IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.114180

AN IMAGE & TEXT ENYCYPTION DECRYPTION USING AES AND DES ALGORITHM

Prof. A. B. Bagwan, Omkar More, Rutuja Patil, Shubham Surve, Vijay Patil

Professor, Computer Engineering, Siddhant College, Pune, India[1]

Student, Computer Engineering, Siddhant College, Pune, India[2,3,4,5]

Abstract: With the fast progression of digital data exchange in electronic way, information security is becoming much more important in data storage and transmission. Cryptography has come up as a solution which plays a vital role in information security system against malicious attacks. This security mechanism uses some algorithms to scramble data into unreadable text which can be only being decoded or decrypted by party those possesses the associated key. These algorithms consume a significant amount of computing resources such as CPU time, memory and computation time. In this paper two most widely used symmetric encryption techniques i.e. data encryption standard (DES) and advanced encryption standard (AES) have been implemented. After the implementation, these techniques are compared on some points. These points are avalanche effect due to one bit variation in plaintext keeping the key constant, avalanche effect due to one bit variation in key keeping the plaintext constant, memory required for implementation and simulation time required for encryption.

Keywords: Computer Communication- Networks, Distributed Systems, Social Network, Rating

I. INTRODUCTION

This web application majorly focusses on sharing data over network in encrypted format. So, data can be more secure. In this application we are using 2 algorithms to encryption/decryption so user can choose their own way to secure their data. And we can see the time different chart for this algorithm. Website is allowed user to register and share plain data or encrypted data over site with your friends and family.

II. AES

AES is an iterative rather than Feistel cipher. It is based on ‘substitution–permutation network’. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations). Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix. Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

ENCRYPTION PROCESS

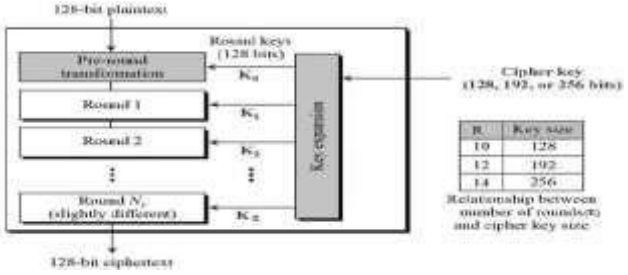

Figure 1: Encryption Process

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.114180

1. BYTE SUBSTITUTION (SUB BYTE)

The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.

2. SHIFTROWS

Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows:

- First row is not shifted.
- Second row is shifted one (byte) position to the left.
- Third row is shifted two positions to the left.
- Fourth row is shifted three positions to the left. • The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

3. MIXCOULUMNS

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

4. ADDROUNDKEY

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

DECRYPTION PROCESS

The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order – • Add round key

- Mix columns
- Shift rows
- Byte substitution

Since sub-processes in each round are in reverse manner, unlike for a Feistel Cipher, the encryption and decryption algorithms need to be separately implemented, although they are very closely related.

III. DES

The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).

DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only). General Structure of DES is depicted in the following illustration

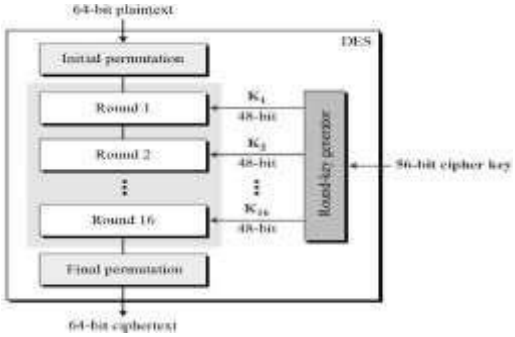

Figure 2: DES Process

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.114180

IV. SYSTEM ARCHITECTURE

Here we are going to discuss the working of the system. We are going to develop the application for the public users. Users can register to the application through mobile number, Email. They can login to the account using registered details. In this application they can share text and image data over the network with encrypted or plaint format.

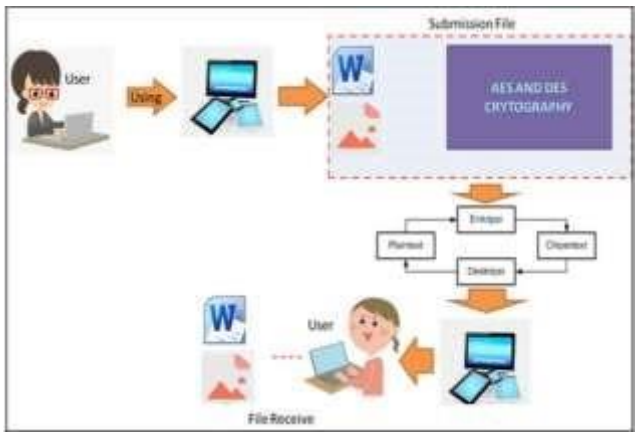

Figure 3: System Architecture

V. GENERAL DESCRIPTION

This web Application allows Users the following functionality

1. . Register User: - User can register using email id and password.
2. Login: - User can login to the system using same credential that he/she used while registering himself.
3. After successful login
4. User can modify profile, share files without encryption and with encryption (AES/DES)

VII. CONCLUSION

Encryption algorithm plays an important role in communication security where simulation time, memory usages and level of encryption the major issue of concern. Two most commonly used encryption algorithms DES and AES are used for performance evaluation DES is the most widely used encryption scheme, especially in financial applications. In DES memory required for implementation 43.3 KB is the high. In AES the avalanche effect is very high. AES is ideal for encrypting messages sent between objects via chat-channels, and is useful for objects that are part of a game, or anything involving monetary transactions. Our future work will include experiments on image and focus will be to improve security level.

VIII. ACKNOWLEDGEMENT

It gives us a great pleasure and immense satisfaction to present this special topic project report on An Image and Text Encryption and Decryption using AES and DES Algorithm which is the result of unwavering support, expert guidance and focused direction of our guide Prof. Sushma Ghose to whom we express our deep sense of gratitude and humble thanks for her valuable guidance throughout the project building work. The success of this project has throughout depended upon an exact blend of hard work and unending co-operation and guidance, extended to us by the superiors at the college.

Furthermore, we are indebted to the Head of Computer Department Prof. Kamal Reddy and Principal Prof. U.V. Shinde whose constant encouragement and motivation inspired us to do our best.

Last but not the least, we sincerely thanks to our classmates, the staff and all others who directly or indirectly helped us and made numerous suggestions which have surely improved the quality of the work.

DOI: 10.17148/IJARCCE.2022.114180

VI. REFERENCES

* Rismayani -, "INFORMATION SYSTEM FILE DELIVERY USING BLOWFISH ALGORITHM AND CRYPTOGRAPHY AES ANDROID-BASED (CASE STUDY : LPPPTK KPTK DISTRICT GOWA)," Masy. Telematika Dan Inf. J. Penelit. Teknol. Inf. Dan Komun., vol. 10, no. 1, Art. no. 1, Sep. 2019, doi: 10.17933/mti.v10i1.140.
* J. Daemen and V. Rijmen, The Design of Rijndael: AES - The Advanced Encryption Standard. Springer Science & Business Media, 2013.
* H. Mukhtar, Kriptografi untuk Keamanan Data. Republish, 2018.
* A. Kahate, Cryptography and Network Security. Tata McGraw-Hill Education, 2013. * V. Gruhn and R. Striemer, The Essence of Software Engineering. Springer, 2018.
* M. Hočevar et al., WP 3 Development of Mobile-based Measurement System, D9 Mobile Unit Design: CTProfiler - Performance Evaluation of Cooling Towers. University of Ljubljana, Faculty of mechanical engineering, 2018.
* Rismayani and A. Irmayana, "The implementation of e-learning into mobile-based interactive data structure subject," in 2017 5th International Conference on Cyber and IT Service Management (CITSM), Aug. 2017, pp. 1–5, doi: 10.1109/CITSM.2017.8089234.
* M. a. T. Abubakar, A. Aloysius, Z. Umar, and M. Dauda, "Comparative Analysis of Some Efficient Data Security Methods among Cryptographic Techniques for Cloud Data Security," Niger. J. Basic Appl. Sci., vol. 27, no. 1, Art. no. 1, 2019. * N. A. Al-gohany and S. Almotairi, "Comparative Study of Database Security In Cloud Computing Using AES and DES Encryption Algorithms," J. Inf. Secur. Cybercrimes Res., vol. 2, no. 1, Art. no. 1, Jul. 2019, doi: 10.26735/16587790.2019.004.
* N. B. Anwar, M. Hasan, M. Hasan, J. Z. Loren, and S. M. T. Hossain, "Comparative Study of Cryptography Algorithms and Its' Applications," p. 8, 2019.
* V. B. Banumathi Dr. A., "EFFICIENT ANALYSIS OF ENCRYPTION ALGORITHMS RSA DES AND AES FOR SENSITIVE DATA | Purakala with ISSN 0971-2143 is an UGC CARE Journal," UGC CARE J., vol. 31, no. 4, Apr. 2020, Accessed: Jun. 23, 2020. [Online]. Available: https://www.purakala.com/index.php/0971-2143/article/view/238. * R. Bhangale, "Securing Image Metadata using Advanced Encryption Standard," masters, Dublin, National College of Ireland, 2020.