Comparative Survey of different Cryptographic Algorithm

Alka Pandey **Dr. M.A. Rizvi**

Abstract- Now days, Data security is very challenging issue that touches many areas including computers and communication. Recently, came across many attacks on cyber security that have played with the confidentiality of the users. These attacks just broke all the security algorithms and affected the confidentiality, authentication, integrity, availability and identification of user data. Cryptography is one such way to make sure that confidentiality, authentication, integrity, availability and identification of user data can be maintained as well as security and privacy of data can be provided to the user. Cryptography is used widely for the purpose of secure communication and password management. It comprises the techniques of encryption and decryption mechanism. Encryption is the process of converting normal data or plaintext to something inexplicable or cipher-text by applying mathematical transformations or formulae. These mathematical transformations or formulae used for encryption processes are called algorithms.

In this paper we have analysed ten data encryption algorithms AES, DES, RSA, DIFFIE HELLMAN, THREEFISH, CLEFIA, ARIA, SPEAK, SIMON and CHIASMU etc, comparing their different parameters. So that in future the best algorithm method can be used for encryption and decryption of data.

Index Terms— Security, Cryptography, Algorithm, Key, Cipher, Security attacks, Encryption, Decryption.

1 Introduction

Need of communication has no alternative since early ages. Today method of communication got improved and now it has widely transformed in technical ways. Along with social communication the exchange of information is also needed where privacy and safety play important role. [1]

The need of exchanging information without being hacked theft or distorted gave birth to encryption and decryption of information. [2]

The concept behind encryption and decryption to disorganizing or rearranging the information in an unreadable way, this concept of information to protect the information in an unreadable manner is refer to Cryptography. Cryptography is derived from two Greek words: "Kryptos" meaning 'hidden' and "graphein" meaning 'to write' i.e. hidden writing. The main feature of Cryptography is the use of a secret key to encrypt and decrypt the sensitive information. Cryptography is not only restricted to providing confidentiality and privacy but also provides authentication, data integrity, non repudiation etc. Parameters considered while adopting a Cryptographic techniques can be broadly divided into two broad spectrums: Asymmetric key Cryptography and Symmetric key Cryptography. Symmetric key Cryptography uses a single key for the purpose of encryption and decryption, and is shared with both the sender and the receiver.

- *Ms. Alka Pandey is currently pursuing masters degree program in Computer technology Application in Rajiv Gandhi prodyogiki vishwavidyalaya, Bhopal, India,. E-mail: alka141191@gmail.com*
- ***Dr. M.A. Rizvi** is currently working as Associate and Head professor in NITTTR ,Bhopal ,India,E-mail: marizvi@nitttrbpl.ac.in*

It is one of the earliest used techniques of Cryptography. Asymmetric Key Cryptography on the other hand uses two keys for the purpose of encryption and decryption.

A Cryptographic protocol is a procedure carried out between two parties which is used to perform some security task. Typically cryptographic protocol makes use of one, or more, cryptographic primitives and/or schemes. An example might be the transmission of a credit card number from Bob to an e-commerce web site Alice. Such a protocol might involves a digital signature scheme9so Bob knows he is talking to Alice), and a form of encryption (to ensure Bob's credit card details are not intercepted in transit). Examples of deployed protocols which perform such operations are TLS or IP-Sec.

2. BASIC TERMS OF CRYPTOGRAPHY

Encryption - It is the act of obscuring a message by mystifying its contents. It can also be used to create digital signatures, which helps in the authentication of a original message.

Decryption – It is the inverse process of encryption. Usually the cipher text or algorithm used for encryption is the one used for decryption.

Cipher – It is method, an algorithm function or process for performing encryption or decryption. A cipher is a set of well defined steps which can be followed to Crypt data.

Plaintext - any information before being encrypted or in its original undisturbed form.

Cipher text - It is the output or the incomprehensible code obtained by encryption of the plain text.

Cryptanalysis - It is the act of trying to decipher an encrypted message without the cognition of the

actual keys or the algorithm used during encryption. The Cryptanalyst may have some part of the plaintext and is interested in the rest of it have the cipher text and may want to know about the key and algorithms used. [4]

Cryptographic Attacks - They are classified as

1) **Passive attack** - The goal here might be to only read the contents of a message and not change anything.
2) **Active Attack** - The goal here is to change the contents of the message to disable future use or understanding of the message.

Cryptanalytic Technique -

2) Cipher Text Only - The attacker tries to decipher the message without having the knowledge about the kind of information contained in the message and must conjecture from the cipher text only. **Known Plaintext Attack** – It is easy to predict or guess some part of Plaintext for Attackers.

3) Man - in - the - Middle Attack - The idea behind this attack is to interpose the communication between two parties. The attacker can access the traffic, information, modify the original form and then forward it to the receiver. Such attacks can be prevented by public key encryption.

4) Correlation - The main source of information in the communication are the correlation between the secret key and the cipher text, and hence it enables the attackers.

5) Attack Against or Using the Underlying Hardware

These attacks make use of the data of the very fine measurements of the cryptographic device to compute the key and the encryption information.

6) **Faults in the Cryptosystem** - These can even lead to the discovery of the secret key [4]

3. NEED OF CRYPTOGRAPHY

In the field of sharing information, data and important files it has become mandatory. Not only in communication but also in defence areas, commercial field and to protect individual data as well as extensive applications in our daily lives. The technique of cryptography covers all these parameters of security issues. It has become very essential tool in protecting the sensitive information from unauthorized access and to provide information security. [6]

4. SPECIFIED PROTOCOL USED IN DATA SECURITY

The protocols here were designed for specific tasks.

4.1 TLS

General Description: The TLS protocol (the current version v1.2) is primary aimed at securing traffic between an unauthenticated web browser and an authenticated web site, although the protocol is now often used in other application due in part of the availability of a verity of libraries implementing TLS. The TLS protocol suite aims to provide a confident ail channel rather than simply a key agreement protocol. The protocol is broken up into two phases: A handshake (or key agreement) phase and a record layer encryption phase. [6]

Limitation: Due to the non-systematic development process, the protocol is hard to analyse and easily prone to implementation weaknesses. [7]

4.2 SSH

General Description: Secure Shell (SSH) was originally designed as a replacement for insecure remote shell protocol such as telnet. It provides a secure channel between two networked computers for applications such as secure file transfer. In general the host one is connecting to be authenticated, whereas the client is not (although some corporations do insist on client side authentication for SSH usage). [16]

Limitation: The main issues with SSH, much like TLS, is that most of the standard encryption algorithm for the transport layer are not sufficient to ensure complete security. They possess a number of cryptographic weaknesses, which would not exist if the protocol choices had been made more recently.

4.3 IPSec

General Description: IPSec provide security at the IP network layer of the TCP/IP protocol stack. This differs from protocols such bas TLS and SSH, which provide security at higher layers such as the application layer. The main use of IPSec has been to create virtual private network (VPNs) which facilities secure communication over an untrusted network such as the internet. [11] There are two main IPSec protocols which specify the actual cryptography processing applied to packets. These are called Authentication Header and Encapsulating security payload.AH provides integrity protection, data origin authentication and anti-reply service.ESP provides similar service to AH and in addition provides confidentiality and traffic flow confidentiality service through symmetric key encryption and variable length padding of packets.Limitation: The key agreement phase of IPSec, called IKE, is well studied and well defined. As for TLS ads SSH the payload encryption algorithm has had a number of issues over the years, related to pour acceptance of the need for AEAD? IND-OCA encryption algorithm.

4.4 Kerberos

General Description: Kerberos is an authentication service which allows a client to authentication his or herself to multiple services e.g. a printer or a file server. It uses a trusted authentication server which will grant tickets to participating users or parties allowing them to show their identity to each other.

It is primarily based on symmetric –Key primitives; the specific construction being derived from the Needhaam-Schroeder protocol. Public key primitives, namely RSA signature, may also be used during the initial authentication phase. [16] Limitations: Again there are issues related to the usage of strong encryption schemes due to the age of the documents defining the protocols.

5. ASSESSMENT ON DIFFERENT CRYPTOGRAPHIC ALGORITHMS

5.1 DES

It was found by IBM in the year 1977, which is a symmetric key algorithm which was found by IBM in the year 1977. This algorithm uses a block size of 64bits and a key size of 54bits. This algorithm is a block cipher and it uses feistel network to transfer messages. It takes about 16 rounds to convert messages and its network security can be broken by brute force attack. Advantage of this algorithm is that DES has been around a long time, no real weakness has been found, and very efficient attack is still found to be brute force attack

5.2 RSA

Rivest-Shamir-Adleman (RSA) is asymmetric algorithm developed by Ron Rivest, Adi Shamir and Leonard Adleman in the year 1977. This algorithm uses a key size greater than 1024bits and its block size depend on the key size that is being used. Block size is often calculated with a formula i.e. 1+floor ((x-1)/8)' where x is the key size Benefit of this algorithm is that it uses public key to transfer messages and also provides security to digital signatures that cannot be repudiated. Drawback of the algorithm is that even though the public key is safe its speed is comparatively low. [12]

5.3 AES

Rijndael was selected as the (AES) Advanced Encryption Standard in Oct-2000 Designed by Vincent Rijmen and Joan Daemen in Belgium NIST. This algorithm uses a key size of 128, 192 or 256bits and a block size of 128, 192 or 256bits. Benefit of this algorithm is that it is more secure and faster in both hardware and software. Drawback of the algorithm is that it needs more processing and requires more rounds of communication when compared to DES.

5.4 Diffie-hellman

Diffie-hellman was found by Whitfield diffie and martin Hellman in the year 1976. This algorithm doesn't have specified key size because it uses key exchange management and has a block size of 64bits.

5.5 Aria

Aria algorithm was found by South Korean researchers in the year 2003. This algorithm has a key size of 128, 192 or 256bits and a block size of 128bits. It is a block cipher and uses substitution permutation network to transfer messages. It takes 12, 14 or 16 rounds to convert a message and its security is broken by man in the middle attack. Benefit of this algorithm is that data and indexes are crash safe and it can replay almost everything from the log. Therefore, you make a backup of aria by just copying the log.

5.6 Clefia

Clefia algorithm was found by Sony in the year 2007. This algorithm has a key size of 128, 192 or 256bits and a block size of 128bits. this algorithm is that the last feature of 4 branch structure because of diffusion speed of smallest F-functions is slower. [13]

5.7 Threefish

Threefish algorithm was found by Bruce shinier, Neils Ferguson, Stefan lucks, Doug whiting, Mihir bellare, Tadayoshi kohno, Jon callas and jess walker in the year 2008. This algorithm has a key size of 256, 512 or 1024bits and a block size of 256, 512 or 1024bits. It is a block cipher and uses feistel network to transfer messages. It takes 72 rounds to convert a message and its security is broken by boomerang attack. Benefit of this algorithm is that it provides a good and secured class of keys. Drawback of this algorithm is that it consumes a lot of memory. [14]

5.8 Speck

Speck was found by Ray Beaulieu, Doughlas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks and Louis wingers in NSA in the year 2013. This algorithm has a key size of 64, 72, 96, 128, 144, 192 or 256bits and a block size of 32, 48, 64, 96, or 128bits. It is a block cipher and uses ARX network to transfer messages. It takes 22, 23, 26, 27, 28, 29, 32, 33 or 34 rounds to convert a message and its security is broken by rectangle attack. computationally simple technique. Drawback of this algorithm is that in speck the blocks are recursively and adaely partitioned such that high energy area are grouped together into smaller sets and low energy areas are grouped together as larger sets.[16]

5.9 Simon

Simon was found by Ray Beaulieu, Doughlas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks and Louis wingers in NSA in the year 2013. This algorithm has a key size of 64, 72, 96, 128, 144, 192 or 256bits and a block size of 32, 48, 64, 96, or 128bits.Drawback of this algorithm is that it examines an oracle problem which takes polynomial time on quantum computes but exponential times on a classical compute. [16]

5.10 Chiasmus

Chiasmus was found by BSI in the year 2013. This algorithm has a key size of 160bits and a block size

of 64bits. It is a block cipher and uses substitution permutation network to transfer messages. It takes 12 rounds to convert a message and its security is broken by man in the middle attack. Benefit of this algorithm is that it is easy to install and the draw-back is that its hardware product is subjected to greater risks than a hardware solution.

6. ANALYSIS OF DIFFERENT CRYPTOGRAPHIC ALGORITHM

Table 1 (analysis of different cryptographic algorithm).

PARAMETERS	AES	DES	RSA	DIFFIE-HELLMAN	THREEFISH	CLEFIA	ARIA	CHIASMUS	SIMON	SPECK
DEVELOPER	Vincent Rijmen and Joan Daemen in Belgium NIST	IBM	Rivest, Adi Shamir and Leonard Adleman	Whitfield diffie and martin Hellman	Bruce schneir, Neils ferguson, Stefan lucks, Doug whiting, Mihir bellare, Tadayoshi kohno, Jon callas and jess walker	Sony	South Korean researchers	BSI	Ray Beaulieu, Doughlas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks and Louis wingers	Ray Beaulieu, Doughlas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks and Louis wingers
YEAR	2000	1977	1977	1976	2008	2007	2003	2013	2013	2013
KEY SIZE	128, 192 or 256bits	56bits	>1024bits	uses key exchange management	256, 512 or 1024bits	128, 192 or 256bits	128, 192 or 256bits	160bits	64, 72, 96, 128, 144, 192 or 256bits	64, 72, 96, 128, 144, 192 or 256bits
BLOCK SIZE	128, 192 or 256bits	64bits	Depends on key size	64bits	256, 512 or 1024bits	128bits	128bits	64bits	32, 48, 64, 96, or 128bits	32, 48, 64, 96, or 128bits
ROUNDS	10,12 or 14	16	1 round for each message	14	72	18, 22 or 26	12, 14 or 16	12	32, 36, 42, 44, 52, 54, 68, 69 or 72	22, 23, 26, 27, 28, 29, 32, 33 or 34
CIPHER TYPE	Rijndael Cipher	Block Cipher	Block cipher	symmetric key cipher	Block cipher	Block cipher	Block cipher	block cipher	block cipher	block cipher
NETWORK TYPE	Feistel Network	Feistel Network	Common network	Common network	Feistel network	Feistel network	ssubstitution permutation network	substitution permutation network	Feistel network	ARX network
SECURITY ATTACKS	Chosen plain attack	Brute Force Attack	Timing attack	Eaves dropping	Boomerang attack	Cache poisoning attack	man in the middle attack	man in the middle attack	chosen cipher text attack	rectangle attack
MERITS	more secure and faster in both hardware and Software	no real weakness has been Found	uses public key, provides security to digital signatures that cannot be repudiated	security factors in solving discrete algorithm is very challenging, the shared key is never itself transmitted over the channel	Provides a good and secured class of keys	Enhanced implementation efficiency in terms of both hardware and software, high speed operation	data and indexes are crash safe	Easy to install	It solves black box problem, takes advantage of quantum effect	Image coding has been a very effective and computationally simple technique
DEMERITS	needs more processing	possibility to break the encrypted code in DES	speed is comparatively low	Lack of authentication	consumes a lot of memory	last feature of 4 structure diffusion speed of smallest F-functions is slower	merge tables don't support aria	Hardware product is subjected to greater risks	Examines an oracle problem	Recursively and adaptively partitioned

After analyse (Table 1) all the above defined cryptography technique it can be concluded that there is no algorithm that is considered to be fully secured, all algorithms has its own pros and cons. Till today AES and DES algorithms are used in almost all system. AES is a Rijndael cipher and it is fast too . In DES even now there is no real weakness has been found and the most efficient attack is still brute force attack. But some feel that as

Technology is improving day by day there is a possibility to break the encrypted code in DES. AES is considered to be more secure and it is faster in both hardware and software. By design AES is faster in highlight their differences in terms each of 16 rounds. But AES actually needs more processing. Three fish algorithm provides good and secured class of keys but the problem it has is it consumes a lot of memory. For banks and credit cards RSA algorithms are more preferred as they provide security to digital signatures that can be repudiated by the hackers. Because of this reason RSA is still used in banks. As mentioned earlier every algorithm has its own merits and demerits, the user must decide to choose appropriate algorithms that will best suite his needs.

7. CONCLUSION

In this paper, we have analysed various encryption algorithms. We have found that each algorithm has its own benefits according to different parameters. Based on the comparisons made on different cryptographic algorithms such as AES, DES, Clefia, speck and RSA etc, we found that in this internet world nowadays, security of data play a major role as data and communications are passed and are done over open networks very often. From our evaluation, we found that in cryptographic algorithms symmetric encryption technique and asymmetric encryption techniques both have a higher ratio for encryptio

8. REFFERENCES

[1] Mitali, Kumar Manoj, Sharma Arvind, "A Survey in various cryptography techniques", IJETTCS, volume 3, Issues 4, July August 2014, ISSN2278-6856.

[2] Ritu Tripathi, Sanjay Agrawal, "Comparative Study of Symmetric and Asymmetric Cryptography Techniques", International Journal of Advance Foundation and Research in Computer (IJAFRC),volume 1,issue 6,june 2014, ISSN 2348 – 4853.

[3] Apoorva, Yogesh Kumar," Comparative Study of Different Symmetric Key Cryptography Algorithms",
International Journal of Application or Innovation in Engineering & Management (IJAIEM),volume 2,issue 7,july 2013, ISSN 2319 – 4847.

[4] Mohit Marwaha, Rajeev Bedi, Amritpal Singh, Tejinder Singh "Comparative Analysis of Cryptographic Algorithms", International Journal of Advanced Engineering Technology, EISSN 0976-3945.

[5] Ms. Ankita Umale, Ms. Priyanka Fulare, " Comparative Study of Symmetric Encryption techniques for Mobile Data Caching in WMN", The International
Journal Of Engineering And Science (IJES).

[6] Monika Agrawal, Pradeep Mishra," A Comparative Survey on Symmetric Key Encryption Techniques",
International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 05 May 2012, PP877-882.

[7] An overview of Cryptography www.graykessler.net/library/crypto.html.

[8] What is symmetric Key Cryptography? Webopedia http://www.webopedia.com/terms/symmetric-key-cryptography.html.

[9] Symmetric-key -HowstuffWorks htttp://computer.howstuffwork.com/encryption2.htm.

[10] M. Kumar and E. G. Dharma, "A comparative analysis of symmetric key encryption algorithm",
IJARCET, vol. 3, no. 2, **(2014)**.

[11] Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani, "New Comparative Study Between DES, 3DES and AES within Nine Factors", Journal Of Computing, ISSN
2151-9617.

[12] O.P Verma, RituAgarwal, DhirajDafouti and ShobhaTyagi, "Performance Analysis of Data Encryption Algorithms", IEEE Delhi Technological University,
India, 2011.

[13] Brown Lawrie, Steflik Dick, "Symmetric Encryption Algorithm", CS-480b, Lecture slide (ppt).

[14] MajdiAl-qdah& Lin Yi Hui "simple Encryption/Decryption Application" published in International Journal of computer science and security, volume(1):Issues(1).

[15] A. Kakkar and M. L Singh, "Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in Multimode Network", Published in International Journal of engg, and technology(IJET), vol. 2, no. 1, **(2012)**.

[16] Y. F. Huang, "Algorithms for elliptic curve diffie-Hellman key exchange based on DNA title self assembly", Proceedings of 46th IEEE Theories and
Applications, **(2008)**.

[17] K.B. Priya Iyer, "Comparative Study on Various Cryptographic Techniques", International Conference on Communication, Computing and Information Technology (ICCCMIT-2014).