International Journal of Information Movement Vol.2 Issue II (June 2017)
Website: www.ijim.in ISSN: 2456-0553 (online) Pages 1-7

ANALYSIS OF VARIOUS ENCRYPTION TECHNIQUES

Ms. Aruna Trehan
M.Tech Student
Department of Electronics and Communication Engineering
SSIET, Derabassi
Email: aruna.trehan@gmail.com

Mrs. Parminder Kaur
Assistant Professor
Department of Electronics and Communication Engineering
SSIET, Derabassi
Email: parmindersandal@yahoo.com

Mr. Manpreet Singh
Assistant Professor
Department of Electronics and Communication Engineering
GNA University
Email: manpreetrai01@gmail.com

Abstract:- Cryptography is concerning correspondence in the span of an adversary. It joins assorted subjects like encryption, check, and key assignment to term a couple. The earth of present cryptography gives a hypothetical stronghold concentrated concerning that one can fathom what definitely these subjects are, the best way to assess traditions that infer to light up them and how to gather traditions in whose protection one can have conviction. Elevated automated advances have made mass media data by and colossal available. Starting late, mass media procurements become vital in exercise and alongside these lines protection of sight and sound data have gotten average concern In this paper we analyze the encryption and decryption time of various algorithms on different settings of data.

Keywords: Cryptography, DES, TDES, AES.

Cryptography is the science of retaining mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive data or dispatch it across insecure webs (like the Internet) so that it cannot be elucidate by anybody except the aimed recipient.

1.1 Cryptography:- Cryptography is the science of safeguarding data; cryptanalysis is the science of analyzing and obliterating safeguard communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, appeal of mathematical instruments; chart discovering, patience, determination, and luck. Cryptanalysts are additionally yelled attackers. Cryptology embraces both cryptography and cryptanalysis. Cryptographic strength is measured in the period and resources it must to demand to recoup the plaintext. The consequence of forceful cryptography is cipher text that is incredibly tough to decipher lacking ownership of the appropriate decoding tool. How difficult? Given all of today's computing manipulation and obtainable time even a billion computers substituting a billion checks a second t is not probable to decipher the consequence of forceful cryptography beforehand the finish of the universe. One must to contemplate, consecutive, that forceful cryptography must to grasp up rather well opposite even an incredibly motivated cryptanalyst. Who's candidly to say? No one has proven that the strongest encryption obtainable nowadays will grasp up below tomorrow's computing manipulation.

1.2 HOW DOES CRYPTOGRAPHY WORK?

A cryptographic algorithm, or cipher, is a mathematical aim utilized in the encryption and decryption process. A cryptographic algorithm works in combination alongside a key—a word, number, or phrase—to encrypt the plaintext.The comparable plaintext encrypts to disparate cipher text alongside disparate keys. [1] The protection of encrypted data is completely reliant on two things: the strength of the cryptographic algorithm and the secrecy of the key. A cryptographic algorithm, plus all probable keys and all the protocols that make it work encompass a cryptosystem. PGP is a cryptosystem.

2.0. IMAGE ENCRYPTION TECHNIQUES

Image encryption is a method that provides protection to pictures by changing early picture to one more picture that is tough to understand. Countless encryption methods are continuing that are utilized to circumvent the data stealing. Picture encryption has requests in internet contact, multimedia arrangements, health imaging, telemedicine, martial contact, etc.

2.1 Basic Terms Used in Cryptography

2.1.1 Plain Text- The original message that the person wishes to communicate with the other is defined as Plain Text. In cryptography the actual message that has to be send to the other end is given a special name as Plain Text. Like , Marry is a person wishes to send "Hey my friend" message to the person Tom. Here "Hey my friend" is a plain text message.

2.1.2 Cipher Text- The message that cannot be understood by anyone or meaningless message is what we call as Cipher Text. In Cryptography the original message is transformed into non readable message before the transmission of actual message. For example, "Ajd#@91uk*^5%" is a Cipher Text produced for "Hey my friend".

2.1.3 Encryption- It is the method for converting the Plain Text into Cipher Text.this process is called as an Encryption. Cryptography uses the encryption technique to send confidential messages through an insecure channel. It requires two things- an encryption algorithm and a key. An encryption algorithm is the technique that has been used in encryption of plain text message. Encryption takes place at the side of sender.

2.1.4 Decryption- It is a process of converting Cipher Text into Plain Text. Cryptography uses the decryption technique at the receiver side to obtain the original message from non readable message (Cipher Text). It also requires two things- a Decryption algorithm and a key. A Decryption algorithm means the technique that has been used in Decryption to decrypt the cipher text message. Normally the encryption and decryption algorithm are same.

2.1.5 Key- A Key is defined as a numeric or alpha numeric text or may be a special symbol. The Key is used at the time of encryption takes place on the Plain Text and at the time of decryption takes place on the Cipher Text. The selection of key in Cryptography is very essential as the security of encryption algorithm depends directly on it. For example, if the Marry uses a key of 3 to encrypt the Plain Text "President" then Cipher Text produced will be "Suhvlghqw".

3.0 Purpose of Cryptography

Cryptography provides a number of security goals to ensure the privacy of data, non alteration of data and so on. Due to the great security advantages of cryptography it is widely used today. Following are the various goals of cryptography.

3.1 Confidentiality- Information in computer is transmitted and has to be accessed only by the authorized party and not by anyone else.

3.2 Authentication- The information received by any system has to check the identity of the sender that whether the information is arriving from a authorized person or a false identity.

3.3 Integrity- Only the authorized party is allowed to modify the transmitted information. No one in between the sender and receiver are allowed to alter the given message.

3.4 Non Repudiation- Ensures that neither the sender, nor the receiver of message should be able to deny the transmission. Access Control- Only the authorized parties are able to access the given information.

4.0 Classification of Cryptography

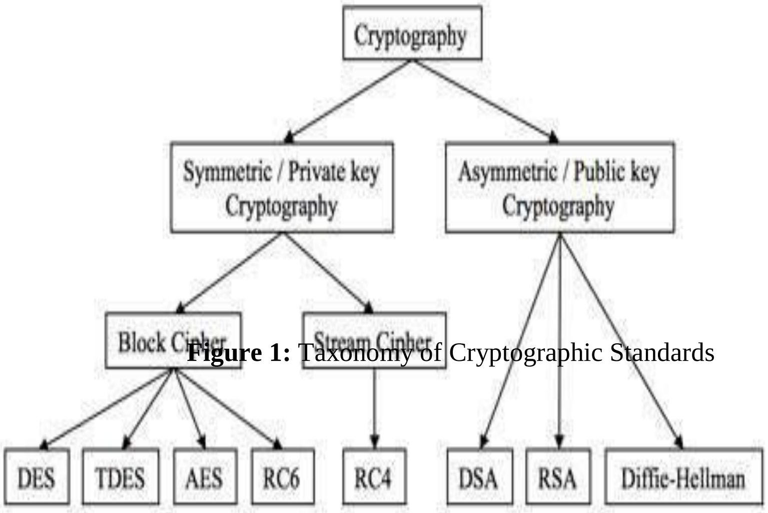


Figure 1: Taxonomy of Cryptographic Standards

Encryption algorithms can be classified into two broad categories- Symmetric and Asymmetric key encryption.

4.1 Symmetric Encryption- In symmetric Cryptography the key used for encryption is similar to the key used in decryption. Therefore the key distribution has to be made prior to the transmission of information or data. The key plays a very essential role in symmetric cryptography as their security directly rely on the nature of key i.e. the key length etc. There are various symmetric key algorithms such as DES, TRIPLE DES, AES, RC4, RC6,BLOWFISH[2]. There are various encryption algorithms (encryption standards) in the field of cryptography. These are symmetric and asymmetric encryption algorithm. Some basic symmetric encryption algorithms are studied and detailed below:-

4.1.1 DES- The DES (Data Encryption Standard) was created by IBM in 1975.It was the first encryption standard and remained a worldwide standard for a long time and was replaced by the new Advanced Encryption Standard (AES) [2].It offers a basis for comparison for various algorithms .DES is a block cipher based symmetric algorithm, same keys are used for both encryption and decryption. 56 bits key is used by DES.It encrypts the data in 64 bits blocks of data. By using it three times ,the Triple DES (TDES) i.e block cipher is formed from the DES cipher [1].DES is not so strong Many attacks recorded against it.

4.1.2 Triple DES- It is a block cipher formed from the DES cipher by using it three times[1].This standard was created by IBM in 1978.When it was found that a 56-bit key of DES is not so strong against brute force attacks and many other attacks, TDES was made as a same algorithm with long key size. In 3DES, DES is performed three times to improve security. It is also a block cipher technology having key size of 168 bits and block size of 64 bits.DES is performed three times, so it is slower algorithm [2].Triple DES has low performance in terms of power consumption and throughput when compared with DES. It’s process is time consuming as it requires more time than DES because DES is repeated three times [7].

4.1.3 Blowfish- It is Block cipher based encryption algorithm provided by Bruce Schneider.. It has variable length key ranging from 32 bits to 448 bits and block size of 64 bits. [1] [2].The algorithm operates with two parts: a key expansion part and a data encryption part. The role of key expansion part is to converts a key of at most 448 bits into several sub key arrays to taling 4168 bytes. All operations are performed by EX-ORs and additions on 32-bit words. [3] It endures from weak key problems.Therefore some attacks are possible against it [5].

4.1.4 RC4- It is a stream cipher algorithm designed in 1987 by Ron Rivest for RSA Security. It is having key size of 40 or 2048 bits. It functions with byte-oriented operations. The algorithm is depend on the use of a random permutation. By RSA Security,the RC4 was kept as a trade secret. In September 1994, the RC4 algorithm was anonymously posted on the Internet on the Cypherpunks anonymous remailer"s list [13].The RC4 algorithm is simple and easy to explain [1].RC4 is suited for text data [7].

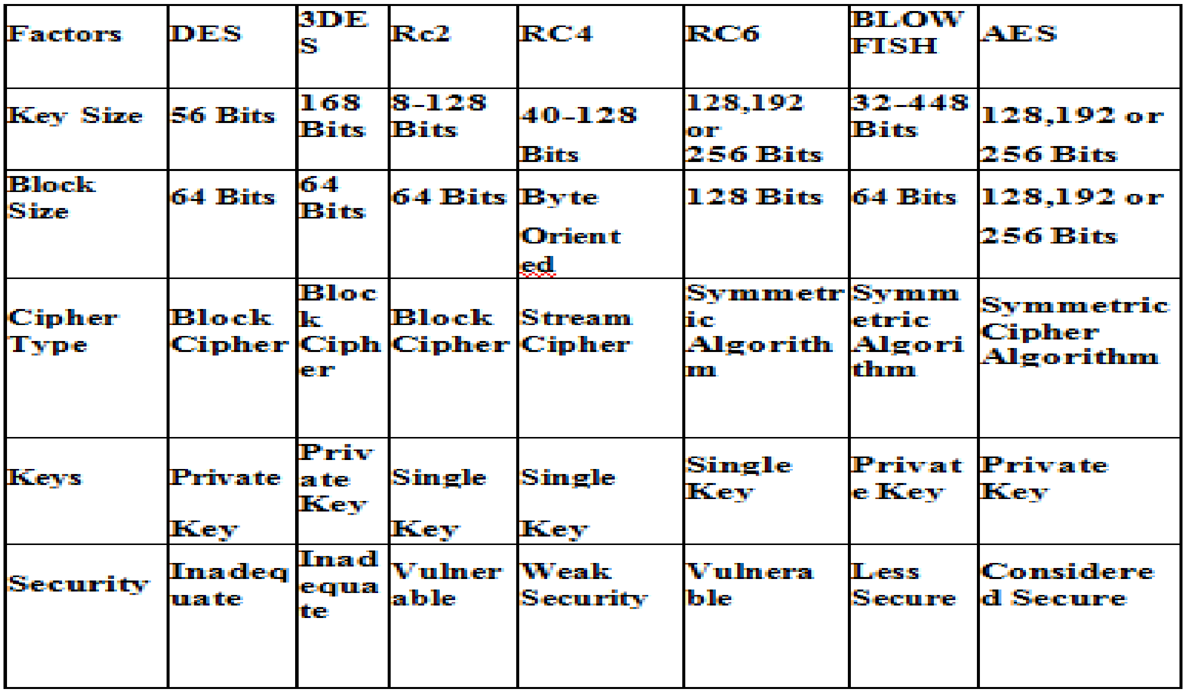
4.1.5 **RC2-** It is a symmetric block cipher based technology developed by RSA Data security. It works on block size of 64 bit and make use of variable size keys ranging from 8-128 bits[5].RC2 has disadvantage over other algorithms in terms of time consumption. RC2 is insecure to differential attacks [7].

4.1.6 RC6- It is more accurately specified as RC6-w/r/b where the word size is w bits, encryption consists of a nonnegative number of rounds r, and b denotes the length of the encryption key in bytes [4]. RC6 uses a block size of 128 bits and having key sizes of 128, 192 and 256 bits. It is same as to RC5 in structure. It is symmetric cipher algorithm.RC6 is insecure to brute force attacks [5].

4.1.7 AES- It is most widely adopted encryption standard.AES was originally called Rijndael. This standard was created by Joan Daemen and Vincent Rijmen in 1998.The Advanced Encryption Standard (AES) algorithm is a symmetric block. AES algorithm can encrypt and decrypt the plaintext and cipher text of 128-bits. It uses variable length key of size 128,192,256 bits [5].The number of rounds in the encryption or decryption processes depends on the key size used by it. General operation is therefore similar to the Data Encryption Standard (DES) .It requires very low RAM space and is very fast. [4] .It can be used for encryption of Text, Audio, and Image data.AES provides excellent Data Security [1] [2].

COMPARISON TABLE

This table compares the above stated encryption standards based upon different factors.



Factors	DES	3DES	Rc2	RC4	RC6	BLOWFISH	AES
Key Size	56 Bits	168 Bits	8-128 Bits	40-128 Bits	128,192 or 256 Bits	32-448 Bits	128,192 or 256 Bits
Block Size	64 Bits	64 Bits	64 Bits	Byte Oriented	128 Bits	64 Bits	128,192 or 256 Bits
Cipher Type	Block Cipher	Block Cipher	Block Cipher	Stream Cipher	Symmetric Algorithm	Symmetric Algorithm	Symmetric Cipher Algorithm
Keys	Private Key	Private Key	Single Key	Single Key	Single Key	Private Key	Private Key
Security	Inadequate	Inadequate	Vulnerable	Weak Security	Vulnerable	Less Secure	Considered Secure

5.0 Literature Survey/Related work

S. Sharma, L. Kumar in [11] has proposed an encryption algorithm for audio file using RSA algorithm.RSA is asymmetric encryption technique. In this paper a frequency domain of the wave audio signal is taken for the encryption and decryption. An audio signal can be separated into different frequency bins with respect to phase and magnitude values by applying DFT on the audio signal. RSA technique is used for the encryption and decryption on the lower frequency bands because all the frequency regions do not participate equally in the communication. After applying the encryption on different frequency bands, it is observed that, the encryption on the lower frequency band is more effective than the higher one. The technique is applied on phase values.

B. Gadanayak, C. Pradhan, Utpal Chandra Dey in [12] has compared different encryption techniques on MP3 compression. These techniques are applied on audio data, for securely transmitting audio data over the network. Total Data Encryption Standard (DES), total Advanced Encryption Standard (AES) and selective AES encryption techniques are applied on the quantized audio data. A comparison between these encryption techniques is discussed by calculating the time consumption as well as SNR values. Experimental results demonstrate that the time consumption for selective AES encryption on MP3 compression is less than total AES and DES encryption techniques on MP3 compression. So, the selective encryption technique is better than total DES and AES encryption techniques as it takes less time with degradation of signal that is inaudible to the unauthorized users. That the selective AES encryption technique is better than the other two encryption techniques

B. Gadanayak, C. Pradhan in [13] have proposed a new encryption technique, which provides good security to the MP3 audio data.This encryption technique for the audio is applied at the time of compression. Advanced Encryption Standard (AES) encryption is applied On the quantized audio data which is performed before the Huffman‟s entropy coding the encryption technique is applied to the whole audio data, so it is very difficult for the unauthorized user to access the audio data. The AES encryption technique enhances the cryptographic security of the MP3 audio content.

Z. Su, G. Zhang and J. JianG in [10] have surveyed Chaos-Based multimedia encryption techniques. One of the techniques is Encryption considering regions-of-interest. This approach is proposed by Tzouveli et al. In this approach a human video object encryption system (henceforth called HVOE) based on logistic map is proposed. In HVOE, face regions are first efficiently detected, and afterwards body regions are extracted using geometric information of the location of face regions. Then, the pixels of extracted human video objects are encrypted based on logistic map. It can resist brute-force attack, different-key attack and differential attack, and it is efficient in computational resources and running time. But, these chaos-based multimedia encryption methods are not yet mature and more efforts are needed for its further development toward practical applications with high security, low computational complexity, invariance of compression ratio, format compliance, real-time, multiple levels of security, and strong transmission error tolerance. Chaos-based multimedia encryption techniques can be used as the foundation of future research.

H. gang Wang, M. Hempel, D. Peng et.al in [14] has proposed an index-based selective audio encryption scheme for WMSNs in order to ensure security, audio quality and energy efficiency. The scheme protects data transmissions by incorporating both resource allocation and selective encryption based on modified discrete cosine transform (MDCT). In this scheme, the audio data importance is leveraged using the MDCT audio index, and wireless audio data transmission proceeds with energy efficient selective encryption. The proposed approach offers a significant gain in terms of energy efficiency, encryption performance and audio transmission quality.

R.Gnanajeyaraman K.Prasadh, Dr.Ramar have proposed a novel higher dimensional chaotic system for audio encryption in [7].In this system variables are treated as encryption keys in order to achieve secure transmission of audio signals. Since the highly sensitive to the initial condition of a system and to the variation of a parameter, and chaotic trajectory is so unpredictable. This gives much higher security. The higher dimensional of the algorithm is used to enhance the key space and security of the algorithm. The security analysis is done. The experiments show that the algorithm has the characteristic of sensitive to initial condition, high key space; digital audio signal distribution uniformity and the algorithm will not break in chosen/known-plaintext attacks.

S. R. Rupanagudi ,V.G. Bhat et.al proposed that that by utilizing a combination of the AES method of encryption/decryption along with visual cryptography, they can ensure the highest form of security. In comparison with individually deploying the AES or visual cryptography methods, the novel methodology presented in this paper could be used in several applications specially related to defence, safeguarding national security and the likes.

Dr. R. Prema proposed that the protocol has been implemented using Network Simulator (NS2). The performance metrics was based on power consumption, packet delivery ratio.The AES Based Secure Transmission in Wireless Sensor Networks attains the application specified communication delays at low energy cost by dynamically adapting transmission power and routing decisions along with incorporating a novel cryptosystem for security.

M. Mohurle and V. V. Panchbhai , a hardware implementation of the AES-256 encryption and decryption algorithm was proposed. The AES cryptography algorithm can be used to encryption and decryption blocks of 128 bits and is capable of using cipher keys of 256 bits. Feature of the proposed pipeline design was depending on the round keys, which are consumed different round of encryption, are generated in parallel way with the encryption process. This lowers delay of the each round of encryption and reduces the encryption delay of a plaintext block. Xilinx ISE.14.7 (64-bit) is used for simulation by using VHDL and hardware implementation on FPGA (Xilinx Spartan 6 or A1tera Cyclone 2 FPGA device)

6.0 Conclusion

In this paper, it has been surveyed about the existing works on the encryption techniques. Those encryption techniques are studied and analyzed well to promote the performance of the encryption methods also to ensure the security proceedings. The selected algorithms are AES, 3DES, Blowfish and DES. 3DES has least efficient of all the studied algorithms. In future we can use Encryption techniques in such a way that it can consume less time and power furthermore; we try to develop stronger Encryption Algorithm with high speed. Advanced Encryption Standard (AES) is the most widely used encryption process in industry as well as for personal use. However, the time taken for encryption and decryption is directly proportional to the size of data. In the proposed methodology, we will design an authentication scheme which is embedded right next to AES in the same workflow.

7.0 References

[1]. Gunjan Gupta,„„Review on Encryption Ciphers of Cryptography in Network Security" International Journal of Advanced Research in Computer Science and Software Engineering, Vol.2, Issue7.Julyl2012 [2]. Yashpal Mote, Paritosh Nehete, Shekhar Gaikwad"Superior Security Data Encryption Algorithm (NTRU)"International Journal of Engineering Sciences, Vol.6, July 2012

[3]. M. Anand Kumar,Dr.S.Karthikeyan"Investigating the Efficiency of Blowfish and Rejindael (AES) Algorithms" I. J. Computer Network and Information Security,vol.2,issue22,2012

[4]. G Ramesh, Dr R Umarani"A New Symmetrical Encryption Algorithm with High Security and Data Rate For WLAN andwidth Line"International Journal of Information Technology, Vol.2, Isssue4, April2012 [5]. Milind Mathur, Ayush Kesarwani "Comparison between DES, 3DES, RC2, RC6, BLOWFISH AND AES" Proceedings of National Conference on New Horizons in IT - NCNHIT 2013

[6]. Rohan Rayarikar, Sanket Upadhyay, Priyanka Pimpale"SMS Encryption Using AES Algorithm on Android "International Journal of Advanced Computer Applications, Vol.50, No.19.July2012

[7]. G. Ramesh, Dr.R Umarani "A Survey on Various Most Common Encryption Techniques" International Journal of Advanced Research in Computer Science and Software Engineering, Vol.2, No.2.March-April2012

[8]. Agus Dwi Suarjaya"A New Algorithm for Data Compression Optimisation"International Journal of Advanced Computer Science and Applications, Vol.3, No.8.2012

[9]. Hyubgun Lee, Kyounghwa Lee, Yongtae Shin"AES Implementation and Performance Evaluation on 8-bit Microcontrollers" International Journal of Computer Science and Information Security, Vol. 6 No. 1, 2009

[10]. Zhaopin Su, Guofu Zhang and Jianguo Jiang "Multimedia Security: A Survey of Chaos-Based Encryption Technology "School of Computer and Information, Hefei University of Technology China, No.5.2012

[11]. Sheetal Sharma,Lucknesh Kumar,Himanshu Sharma "Encryption of an Audio File on Lower Frequency Band for Secure Communication "International Journal of Advanced Research in Computer Science and Software Engineering,Vol.3,Issue7.Julyl2013

[12]. Bismita Gadanayak, Chittaranjan Pradhan, Utpal Chandra Dey"Comparative Study of Different Encryption Techniques on MP3 Compression "International Journal off Computer Applications (0975 – 8887) Volume 26– No.3, July 2011

[13]. Bismita Gadanayak, Chittaranjan Pradhan"Encryption on MP3 Compression"MES Journal of Technology and Management

[14]. Hong gang Wang, Michael Hempel, Dongming Peng Hamid Sharif and Hsiao-Hwa Chen"Index-Based Selective Audio Encryption for Wireless Multimedia Sensor Networks" IEEE TRANSACTIONS ON MULTIMEDIA, VOL.12, NO. 3, APRIL 2010

[15]. R.Gnanajeyaraman K.Prasadh, Dr.Ramar "Audio encryption using higher dimensional Chaotic map "International Journal of Recent Trends in Engineering, Vol. 1, No. 2, May 2009

[16]. M.Mohurle and V.V. Panchbhai "Review on realization of AES Encryption and decryption with power and area optimization" International conference on power electronics.

[17]. Dr.Prema "AES Algorithm based secure data transmission for wireless sensor networks" International Journal of applied engineering research,vol 11,No.5,2016