RESEARCH ARTICLE OPEN ACCESS

Cyber Security Algorithms

Suchita Jangir, Radhika Sharma

Computer Science Engineering, Arya Institute of Engineering and Technology, Jaipur (Rajasthan)
Computer Science Engineering, Arya Institute of Engineering and Technology, Jaipur (Rajasthan)

ABSTRACT

Cyber Security is a subject in computer science branch. Securing the information has become the major problem in current days because of loss of data. The perpetration of algorithms in encountering the wide range of cyber security problems surveyed, like,triple DES, advanced encryption standard (AES) and RSA. These are used to identify the advantages of employing in enhancing cyber security techniques.

Keywords — RSA,DES,AES

I. INTRODUCTION

The purpose of this paper is understanding cyber security and its algorithms: Triple DES Advanced encryption standard (AES) and RSA. Its goal is to reduce the threat of cyber-attacks. The cyber attacks adding day by day due to significant growth in the usage of digital technologies, like, internet, mobile, smart devices, sensors and many more. Now a days an individual can send and receive many information may be video, any email or anything only by Clicking a button but did she/he ever think about how safe this information transmitted to another with no loss of data? To protecting this critical informationcybersecurity,algorithms or styles are used.

Types of cyber security algorithms

a) TRIPLE DATA ENCRYPTION ALGORITHM

b) PUBLIC KEY CRYPTOGRAPHY

c) AES ALGORITHM

II. TRIPLE DATA ENCRYPTION ALGORITHM

It is a type of cryptography algorithm whichinternally use of 3des blocks so there are 3 keys used in these algorithms and each key size 56 bits length so the total size of keys 56*3bits length.

WORKING

Encrypt the blocks using only DES with keys k1Now decipher the output of step 1 using only 1 DES with keys k2eventually,cipher the output of step 3 is the cipher text. Converting cyphertext to plaintext known as decryption. User first decrypt using k3,then encrypt with k2, and eventually decipher with k1.

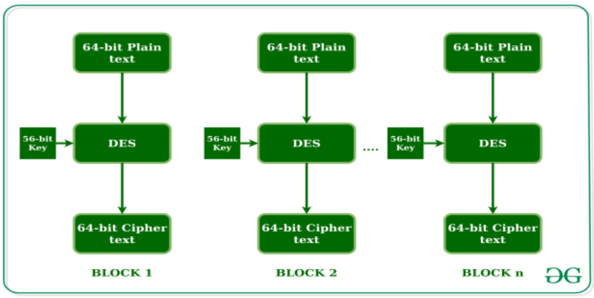

figure 1. des algorithm working

III. RSA ENCRYPTION

RSA cryptography algorithm it means that it works two keys public key and private key public key given to everyone and private keys as use as private. senders send public key to server with requests for data. Server encrypts data with the help of sender's public keys and send the encrypt data receiver receives the data and decrypts the information.

WORKING

The process of rsa is depend on the fact that rsa is hard to simplify a big integer the public key have two numbers first number is multiplication of two big prime numbers. and private key is also simplief from the same two prime numbers.therefore, if somebody can simplief the big number,the private key is adjustable so the encryption length between the key size and if we twice or thrice the key size.the strength of encryption increases exponential .it can type in 1024 or 2048 bits.

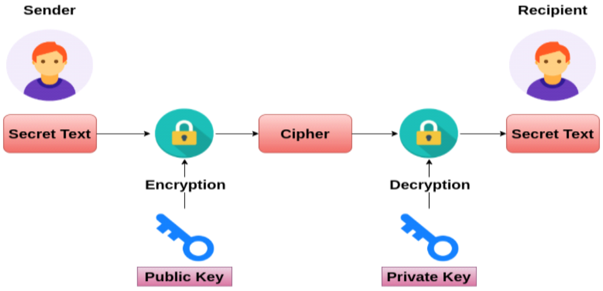

FIGURE2 :RSA ALGORITHM WORKING

IV. AES

AES stands for advanced encryption standards and is highly used symmetric encryption algorithms. it is only used for encryption and security of electronic data. Advanced encryption standard used instead of data encryption standards.it is very efficient and fast compare to data encrypted standard.

Working

Rijndael algorithm is more iterative than Feistel cipher. Grounded on 'permutation network replacement'. It contains a series of interactive functions, some of which involve fitting inputs with certain outputs (inputs) and others include shoving pieces (permissions). Interestingly, AES makes all of its computations in bytes rather than bits. Therefore, AES handles 128 bits of navigation block as 16 bytes. These 16 bytes are arranged in 4 columns and rows of processing as a matrix different from DES, the number of cycles in AES varies and depends on key length. AES uses 10 rounds of 128bit keys, 12 rounds of 192bit keys and 14 rounds of 256bit keys. Each ofthese cycles uses a 128 bits rotating key, calculated from the first AES key.

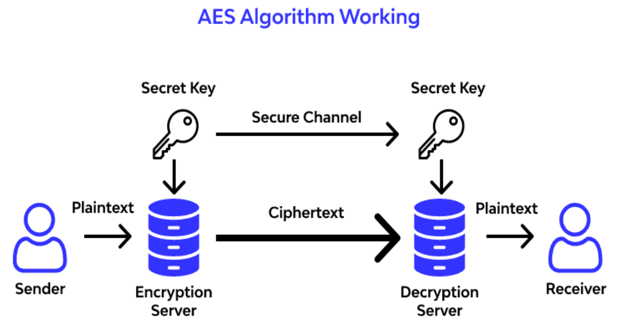

FIGURE 3: AES ALGORITHM WORKING

V. CONCLUSIONS

Rijndael algorithm Computation time fasterthan compare to DES and Public key cryptography. Memory utilization AES requires moderate memory space and DES requires least memory space and public key cryptography requires more memory spacesecurity level AES has excellent security and DES has adequate public key cryptography has least secure .so that the finally conclusion that AES is better than DES and Public key cryptography.

REFERENCES

[1]. Cyber Security: Understanding cyber-crimes

[2]. A Look back on cyber security 2012 byLuis corrons.

[3]. Computer Security Practices in Non-Profit Organization-A net action report by Audric Krause.

[4]. P. Sen, R. Jain, V. Bhatnagar and S. Illiyas, "Big data and ML: Interaction & Challenges," IEEE 2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2022, pp. 939-943, 2022.

[5]. S. Mishra, M. Kumar, N. Singh and S. Dwivedi, "A Survey on AWS Cloud Computing Security Challenges & Solutions," 2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, pp. 614-617, 2022.

[6]. H. Arora, M. Kumar, T. Rasool and P. Panchal, "Facial and Emotional Identification using Artificial Intelligence," IEEE 2022 6th International Conference on Trends in Electronics and Informatics (ICOEI), pp. 1025-1030, 2022.

[7]. Dr. Himanshu Arora, Gaurav Kumar soni, Deepti Arora, "Analysis and performance overview of RSA algorithm", International Journal of Emerging Technology and Advanced Engineering, vol. 8, issue. 4, pp. 10-12, 2018.

[8]. Rahul Misra and Ramkrishan Sahay, "A Review on Student Performance Predication Using Data Mining Approach", International Journal of Recent Research and Review, vol. X, no. 4, pp. 45-47, December 2017.

[9]. H. Arora, G. K. Soni, R. K. Kushwaha and P. Prasoon, "Digital Image Security Based on the Hybrid Model of Image Hiding and Encryption," IEEE 2021 6th International Conference on Communication and Electronics Systems (ICCES), Coimbatre, India, pp. 1153-1157, 2021.

[10]. A. Dhoka, S. Pachauri, C. Nigam and S. Chouhan, "Machine Learning and Speech Analysis Framework for Protecting Children against Harmful Online Content," 2023 Second International Conference on Electronics and Renewable Systems (ICEARS), pp. 1420-1424, 2023.

[11]. S. Mishra, D. Singh, D. Pant and A. Rawat, "Secure Data Communication Using Information Hiding and Encryption Algorithms," IEEE Second International Conference on Artificial Intelligence and Smart Energy (ICAIS), Coimbatore, India, pp. 1448-1452, 2022.

[12]. H. Arora, T. Manglani, G. Bakshi and S. Choudhary, "Cyber Security Challenges and Trends on Recent Technologies," IEEE 6th International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, pp. 115-118, 2022.