain text, key. The security based terms for proper authentication. This paper concluded that the algorithms AES, DES, 3DES, and Blowfish are symmetric and better in terms of space requirement and speed in comparison to asymmetric algorithms RSA the symmetric algorithm Blowfish is more secure in terms of security attacks of data and related things to it.

Darshana Patil [6] has discussed that security of data is the first priority for any organization. Different techniques and algorithms are used in this research paper like an encryption key, decryption key, symmetric key, asymmetric key, and cryptography. This paper concluded that the encrypt/decrypt text blocks using a generated key without a password. The proper technique has been implemented in this research paper using Java programming.

B. Nithya and P.Sripriya [4] have discussed in this paper that presents a review of the study of algorithms and their comparisons. Keywords used are plain text, cipher text, encryption, decryption, security attacks. The conclusion includes that the different types of algorithms and their speed and memory and this shows that symmetric algorithms are faster than asymmetric algorithms.

Sarita Kumari [22] has discussed that security is something that refers to the private world that is not accessible without proper knowledge of security algorithms. The keywords are data encryption and decryption, compression, cryptography, security, integrity. This research paper concludes that among all the algorithms of cryptography AES is the best one for secure data analysis and attacks.

Nadeem[16] has discussed the popular secret key algorithm AES, DES, 3DES, Blowfish, and their performances. It concluded that the algorithm Blowfish is more beneficial in comparison to the other algorithms and AES is better in terms of security than DES and 3DES. As the name suggests 3DES is 3 times slower than DES and it requires 3 times more amount of data to be processed.

Tamimi[25] has discussed in the research paper that the symmetric algorithms in which the comparison was made by the author were AES, DES, 3DES, and Blowfish. This includes two modes of operation ECB, CBC this also includes C# programming language for working. It concludes that AES is poor in time management as compared to other algorithms.

Apoorva et al [2] compared and thus discussed in the research paper about the symmetric algorithms of cryptography techniques for encryption and decryption. The author discussed the symmetric algorithms such as AES, TWOFISH, CAST-256, and BLOWFISH. The comparison among these symmetric algorithms takes place due to the performance and behaviour rate. The comparison of the symmetric keys was made on different scales such as as-speed, its size. The author of this research paper concluded that Blowfish symmetric algorithm is the best algorithm and is more powerful in comparison to the other algorithms. The clarity of the data is only visible on the basis of the size parameter and conclusion gives that Blowfish is the best algorithm in case of security measures. This research paper is based on different algorithms and thus their working and security reliability.

Mukund R.Joshi and Renuka Avinash Karkadi[15] discussed in the research paper on cryptography. The author mainly focuses on the cryptographic techniques and network security. This research paper involves the study and proper definition of the term network security and thus protecting it via cryptography and its algorithms. This research paper includes cryptographic principles and their types in detail. It discusses asymmetric and symmetric cryptography. This paper concludes that cryptography is a technique of security which involves the protection of data and thus network systems.

Cornwell [5] discussed in the research paper about the cryptographic keys and it mainly focuses on the BLOWFISH algorithm and thus, he concluded that the BLOWFISH algorithm in comparison with the other algorithms DES,3DES, AES is better in many ways like the security of data BLOWFISH is more reliable than the other algorithms and is more effective in key size, security of data and etc. he designed the particular BLOWFISH algorithm for the encryption of data and thus its security purposes and attacks in cryptography techniques.

Marwaha et al [12] discussed in the research paper about the three algorithms of the cryptography namely DES, 3DES, RSA. The DES and 3DES are symmetric algorithms which use the same key for encryption and decryption process "private" and "public" keys. While RSA algorithm is asymmetric key cryptography and uses different keys for encryption and decryption "public" or "private". They discussed in the research paper that the term security is valid and more useful for a the3DES algorithm in comparison to the other algorithms DES and RSA. It was concluded in this research paper that which algorithm is more secure and valid for the different keys of encryption and decryption process. For hacking purposes, the DES algorithm is very weak as it takes less time for the encryption and decryption of messages and thus is less secure in comparison to the other two algorithms 3DES and RSA.

Saini [19] discussed in the research paper about the different algorithms and its performances comparison DES, AES, RC2, RC6, 3DES, and BLOWFISH. He studied various research papers and tried to figure out that which algorithm is the best one. On the basis of table comparison and different studies on algorithms he compared different algorithms on the basis of the different keys, size, space, etc. he concluded that cryptography is something about what we see and what we get.

Abdul et al [1] discussed various algorithms of cryptography and their performances rate. They mainly discussed six algorithms AES, DES, 3DES, RC2, RC6, and BLOWFISH. These were compared so thus there performance rate were seen in the conclusion. They were compared on the parameter like key size, memory, security, shape, etc. their performances were noted and thus a very brief comparison was made between them their speed of encrypting and decrypting messages was also made and thus it was concluded that the BLOWFISH is the best performing algorithm in comparison to the other algorithms. The BLOWFISH algorithms followed by RC6 AND RC2 are good and more secure in comparison to the other algorithms. but these three algorithms have a disadvantage over the other algorithms in terms of the time-consuming power these algorithms were slow in comparison to AES,3DES, DES. They also concluded that 3DES is less secure in comparison to DES.

Seth et al [23] discussed in the research paper about the comparison of the algorithms mainly three algorithms were taken namely RSA, AES, DES. It was compared on the basis of their size, time, space and output results. He made various comparisons use different values and found that RSA uses more encryption time and its calculation was also very long and time taking it consumes more space and is less volatile than the other two algorithms. AES uses less space and DES is easy to calculate in comparison to the RSA algorithm.

Deepti Chaudhary and Rashmi Welekar [7] discussed in their research paper about the "visual cryptography". As the cryptography is based on the security of network issues similarly the visual cryptography is based on the visual information (text, picture, videos, etc") they are encrypted in such a way that decryption becomes mechanical operation .this research paper concluded about the visual security threats and their overcome. It also discusses the image processing.

Pallavi H. Dixit et al [17] discussed the multilevel network security and steganography. This paper presents level security in the network world. In this research paper the comparison on the basis of time, speed, and space was made and thus it is more beneficial for the embedded mobile security systems like ATM, mobile, online transactions, banking (online), smart card, visa, etc.

Yevgeniy does et al [27] discussed in the research paper about the cryptographic keys and preventing the particular system or network from data leakage. It mainly focuses on how to make our network strong and prevent the system from losing information to the thefts and securing it in a more efficient and possible way.

Singh et al [24] discussed in the research paper about the basic algorithms of cryptography AES, DES, 3DES, and BLOWFISH. The comparison was made on the basis of the size, speed, space and performance rate of encryption and decryption process. It was concluded that AES is the best algorithm in comparison to the other algorithm in many aspects like security issues and like space consumption and rate of encryption and decryption. But when we add the gate and some more functions to cryptographic techniques like XOR gate and HASH function then BLOWFISH is the best algorithm in all aspects in comparison to the other algorithms AES, DES,3DES.

Sandeep Dayal et al [20] discussed the various threats and their security measures and how a system can be protected by the different cryptographic techniques and keys. They discussed the various keys used in the research paper symmetric and asymmetric key of cryptography. There were different techniques for better security options thus the comparison was also made between the algorithms to secure the whole data network and which algorithm is best on the basis of their performances like size, area they acquire, speed of message decoding and encoding and thus the motive of this research paper was to made the whole network secure and safe to use in this digital world.

Table 1. Symmetric Encryption Techniques [21]

S.No	Encryption Technique	Granularity/(stream/block cipher)	Key size	Vulnerable to attack	Uniqueness about the technique
1	Caesar cipher	Block cipher	25 keys	Brute force attack	Simple substitution with alphabet
2	Playfair	Block cipher	25 keys	Brute force attack, Frequency analysis	Use pair of letters and substitute with 5*5 matrix designed with key and remaining alphabet
3	Hill cipher	Block cipher	25 keys	Known plaintext attack	Based on linear algebra, convert plaintext into matrix based on ASCII value
4	Vigenere cipher	Block cipher	25 keys	Frequency analysis, kasiski examination	Arrange the letters in 26*26 matrix and perform substitution with pair of letters
5	Vernam cipher	Stream cipher	25 keys	Known plaintext	XOR operation between plaintext bits and key bits
6	One time pad	Stream cipher	Equal to plain text size	Key and cipher text chosen	Same as vigenere cipher but here key size must be equal to plaintext size

Table 2. Asymmetric Encryption Techniques [21]

S. No.	Encryption Technique name	Granularity (Stream/ Block Cipher)	Key Size	Vulnerable to Attack	Uniqueness about the Technique
1	Camellia	Block Cipher (128 bits)	128,192 or 256 bits	Algebraic attack	16 rounds 8*8 S-boxes , Nested feistel network
2	Rijndael	Block Cipher (128 bits)	128,192 or 256 bits	Related key attack, algebraic attack	10,12,14 rounds (depending on the key size) maximal size of the input file of 2097152 bytes
3	Skipjack	Block Cipher (64 bits)	80 bits	Slide attack	32 rounds unbalanced feistel network structure

4	AES	Block Cipher (128 bits)	128,192 or 256 bits	Known plain text, side channel attack	Substitution-permutation network, 10 or 12 or 14 rounds
5	SEED	Block Cipher (128 bits)	128 bits	Chosen plain text, known plain text	16 rounds 8*8 S-boxes nested feistel structure, free to use
6	Twofish	Block Cipher (128 bits)	128 256 bits	Truncated differential cryptanalysis	16 rounds feistel structure free to use
7	RC2	Block Cipher (64 bits)	8-128 bits (64 bits)	Related key attack, Chosen plaintext	18 rounds source heavy feistel network structure
8	CAST-128	Block Cipher (64 bits)	40 to 128 bits	Chosen cipher text and known plain text	12-16 rounds feistel network structure
9	RC-5	Block Cipher (64, 128,32 bits)	0 to 2040bits (suggested 128 bits)	Differential attack	Feistel-like network,1 to 255 (suggested 12)
10	BLOWFISH	Block Cipher (64 bits)	32-224 bits	Second order differential attack, weak key	16 rounds feistel structure, free to use, key independent S-box
11	IDEA	Block Cipher (64 bits)	128 bits	Weak keys	8.5 rounds feistel network structure
12	TDES	Block Cipher (64 bits)	112 or 168 bits	Theoretically possible, Known plaintext. Chosen plaintext	48 rounds feistel network structure, three different keys used
13	DES	Block Cipher (64 bits)	56 bits	Differential and linear cryptanalysis, Brute force attacks	16 rounds feistel structures, left circular shift, substitution 32-bit swap

Table 3. Comparison of some Existing Algorithms

Title Name	Objective	Parameters	Conclusion	Year	Ref. No
“Performance comparison: security design choice”	The comparison of (DES ,3DES,RC2 AND AES)algorithms	Different encryption algorithms by .NET, Keys , size , space	AES is best algorithm. As compared to the other algorithm AES perform better security operations as compared the other one	2002	[7]
“Performance comparison of data encryption algorithms”	Discussed papules key algorithms AES, DES,3DES Blowfish &their performance	Implementation in java programming	Blowfish is best algorithm and AES is better in terms of security than DES, 3DES. 3DES is 3 times slower than	2008	[16]

			DES.		
“Performance analysis of Data encryption algorithms”	Comparison between the symmetric algorithms	Includes C# programming, Keys , size , space	AES is poor time management as compared to other algorithms and techniques.	2008	[25]
“Performance evaluation of symmetric encryption algorithms”	Discussed various &algorithm cryptography mainly 6 AES, DES,3DES,RC2,RC6& Blowfish	Key size, memory, security, shape, etc.	Blowfish is best followed by RC6 &RC2 but show & power consuming Others.	2009	[1]
“Blowfish survey”	Keys & mainly focuses on blowfish and compared with other algorithms	Key size, security of data , etc.	Blowfish is best algorithm. The comparison was made on the basis of the keys and their parameters and different algorithms.	2010	[5]
“DES, AES, Blowfish symmetric key cryptography algorithm 3 simulation based performance analysis”	Comparison between symmetric keys DES,AES and Blowfish	Between size (key, block) and speed	Blowfish is best. It was concluded that Blowfish was better than the other symmetric keys like DES & AES.	2011	[26]
“Comparative analysis of encryption algorithms for data communication”	Compression between three algorithm RSA,DES,AES	Size , time, space and output results	The conclusion after comparing many algorithms was made that RSA is long & take more time. AES uses less space &DES is easy to calculate	2011	[23]
“A study of new Trends in blowfish algorithms”	Basic algorithms ad their comparison AES,DES,3DES &blowfish	Size , speed , space and performance rate of encryption and decryption	AES is best algorithm. In this paper XOR gate & Hash function are also included and concluding that blowfish is best algorithm for cryptographic techniques.	2011	[24]
“A comparative survey on symmetric key encryption techniques”	User many cryptographic techniques to secure data	Symmetric , asymmetric encryption techniques, cipher text , plain text ,keys	Blowfish is more secure in terms of attack & security. As compared to the other cryptographic techniques for a more secure network.	2012	[13]
“Comparative	Symmetric algorithms	On the basis of speed and	Blowfish is the	2013	[2]

study of different symmetric key cryptography”	of cryptography technique	size	most powerful & best algorithm in terms symmetric and asymmetric keys and cryptographic techniques		
“Comparative analysis of cryptographic algorithms”	3 algorithms DES, 3DES and RSA	Public & private keys of symmetric/asymmetric keys	DES is slow and less secure than 3DES &RSA. The algorithm DES was stated best when compared to 3DES & RSA in this research paper.	2013	[12]
“A review on symmetric key encryption techniques in cryptography”	To get the proper know large of security system attacks uniqueness of parameters & techniques	Cryptography , symmetric keys , asymmetric key and cryptanalysis	To make data secure in the daily online crime based world.	2014	[21]
“A survey on encryption & decryption algorithms”	Review & survey symmetric & asymmetric technique &algorithms	On the basis of high security rate	It was concluded in this research paper that different symmetric and asymmetric keys were compared and a more secure network was created.	2014	[11]
“Survey on performance analysis of various cryptographic algorithms”	Comparison of algorithms DES, AES,RC2,RC6,3DES &Blowfish	Keys , size , space	Concluded that cryptography is the way to secure data and different algorithms were compared in this research paper.	2014	[19]
“Network security with cryptography”	Focuses on cryptographic technique &network security	Symmetric/asymmetric cryptography	This paper mainly concluded about the cryptography and their techniques .Cryptography is the technique of security which involves the protection of data	2015	[15]
“Secure authentication using visual cryptography”	Fourier on visual cryptography and image processing	Text, pictures, videos ,etc.	The conclusion was that Visual security threats are also increasing day by day so a better way to overcome it was made.	2015	[7]
“Multiple network security combining cryptography &	Multilevel network security &steganography uses	Time, speed , space	More beneficial for embedded system like ATMs, mobile,	2015	[17]

steganography on ARM platform”	Blowfish &LSB (least significant bit)		online transactions , banking (online)		
“Survey paper on cryptography”	Based on authentication &confidentially	Authentication and confidentiality , Keys , size , space	AES is more efficient &good for security purposes. This survey was based the authentication and confidentiality of the data.	2016	[9]
“A review of cryptographic algorithm in network security”	Study of algorithms & their comparisons	Plain text , cipher text , encryption ,decryption , security attacks	Symmetric algorithms are faster than a asymmetric algorithms. The conclusion was made on the basis of different algorithms	2016	[4]
“A survey on cryptography encryption algorithms”	Evaluation parameter like encryption & decryption time ,memory avalanche effect , entropy, correlation assessment	Encryption/ decryption time ,memory , avalanche effect , entropy ,correlation assessment	Hisea was most secure & blowfish was best for encryption and decryption. AES was best and good for avalanche effect	2017	[14]
“A survey on an enhanced cryptographic technique for massages encryption & decryption”	Different techniques algorithms here used and comparison was mod	Encryption /decryption keys , symmetric/asymmetric keys and cryptography	Encryption decryption text block & using a generated key without password. This concludes that the network is more secure in this algorithm based research paper	2017	[6]
“A research paper on cryptography encryption decryption compression techniques”	Focuses on key features lie data encryption ,decryption ,comparison cryptography , security integrity	Data encryption / decryption , compression , cryptography , security , integrity	AES is best among all algorithms as the survey was made between them on the basis of encryption and decryption techniques and cryptography scales and measures	2017	[22]
“Efficient public key cryptography in presence of key leakage”	Keys & preventing from data leakage	Cryptographic keys	This paper mainly concluded the data from leaking and making the system a secure one	2017	[27]
“A review paper on network security cryptography”	Discussed various keys & compared them.	Size , area they acquire, speed of message decoding and encoding	This research paper concludes that how To make network secure & safe from the online thefts.	2017	[20]

V. Conclusion

Cryptography is the very basic to secure a network or online data in such a way that the hackers or the third person who wants to hack our data or message cannot succeed in their task. In this digital world the crimes (cyber) are increasing day by day in such a way that are making a particular network unsecure to use and creating many crimes in their possible way. For overcoming these malicious activities cryptography was introduced and this work presents a survey that helps the researchers to find the gaps in the field of security. This work also shows a comparison table on the bases of objective, characteristics. Here the authors have compared the cryptographic algorithms and symmetric and asymmetric keys on the basis of different parameters and thus have made conclusions to the best algorithm which can make our network secure and authenticated and confidential one.

References

[1] Abdul D.S, Kader H.M Abdul, Hadhoud, M.M., “Performance Evaluation of Symmetric Encryption Algorithms”, Communications of the IBIMA, Volume 8, 2009, pp. 58-64.

[2] Apoorva, Kumar Yogesh, “Comparative Study of Different Symmetric Key Cryptography”, IJAIEM, Vol. 2, Issue 7, July 2013, pp.204-206.

[3] Babita and Gurjeet Kaur, "network security based on cryptography and steganography techniques", International Journal of advanced research in computer science. VOL 8, NO. 4, May 2017(special issue), pp. 161-165.

[4] B.Nithya and P.Sripriya" A review of cryptographic algorithms in network security". International journal of engineering and technology (IJET). Vol 8,no.1, FEB-MAR 2016. pp. 324-331.

[5] Cornwell Jason W, “Blowfish survey”, department of computer science, Columbus state university, Columbus, GA, 2010

[6] Darshana Patil and P.M.Chawan" A survey on enhanced cryptographic techniques for messages encryption and decryption". International journal of innovative research in computer and communication engineering. Vol 5, Issue 3,March 2017. pp. 3713-3719.

[7] Deepti Chaudhary and Rashmi Welekar, “secure authentication using visual cryptography”, International Journal of computer science and applications, vol 8, no. 1, JAN-MAR 2015, pp. 65-68.

[8] Dhawan Priya, “Performance Comparison: Security Design Choices”, Microsoft Developer Network October 2002.

[9] Harpreet Kaur, Vaishali Verma, Jaya Mishra." A survey paper on cryptography" International conference on innovative trends and technologies in engineering sciences and education. 8th & 9th September. www.conferenceworld.in. pp. 129-136.

[10] Kamal Kumar Gola, Zubair Iqbal, and Bhumika Gupta, "Modified RSA digital signature scheme for data confidentiality", IJCA (0975 – 8887) Volume 106 – No 13, November 2014

[11] M.Chanda Mona, S.Banu Chitra, V.Gayathri" A survey on various encryption and decryption algorithms". International journal of security and Singaporean journal of scientific research. VOL 6, NO. 6, 2014. pp. 289-300.

[12] Marwaha Mohit, Bedi Rajeev, Singh Amritpal, Singh Tejinder, “comparative analysis of cryptographic algorithms”, International Journal of advanced engineering technology/IV/III/ July Sep 2013/16-18.

[13] Monika Agrawal and Pradeep Mishra."A comparative survey on symmetric key encryption techniques". International journal on computer science and engineering (IJSCE).VOL.4, NO.5, May 2012. pp. 877-882.

[14] Muhammad Faheem Mushtaq, Sapiee Jamel,Abdul Kadir Hassan Disina, Zahraddeen A.Pindar,Nur Shafinaz Ahmad Shakir, Mustafa Mat Deris."A survey on the cryptography encryption Algorithms", International Journal of advanced computer science and applications, volume 8, number 11, 2017. pp. 333-344.

[15] Mukund R.Joshi and Renuka Avinash,”Network security with cryptography”. International journal of computer science and mobile computing(IJCSMC). VOL 4, Issue 1, January 2015, pp. 201-204.

[16] Nadeem Aamer, “Performance Comparison of Data Encryption Algorithms”, Oct 2008.

[17] Pallavi H.Dixit,Kamlesh B.Waskar, Uttam L.Bombale, “Multilevel network security combining cryptography and steganography on ARM platform", a journal of embedded systems, 2015, Vol 3, no. 1, pp. 11-15.

[18] Prerna Mahajan and Abhishek Sachdeva, "A Study of encryption algorithms AES, DES and RSA for security", Global Journal of CS and technology network, web and security. Vol 13, issue 15 version 1.0, year- 2013. pp. 15-22.

[19] Saini Bahar, “survey on performance analysis of various cryptographic algorithms”, International Journal of advanced research in computer science and software engineering, Volume 4, issue 4, April 2014, pp. 1-4.

[20] Sandeep Tayal, Nipin Gupta, Pankaj Gupta, Deepak Goyal, Monika Goyal.” A review paper on network security and cryptography”, advances of computational sciences and technology. Vol 10, no. 5, 2017, pp. 763-770.

[21] Saranya K, Mohanapriya K, Udhayan J."A review on symmetric key encryption techniques in cryptography". International journal of science, engineering, and technology research(IJSETR), VOLUME 3, issue 3, March 2014. pp.539-544.

[22] Sarita Kumari"A research paper on cryptography encryption and compression techniques". International journal of engineering and computer science. VOL 6,Issue 4,April 2017.pp. 20915-20919.

[23] Seth Shashi Mehrotra, Mishra Rajan, “Comparative analysis of Encryption algorithm for data communication”, International Journal of Computer Science and Technology, vol. 2, Issue 2, June 2011, pp. 292-294.

[24] Singh Gurjeevan, Kumar Ashwani, Sandha K.S. “A Study of New Trends in Blowfish Algorithm” International Journal of Engineering Research and Applications (IJERA), Vol. 1, Issue 2, pp.321-326

[25] Tamimi A. Al., “Performance Analysis of Data Encryption Algorithms”, Oct 2008.

[26] Thakur Jawahar, Kumar Nagesh. “DES, AES, and Blowfish Symmetric Key Cryptography algorithm3 Simulation-Based Performance Analysis”, IJETAE, Vol. 1, Issue 2, DEC. 2011, pp. 6-12.

[27] Yevgeniy Dodis, Kristiyan Haralambiev, Adriana Lopez-Alt, Daniel Wichs, "Efficient public-key cryptography in the presence of key leakage”, computer science dept. august 17, 2017. pp. 1-33.