International Journal of Engineering Applied Sciences and Technology, 2021
Vol. 5, Issue 11, ISSN No. 2455-2143, Pages 284-288
Published Online March 2021 in IJEAST (http://www.ijeast.com)

A SURVEY ON DIFFERENT ENCRYPTION TECHNIQUES FOR IMAGE, VIDEO, AUDIO AND DOCS

Arjun Poduval, Nandini Rai, Parvez Khan, Atish Sane
Student, Department of EXTC
St. John College of Engineering, Palghar
Maharashtra, India

Tushar Chaudhari
Project Guide, Asst Professor
Department of EXTC
St. John College of Engineering, Palghar
Maharashtra, India

Abstract— Encryption and Decryption of different files by various cryptography methods has been studied by the R&D community for years. Cryptography methodology has advanced considerably throughout the years, and plenty of encrypting techniques are currently offered to be used as per the necessity. Also, there has recent development in these techniques to satisfy the ever increasing demand of providing higher and economical security of the info. Having such a big amount of cryptography ways makes it very exhausting to settle on one. Though selecting the correct encryption methodology as per the necessity is incredibly necessary. In this paper, we have analysed and studied different encryption methods like AES, DES, RSA, Blowfish and Twofish for different types of files like Docs, PDFs, Images, Audio, and Video. The end result is concluded based on the different performance parameters and a brief and clear conclusion is made for each method.

Keywords— **AES, DES, RSA, Blowfish, Encryption, Decryption**

I. INTRODUCTION

In this century, generation has grow to be component and parcel of one's life. Internet is one of the fundamental mediums thru which statistics is being shared on this twenty first century. Whereas cell telephones have made connectivity seamless for human beings. But this makes the confidentiality, integrity, and availability of statistics shared over public community a first-rate issue. Cyber-assaults are as common because the connectivity supplied for the customers. When it involves records breach withinside the Indian context, the primary issue we consider is Aadhaar. As lately as February 2019, Aadhaar information of over 6.7 Mn customers containing information including names, addresses and the numbers have been leaked on Indane's website. Whereas in recent times, touchy statistics like social protection numbers, credit score card statistics and financial institution account information at the moment are saved in cloud garage offerings like Dropbox or Google Drive. Hence, securing the records is one of the fundamental concern. Encrypting records is one of the maximum simplest and stable manner to shield the records from specific cyber-assaults. Encryptionis the technique thru which records is encoded in order that it stays hidden from or inaccessible to unauthorized customers. It enables shield non-public statistics, touchy records. When your records is encrypted, although an unauthorized man or woman or entity profits get admission to to it, they may now no longer be capable of study it. There are specific encryption strategies like DES, AES, Twofish, Blowfish, etc. to be had in recent times that may be used for securing the records. For one man or woman, a few statistics is classed as very crucial while a few are simply easy beneficial records. Thus, encrypting the statistics which appears to be an problematic and tough assignment hinders not unusualplace human beings to stable their records. But for an attacker nearly all of the records of someone is manner of creating the man or woman vulnerable. Though, is there a not unusualplace code set of rules or Application that could encrypt any form of documents required for the user? We are going to peer the latest traits and pop out with a not unusualplace code set of rules for encrypting and decrypting the documents.

.

International Journal of Engineering Applied Sciences and Technology, 2021
Vol. 5, Issue 11, ISSN No. 2455-2143, Pages 284-288
Published Online March 2021 in IJEAST (http://www.ijeast.com)

II. ALOGRITHMS USED FOR ANALYSIS

A. AES Algorithm –

Advanced Encryption Standard (AES) algorithm is one on the most common symmetric block cipher algorithm in worldwide. This algorithm has steps like ShiftRows, and others to encrypt and decrypt sensitive data and is used for hardware and software application around the globe. It is nearly impossible for hackers to get hold of data when encrypting by AES algorithm. Till date there is no evidence to crake this algorithm. AES has the ability to deal with three different key sizes such as 128, 192 and 256 bit and each of them require ciphers with 128 bit block size. To provide data security that is transferred to the network, AES is considered a fast and best algorithm. AES is an open source cryptography with symmetric keys used for encryption and decryption of files. **[1]**

B. DES algorithm –

DES algorithm uses symmetric block cipher for encrypting and decrypting files or information. Encryption converts data into gibberish language referred to as cipher text. Decrypting the cipher text offers us back the authentic information called plaintext. Converting the information from cipher to plain we use a structured form of algorithm referred to as Symmetric algorithm. DES takes an input of 64bits and the output is likewise of the same size. The procedure calls for a second input,that is a secret key with length of 64bits. Block cipher algorithm is used in which message is split into blocks of bits. Block cipher is used for encryption and decryption. These blocks of bits are positioned via substitution, transposition, and different distinctive mathematical functions. **[6]**

C. Blowfish algorithm –

Bruce Schneier, one of the worlds leading cryptologists, designed the Blowfish algorithm [2] and made it available in the public domain. Blowfish is a variable key length and 64-bit block cipher. The algorithm came in action in 1993, and has not been cracked yet. It may be optimized in hardware packages because of its compactness. It includes parts: a key-expansion component and a data- encryption component. Key expansion converts a key of at maximum 448 bits into several sub-key arrays totalling 4168 bytes. Data encryption takes place thru a 16-spherical (commonly) network. Each round includes a key-based permutation, and a key- and data-based substitution. All operations are XORs and additions on 32-bit words. The handiest extra operations are 4 listed array data lookups consistent with round. **[2]**

***D.* RSA algorithm –** The RSA algorithm is the most famous and confirmed asymmetric key cryptographic algorithm; it can opposite the password assault to present. RSA comes from the founder name, the first algorithm encryption and virtual signature. The safety is withinside the top number count math from two massive of the number. In RSA, two algorithm number used to create public and private key. It became difficult to recognize the authentic message from the sign key. It became secure from brute pressure assault too. **[8]**

III. EVALUATION PARAMETERS

1. Encryption time:
   The time taken to transform plaintext to cipher textual content is encryption time. Encryption time relies upon upon key length, plaintext block length and mode. Encryption time must be much less to make the gadget speedy and responsive. Encryption time is measured in milliseconds.

2. Decryption time:
   The time to reconvert plaintext from cipher textual content is known as decryption time. The decryption time just like encryption time must be much less to make system responsive and fast. Decryption time influences overall performance of system. Decryption time is measured in milliseconds.

3. Avalanche effect:
   In cryptography, a
   belongings referred to as avalanche impact displays cryptographic power of an algorithm. If there's a small alternate in an input the output changes significantly. We have measured Avalanche effect by the usage of hamming distance.
   Hamming distance in facts concept is degree of dissimilarity. Higher the avalanche impact, higher is the overall performance of the cryptography algorithm.

   Avalanche effect = (hamming distance ÷ file size)

4. Entropy:
   Randomness is an critical assets in cryptographic procedures due to the fact statistics need to now no longer be capable of be guessed via way of means of an attacker. Entropy is degree of randomness in the statistics. It measures uncertainty in the statistics.

IV. IMPLEMENTATION

We have used and compared DES, AES, blowfish and RSA. We used the process of Java algorithms using IntelliJ IDEA. We have used packages such as java security and java crypto. These packages provide security features such as encryption, encryption, key generation, and key management infrastructure, authentication and authorization features. However, blowfish is not provided for java security and the crypto library. We used blowfish in Java, converted it into a pot and added a blowfish pot to the crypto library without. We

International Journal of Engineering Applied Sciences and Technology, 2021
Vol. 5, Issue 11, ISSN No. 2455-2143, Pages 284-288
Published Online March 2021 in IJEAST (http://www.ijeast.com)

have used a variety of files such as image, document, audio and video as encryption. The encrypted output of each file is saved as a file, also the input for deletion. For comparison we used the same input files for all algorithms throughout the test. We applied the same program to all implementations and analysis tasks, so that the memory and processor conditions were always the same for all comparative skills. All block cipher algorithms are set in the same mode CBC default to java crypto and security. [3] Java crypto and security package contains classes and implementations platforms that use Java security builds. These categories can be broadly divided into two categories. First, classes use cryptography to perform information functions to be transferred. Second, there are stages of authenticity and control to achieve that use digital message alarms and digital signatures and can verify users and other devices. Libraries of this package, we use various cryptographic algorithms that make small changes in the functions of the beats. The how to use algorithms using java.security and java.crypto functions as follows: Generate key using the key generator section, create a cipher object with algorithm name parameters and mode, start cipher designed for encryption / encryption and enable encryption / encryption using do Final method ().

V. RESULT

A. Encryption Time:

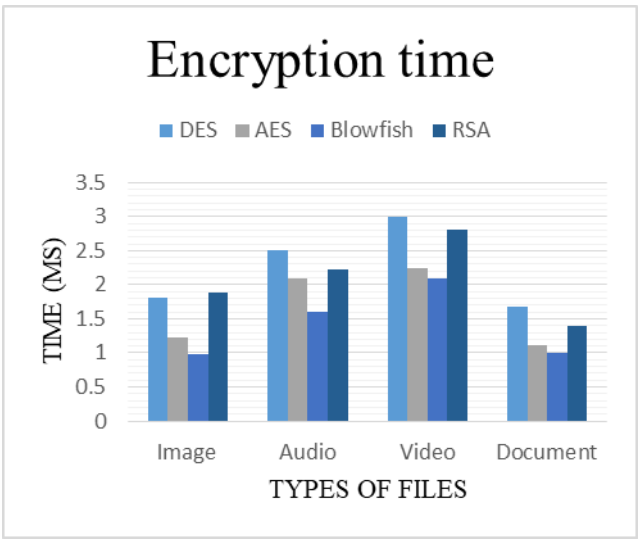

Fig 1

In the above fig. 1, we can see that Blowfish algorithm takes the least encryption time whereas DES takes highest time for encryption. Thus, Blowfish being the fastest algorithm from all the methods used here.

B. Decryption Type:

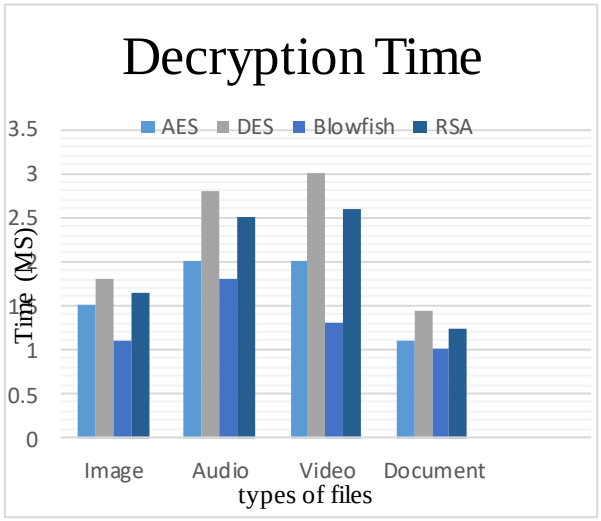

Fig 2

In the above fig. 2, we can see that Blowfish algorithm takes the least decryption time whereas DES takes highest time for decryption. Thus, Blowfish being the fastest algorithm when it comes to decrypting any type of file as per the user requirement.

C. Avalanche Effect:

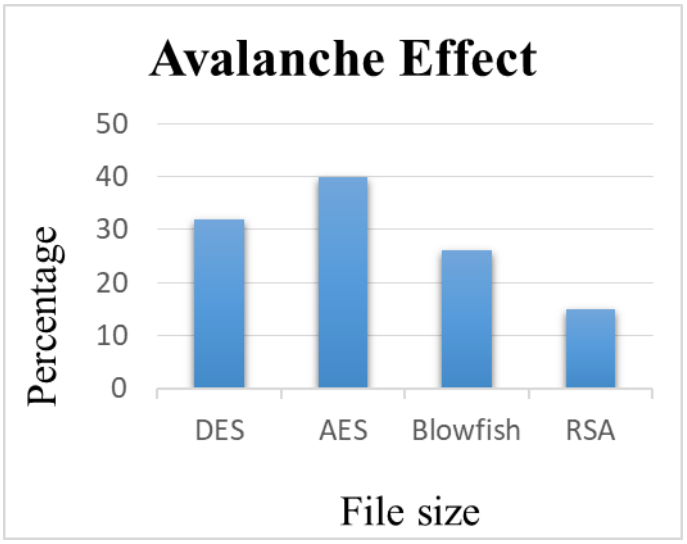

Fig 3

Figure 3 clearly shows that AES algorithm has the highest avalanche effect whereas RSA has the least and Blowfish the second least avalanche effect. If there is a small change in an input the output changes significantly. Higher the avalanche effect, better is the performance of the cryptography algorithm.

International Journal of Engineering Applied Sciences and Technology, 2021
Vol. 5, Issue 11, ISSN No. 2455-2143, Pages 284-288
Published Online March 2021 in IJEAST (http://www.ijeast.com)

D. Entropy:

Encryption method	**DES**	**AES**	**BLOWFISH**	**RSA**
Average entropy per byte	2.9477	3.8024	3.93	3.09

Table 1

Table 1 shows that Blowfish has the highest entropy with AES being second, RSA third and DES having the least entropy among all the algorithms used. Entropy is measure of randomness in the information. It measures uncertainty in the information.

VI. CONCLUSION

Each encryption method has its own strong and weak points. To use appropriate cryptography algorithm in the application, we must have knowledge about the functionality, strengths and weaknesses of high efficiency. The results show that RSA uses a lot time encryption and decryption compared to others. Blowfish spend the least amount of time. Blowfish works well on software, at least on other software platforms. After testing algorithms based on parameters Avalanche results are very high AES results; we can conclude that AES can be used in applications where it is confidential and integrity is paramount. Testing DES, AES, Blowfish and RSA according to entropy parameters, Blowfish gets high scores; which is why we can conclude that Blowfish are very strong in the fight against speculation. The results show that AES requires the highest number of bits to be encrypted and DES requires the least number of bits to be encrypted correctly, indicating that AES requires a very high transmission bandwidth. When time and memory are in a key feature in use, Blowfish is the most relevant algorithm. If cryptographic power is a major factor in operating system, AES is a very well-suited algorithm. If network bandwidth is a major factor in the application; DES is like that a very well-suited algorithm. We can explore other cryptographic methods in the same lines and process others performance metrics and use the most consistent algorithm for targeted application. A proposed indication of future work is possible performance appraisal / security analysis within great depth. For example, an algorithm with complex rounds and a large number of rounds are generally considered to be the safest. The impact of these and other factors on the full functionality of the algorithm needs to be measured.

VII. REFERENCE

1. Abdullah Muhamad -Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data
2. Tingyuan Nie, Teng Zhang -A Study of DES and Blowfish Encryption Algorithm, 978-1-4244-4547-9/09 ©2009 IEEE
3. Patila Priyadarshini, Narayankarb Prashant, D G Narayan, S M Meena - A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish, International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA.
4. Oluwakemi Christiana Abikoye, Haruna Ahmad Dokoro, Abdullahi Abubakar, Akande Noah Oluwatobi and Asani Emmanuel Oluwatobi - Modified Advanced Encryption Standard Algorithm for Information Security
5. Singh Amandeep, Agarwal Praveen, Chand Mehar - Image Encryption and Analysis using Dynamic AES
6. Saikumar Indumathi -DES- Data Encryption Standard, International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056 Volume: 04 Issue: 03 | Mar -2017
7. Abugharsa Ahmed Bashir, Basari Abd Samad Bin Hasan, Almangush Hamida -A New Image Encryption Approach using The Integration of a Shifting Technique and The AES Algorithm, International Journal of Computer Applications (0975 – 8887) Volume 42– No.9, March 2012
8. Arab Alireza, Rostami Mohammad Javad, Ghavami Behnam -An image encryption method based on chaos system and AES algorithm, The Journal of Supercomputing, 2019
9. Laia Yonata et al 2018 J. Phys.: Conf. Ser. 1007 012016 -File Cryptography with AES and RSA for Mobile Based on Android
10. Dr. Rizvi S.A.M, Dr. Hussain Syed Zeeshan, Wadhwa Neeta -Performance Analysis of AES and TwoFish Encryption Schemes, 2011 International Conference on Communication Systems and Network Technologies
11. Luhaniwal Chandani, Vyas R. K -Data Security by Encryption-Decryption using AES Algorithm of Cryptography, International Journal for Research in Applied Science & Engineering Technology (IJRASET) Volume 7 Issue VII, July 2019
12. Jawahira Ahmad, Haviluddin -An audio encryption using transposition method, International Journal of Advances in Intelligent Informatics.
13. Gadanayak Bismita, Pradhan Chittaranjan, Baranwal Neha -Secured Partial MP3 Encryption Technique, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (4), 2011.
14. M Pavana , Mrs R Nagarathna -Video Encryption and Decryption using Modified AES Algorithm, International Journal for Research in Applied Science & Engineering Technology (IJRASET) Volume 7 Issue V, May 2019.

15. Kadam Keshav S., Prof Deshmukh A. B. -Video Frame Encryption Algorithm using AES, International Journal of Engineering Research & Technology (IJERT) Vol. 5 Issue 06, June-2016.
16. Iyer Sridhar C., Sedamkar R.R., Gupta Shiwani -A Novel Idea on Multimedia Encryption using Hybrid Crypto Approach, 7th International Conference on Communication, Computing and Virtualization 2016.
17. Fauziah Noveline Aziz, Setiadi De Rosal Ignatius Moses, Sari Christy Atika -Design and Implementation of AES and SHA-256 Cryptography for Securing Multimedia File over Android Chat Application, International Seminar on Research of Information Technology and Intelligent System, 2018.
18. Tayde Suchita, Asst. Prof Siledar Seema -File Encryption, Decryption Using AES Algorithm in Android Phone, Volume 5, Issue 5, May 2015 International Journal of Advanced Research in Computer Science and Software Engineering.