HIGHLY SECURE DATA ENCRYPTION TECHNIQUES: A REVIEW

[1]Bhawna Ondela, [2]Silky Pareyani

[1]M. tech. Scholar, [2]Assistant Professor
Electronic and Communication Department,
GGCT, Jabalpur

***Abstract*-- Data encryption is a advance method for secure data communication and AES, DES and Blowfish are the three major techniques available for data encryption. Security problems increased day by day as compared to earlier days. When performing some high level operation like net banking or transfer & sharing confidential business data, then these Methods (AES, DES and Blowfish) are quite popular now a days. But speed of encryption and security measure of these popular methods are becoming compromising as these methods became older. Paper shows a comparative analysis of the available Encryption methods by various methods literatures.**

***Index Terms*-- Encryption, Decryption, DES, AES, Blowfish, Performance Metrics, ABPES (advance blowfish parallel Encryption system)**

I. -INTRODUCTION

The Internet and other computer networking and communications technologies are entire altering the types in which peoples communicate and barter information. But, along with the efficiency, speed, and cost-efficient benefits of the digital revolution comes with new challenges to make secure and private communications and information extend the global communications infrastructure. These challenges can be responded to, the security ways of conventional paper-based communications or media envelopes and locked filing cabinets all these are being replaced by cryptographic security approaches. Through the use of approach called encryption, or can say cryptography, communication and data stored and transmitted by various computers can be secure against detection to a very high degree. Until now a day, there is little non-governmental need for encryption capabilities.

Latest encryption technology a mathematical process involving the use of algorithms (formulas) is generally deployed most widely to protect the diplomatic communications and confidentiality of military. However, with the advancement of the computer revolution, and recent development in the science of encryption, a new area for cryptographic items has developed. Electronic communications are now largely used in the people's communication and have become a necessary component for the world wide economy. Computers store and trade an ever-increasing amount of hugely personal information, including medical and financial data. In this electronic context, the need for privacy-enhancing technologies is obvious.

Modern encryption, as we have just discussed, is achieved with algorithms that use keys to encrypt and decrypt messages by turning text or other data into digital code and then by restoring it to its original form [5]. The length of the key determines the codes security level the longer the key, the more secure the code [5]. To decipher an encrypted message without access to a key, a person would need to try every possible key [5]. Computer keys are made of bits of information, binary units of information that can have the value of 0 or 1. Therefore, an 8-bit long key has 256 (2^8) possible values. A 56-bit key creates 72 quadrillion (72,000,000,000,000,000) possible combinations [5].

Without the key to crack a 56-bit encrypted message, a person would have to resort to the so-called brute-force method to decrypt the message i.e., try out every single one of the 72 quadrillion possible combinations. If the key is 128 bits long, attempting to crack the code without the key would be 4.7 sextillion (4,700,000,000,000,000,000,000) times more difficult than cracking a 56-bit key (which itself has 72 quadrillion possible combinations)! Given the current power of computers, experts consider that a 56-bit key could be cracked by using the brute-force method in 10 million hours of computer time (14,000 computers used around the clock for 4 months) [5].

However, a 128-bit key is not considered crack able. Until 1996, the U.S. government considered anything stronger than a 40-bit encryption to be a munitions hence, the export of any piece of information with that level of encryption was illegal [5]. Since then, the government has relaxed its standards and allows the export of 56-bit encryption, with some restrictions.128-bit encryption has now emerged as the standard of illegality [5]. Teble 1 below shows all available Encryption standard methods.

Table 1 Available Standard Encryption methods [5]

Algorithm name	Submitter
CAST-256	Entrust Technologies Inc.
CRYPTON-	Future systems Inc.
DEAL- (Data *Encryption Algorithm* with Larger blocks	Richard outer bridge lars Knudsen
DFC- Decorrelated Fast Cipher	Centre national pour la researcher scientifique Encole normale superienre
E2 – Encryption2	Nippon Telegraph aand Telephone Corporation
FROG-	TecApro International SA
HPC- Hasty Pudding Cipher	Rich schroeppel
MAGENTA- Multifunctional Algorithm to General-purpose Encryption & Network Telecommunication Applications	Deutsche telecom AG
MARS	IBM
RC-6 (Rivest cipher 6) also known as Rijndael	RSA laboratories
SAFER- Secure & Fast Encryption Routine	Cylink Corporation
Twofish	Doug whiting, david wager, chris hall
DES- Data Encryption Standard	National Institute to Standards & Technology (NIST)
IDEA-International Data Encryption Algorithm	James Massey to ETH Zurich & Xuejia Lai
AES Advanced Encryption Standard	Joan Daemen & Vincent Rijmen

II--RESEARCH WORK

A. Achuthshankar et al [1] [2] In this papers, six text files to various sizes are used to conduct experiments, where a comparison to three algorithms AES, DES & Blowfish are performed based on input size to text files & experimental result. [1] takes DES ,AES and BLOWFISH algorithm for implementation. DES (Data Encryption Standard) is a block cipher algorithm. It encrypts and decrypts the data of block size 64 bit with the help of 56 bit key.

AES (Advanced Encryption Standard) is a non –Feistel cipher algorithm. That encrypts and decrypts a data of 128,196 or 256 bits with key of 128,196 or 256 bits respectively and it uses rounds 10, 12 or 14 respectively. There are 3 function is performed that is Encryption, Decryption and Key generation.

BLOWFISH is keyed symmetric block cipher algorithm. It has a 64 bit block size and variable key length from 32 up to 448 bits. The algorithm keeps two sub key arrays that is 18 – entry P-array and four 256 – entry S-boxes.

Working of algorithm Comparison of this algorithm of various data input files is defined there. It is concluded that Blowfish algorithm consumes less execution time, memory usage & produces much throughput. B1owfish performs approximately 4 times faster than AES & 2 times faster than DES. Blowfish consumes less memory compared with AES & DES. AES showed poor performance results compared to other algorithms, since it necessary much processing power. Blowfish is not only fastest however also provides great security through strong key size which enables it to be used in many applications like Bulk Encryption, Random Bit Generation, Internet based Security, Packet Encryption & so many applications. DES is most widely used encryption scene, especially in financial application. AES is ideal to encrypting messages sent between objects via chat-channels & is useful to objects that are part to a game, blowfish may be faster however AES is very highly secure than blowfish and very popular because in area to Encryption Security is everything. Total avalanche to AES observe is 52 & 558.2886 kbps.

Natasha Saini et al [3] This paper describes various types to security which includes confidentiality, integrity & availability to data. There exist various threats to security issues traffic analysis, snooping, spoofing, denial to service attack etc. Brief description to propose framework is defined which uses random combination to public and private keys. They proposed cryptographic techniques are used to security enhancement. like Confidentiality, Integrity, Authentication etc. So the best outcome comes from Private-private key technique..

Uli Kretzschmar et al [4] This paper publish a document for Texas instrument for advance encryption standard they discuss the AES encryption and decryption for microcontroller MSP430. They develop a compact version of AES.

AES is the successor of Data Encryption Standard (DES), which cannot be considered as safe any longer, because of its short key with a length of only 56 bits. The AES algorithm consists of ten rounds of encryption. First the 128-bit key is extended into eleven so-called round keys, each of them 128 bits in size. Each round includes a transformation using the corresponding cipher key to ensure the security of the encryption.

Table 2 Literature Work Comparison

Research work	Work Proposed & Outcomes
Achuthshankar & bala Reddy [1]	They propose a new Encryption procedure ADA (Advance Data Encryption Algorithms) which is a combination to two methods AES & DES and they used flow to DES & AES round. They obtain a highly secure technique with high avalanche and better than available techniques like AES, DES, RC6, TDES, UR5 & CAST-256.
A. Achuthshankar [2]	They compare algorithms AES, DES & blowfish and conclude that blowfish has high throughput and AES is highest secure encryption procedure among all other methods & AES has 52 avalanche rate.
Natasha Saini [3]	They describes security issues in Encryption techniques and propose a new procedure base on Public key-Public key technique, Public key-Private key technique, Private key-Public key technique, Private key-Private key technique they obtain avalanche to their work is 51 bit / 1 bit change.
Uli Kretzschmar [4]	Developed a embedded C code for compact AES to work compatible with MSP430 microcontroller, the only problem with their work that it is platform dependent and not compatible with other microcontroller and microprocessor.

III-CONCLUSION

Paper studied some advance algorithms in these and compares their work which is available for encryption and decryption. Encryption algorithms play an important role in information security where execution time, memory usage and throughput are the major issues of concern. The selected encryption algorithms namely DES, AES and BLOWFISH are used for performance evaluation. Based on input size of text files and experimental result, it is conc1uded that Blowfish algorithm consumes less execution time, memory usage and produces more throughputs.

REFERENCES

[1] A. Achuthshankar, S. bala Reddy, A Novel Symmetric Cryptography Algorithm ADA to Fast & Secure Encryption, 9th International Conference on Intelligent Systems & Control (ISCO), 2015 IEEE

[2] A. Achuthshankar, A novel symmetric cryptography algorithm to fast & secure encryption, 9th International Conference on Intelligent Systems & Control (ISCO), 2015 IEEE

[3] Natasha Saini ,Nitin Pandey, Ajeet Pal Singh, ENHANCEMENT to SECURITY USING CRYPTOGRAPHIC TECHNIQUES, 978-1-4673-7231-2/15/2015 IEEE

[4] Uli Kretzschmar, AES128 – A C Implementation to Encryption & Decryption, Texas Instruments Application Report SLAA397A–July 2009–Revised March 2009

[5] Mansoor Ebrahim , Shujaat Khan , Umer Bin Khalid, Symmetric Algorithm Survey: A Comparative Analysis, International Journal to Computer Applications (0975 – 8887) Volume 61– No.20, January 2013

[6] Czestaw Koscielny, application to DES, IDEA & AES in strong encryption, Quasigroups & Related Systems 14 (2006), 191 – 194, Mathematics Subject Classi_cation: 68P25, 94A60, 11T71

[7] Sandipan Basu, INTERNATIONAL DATA ENCRYPTION ALGORITHM (IDEA) – A TYPICAL ILLUSTRATION, Volume 2, No. 7, July 2011 Journal to Global Research in Computer Science

[8] YI-JUNG CHEN, DYI-RONG DUH & YUNGHSIANG SAM HAN, Improved Modulo (2n + 1) Multiplier to IDEA, Short Paper , JOURNAL to INFORMATION SCIENCE & ENGINEERING 23, 907-919 (2007),

[9] Rajashekhar Modugu, Yong-Bin Kim & Minsu Choi , Design & Performance Measurement to Efficient IDEA (International Data Encryption Algorithm) Crypto-Hardware using Novel Modular Arithmetic Components,I EEE Solid-State Circuits, 2004, 29, (3), pp.303-307

[10] Ranjeet Masram, Vivek Shahare, Jibi Abraham, Rajni Moona ANALYSIS & COMPARISON to SYMMETRIC KEY CRYPTOGRAPHIC ALGORITHMS BASED ON VARIOUS FILE FEATURES, International Journal to Network Security & Its Applications (IJNSA), Vol.6, No.4, July 2014 DOI : 10.5121/ijnsa.2014.6404 43

[11] Kaijie Wu Ramesh Karri Grigori Kuznetsov Michael Goessel, Low Cost Concurrent Error Detection to Advanced Encryption Standard, ITC INTERNATIONAL TEST CONFERENCE, 0-7803-8580-2/04 Copyright 2004 IEEE

[12] Shraddha Soni, Himani Agrawal, Dr. (Mrs.) Monisha Sharma Analysis & Comparison between AES & DES Cryptographic Algorithm , ISSN: 2277-3754 ISO 9001:2008 Certified International Journal to Engineering & Innovative Technology (IJEIT) Volume 2, problem 6, December 2012 362

[13] Lalit Singh Dr. R.K. Bharti, Comparative Performance Analysis to Cryptographic Algorithms Volume 3, problem 11, November 2013 ISSN: 2277 128X International Journal to Advanced Research in Computer Science & Software Engineering