iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VII **Month of publication:** July 2022

DOI: https://doi.org/10.22214/ijraset.2022.45926

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VII July 2022- Available at www.ijraset.com

Use of Cryptography and Signing for Network Security

Aditya B S[1], Sharadadevi Kaganurmath[2]
[1]*Information Science and EngineeringRV College of Engineering Bengaluru, India*
[2]Assistant Professor, *Information Science and EngineeringRV College of Engineering Bengaluru, India*

Abstract: With technological advancements along with tremendous generation and storage of sensitive data, which can be cryptographic keys, passwords or other data that can be crucial for operation of an organization, thereis a need to secure this sensitive data startingfrom its creation, its transfer from one place to another and its final place of storage. Thiscan be done with the help of cryptography and cryptographic algorithms that can help secure this entire process. With cryptography, it is possible to securely transfer sensitive data to ensure that it cannotbe read or tampered by a third party. Cryptography and its related algorithms can also be used to secure the network for safe transfer and storage of sensitive data. In this paper, starting with a brief introduction to cryptography concepts and some networkingprotocols, we shall discuss and compare usage of an algorithm such as AES, hashing and importance of Digital Certificates and Signing operation along with encryption for better security.

I. INTRODUCTION

Cryptography involves the study of methodsto have a safe communication channel to sendmessages between two entities without the original message being stolen or tampered with by converting the original message to another unreadable format. This process that converts the original message into an unreadable format is called encryption and the process of obtaining the original messagefrom the unreadable format is called decryption.

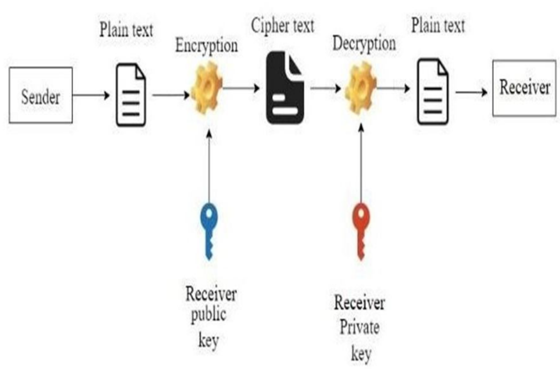


Fig 1: Process of Encryption incryptography

Cryptographic keys are numbers, characters or alphanumeric characters that are used for encryption and decryption. Keys come with various sizes and differently sized keys can be used depending on the use case and strength of encryption needed. Some examples include AES 128 bit, AES 256 bit, RSA 2048 bit, ECC 256 bit etc. Cryptographic algorithms are subdivided intothree categories. These are Symmetric encryption, Asymmetric encryption, and Hash functions. Symmetric key system uses the same key for encryption and decryption whereas Asymmetric key system also known as public-key encryption, uses two separate keys for encryption and decryption, which are public and private keys respectively.

Longer the key size, more secure is the encrypted data and harder for the data to be tampered with or decrypted by an unknown third party. AES 256 bit, for example, ismuch more secure and robust than AES 128 bit. There are special circumstances that make certain key types better than the other even though the key size of the former is bigger than the latter. One such goodexample is RSA 3072-bit vs ECC 256-bit. Although the RSA key here has a bigger keysize, ECC with a smaller key size is more robust, faster, and more secure. This is due tothe mathematical foundation of how keys arederived for ECC (Elliptic CurveCryptography) using elliptic curves drawn ona graph that helps generate random values. As the key size is smaller for ECC in this comparison, it is more efficient and faster forencryption and decryption, which makes it useful in cases where quick results are needed.

II. AES AND ITS USAGE

A. *Comparison of AES with OtherAlgorithms*

Due to the small key size in DES and 3DES (Triple DES), it was soon breakable and insecure. AES was used as an alternative in place of DES and 3DES that offers better security and larger key sizes. AES comes with key sizes 128-bit, 192-bit and 256-bit with 10, 12, 14 rounds performed during the encryption process respectively with the AES256-bit version being the most secure. AES being a symmetric key encryption algorithm provides stronger encryption thanasymmetric encryptions when per bit key
ength is taken into consideration. One majordisadvantage of AES over asymmetric encryption algorithms like RSA or ECC which uses a pair of public and private keys,is that if the key is known, it can be decryptedas the same key is used for encryption and decryption.

B. *Comparison of AES in Different Modes*

Based on the usage, AES algorithm can be implemented in different modes. In cases where plain text patterns must be well hiddenor made random, CBC (Cipher Block Chaining) mode of the AES can be used. In this mode, the entire plain text is broken intoblocks which are encrypted sequentially. While encrypting, an initialization vector, which chooses a unique value of fixed lengthis XORed with the first block and the outputof this operation is XORed with the nextblock. The output of the first and secondblock is then XORed with the next block andso on, until all the blocks are encrypted. Dueto the XOR operation at each step, the outputwill be such that even though they can have the same plain text as input, the encrypted text will never be the same. This way, apattern does not exist and makes decryption harder. Another mode for AES which is better than AES-CBC is the AES-GCM (Galois Counter Mode). In cases where high speed outputs areneeded with low latency and low cost, this mode is preferred. In this mode, each block can be independently encrypted, unlike CBCthat depends on a sequence and if the sequence is altered during decryption, theplain text can be lost. From a computational point of view, AES-GCM is preferred in 128-bit key length. This is faster and more secure compared to a bigger key size AES-CBC that needs a minimum 256-bit key length to be secure.

III. SECURING THE NETWORK

A. *Need for Network security andprotocols*

To safeguard sensitive data in the network, data must be safely stored and transported from one place to another in a network. This helps to prevent data theft, tampering, damage, and unauthorized access of data by third parties. There are sets of rules defined to carry out the procedure of transferring datasafely through a network during the process of communication. These are the network protocols. Some network protocols used are TCP/IP (Transmission Control Protocol/Internet Protocol), UDP (User Datagram Protocol), SMTP (Simple Mail Transfer Protocol) etc.

B. *Three-way Handshake for HTTPS*

One of the most used protocols for secure encrypted internet communications is the TLS (Transport Layer Security) protocol. This is the successor of SSL (Secure Socket Layer), which uses encryption to secure the communication. TLS is faster and more secure when compared to the SSL. TLS makes use of certificates to protect information when transferring between two ends (end user and a website) and helps authenticate a website’s identity for the end user to know that they are using legitimate websites. HTTPS is the combination of HTTP (HyperText Transfer Protocol) and theTLS.

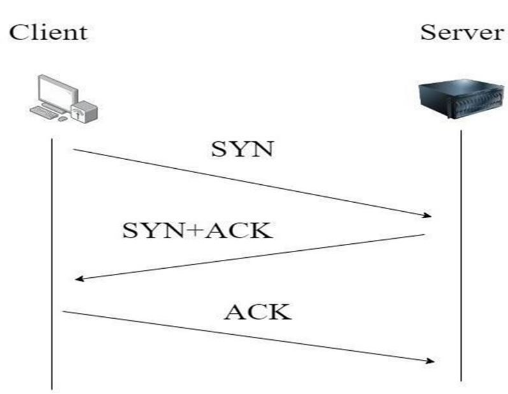


Fig 2: Three-way handshake to establishHTTPS connection

Fig 2 shown above shows the three-way handshake. The client sends a SYN packet tothe server and the server replies with an acknowledgement (ACK) and sends a SYN to the client, which then replies with an ACK.If this handshake is successful and the sent SYN packet is replied with an ACK from both ends, a secured HTTP connection isestablished along with TLS (the handshake) between two entities in a network. This ensures trusted connection between the entities on the network to have confidential communication.

C. Concept of Hashing

Hashing is a process for converting a given input string into another format of fixed length. This process is done with the help of a hash function. Unlike encryption, hashing is a one-way process where once the string ishashed, it is irreversible. The concept of hashing can be used to store data securely andlater used to validate the input data by comparing it with the hash value. It can not only help to search for data faster but also check whether the content is altered or not bya virus or an intruder. This concept can be used in networking to check if the data is tampered or not by comparing it with the stored hash values.

IV. DIGITAL CERTIFICATES AND SIGNING PROCESS.

A. Origin and use of Digital Certificates

Digital certificates are public key certificatesthat contain information to identify devices, organization, entity, servers or a website. They contain a public key which is cryptographically linked with the owner of the key. It helps bring secure and trustedconnections between devices in a network forthe devices to communicate in a confidentialmanner. This works with the help of PKI (Public Key Infrastructure), which is aframework that allows servers and users to securely communicate and exchange sensitive information. PKI consists of components like CA (Certification Authority), RA (Registration Authority) and certificates. CA is responsible for signing and distributing certificates to clients or entities under the assurance of RA. RA ensures that the client requesting for certificate is authentic and is delegated by a CA. This way,the certificate received by CA is then used as an authentication process between two entities in a network to exchange information.

B. Process of Signing with Encryption

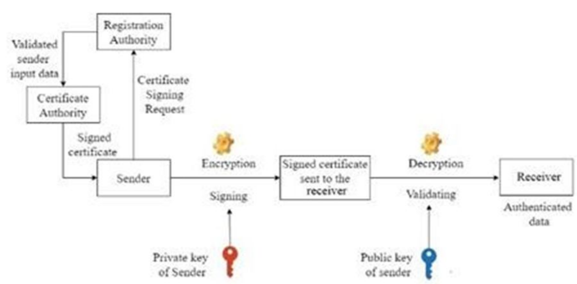


Fig 3: Process of Signing

First, an entity or a server sends a CSR (Certificate Signing Request) to a CA (Certificate Authority) for obtaining a signed certificate. There are many CAs, and the entity may choose the CA of their choice. Once the CA server receives a request, the CA will delegate an RA to process the request by validating and authenticating the data provided by the entity. Once validated, the certificate is then signed using the CAs private key (not shared to the entity or elsewhere) and the certificate containing the public key and sensitive data is shared to thereceiver (from the sender), who then uses thesender's public key to verify the package is valid or not. This can be used to validate sensitive data as well as the sender and ensuresecure transfer of sensitive data from sender to receiver on the network. The most used certificate is the X.509.

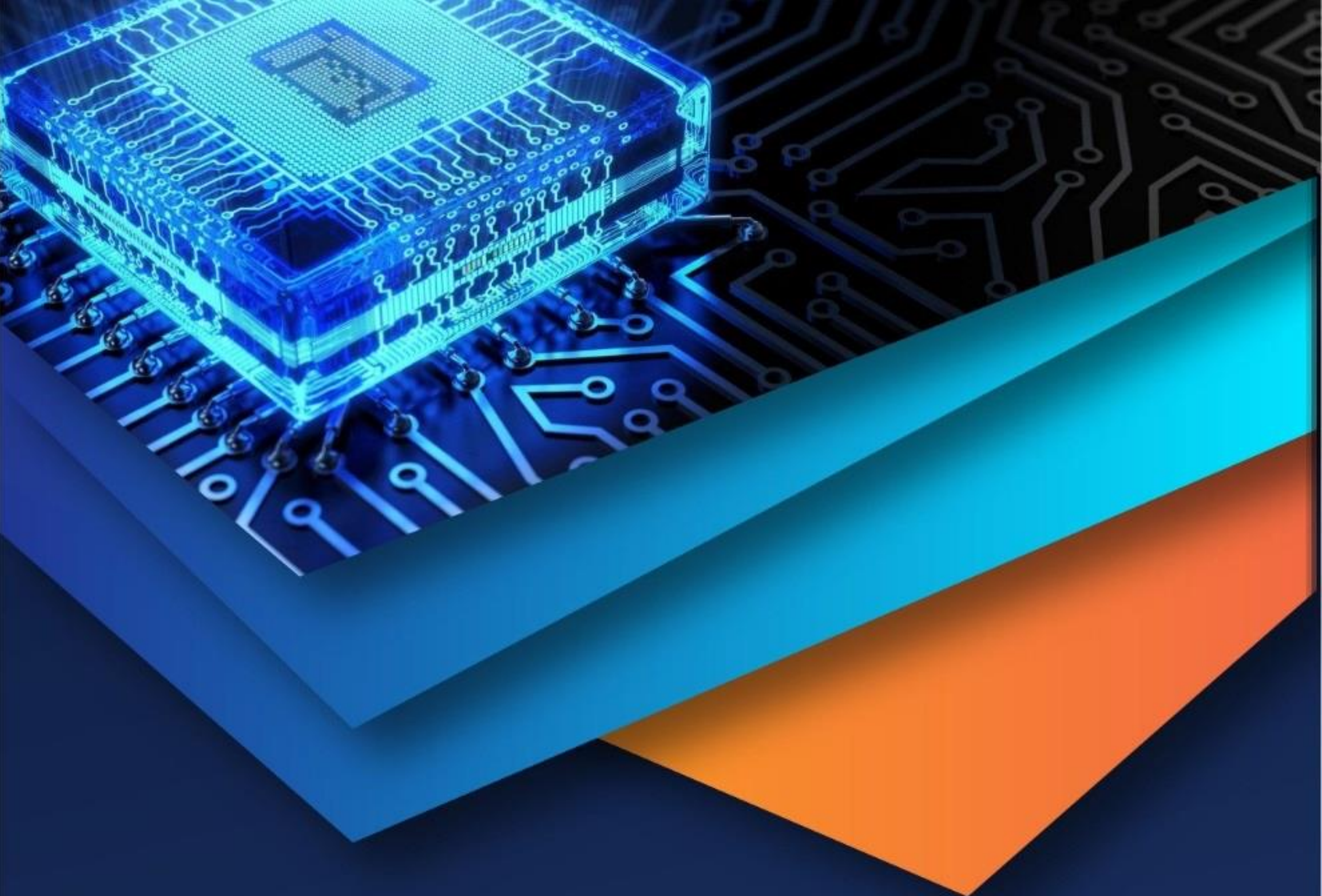
V. CONCLUSION

With large amounts of sensitive data generated day-to-day, there is a need to securely store and transport them. This ismade possible with the help of cryptographythat provides keys and algorithms for securing the data. AES is one of the most robust and secure algorithms that has not been broken down yet and is used in many instances where securing sensitive data is of utmost importance. Network protocols like TCP/IP, UDP and HTTPS are used to have astandardized and secure way of transporting data safely from the sender to the receiver over an unsecure network environment. Digital certificates and the Public Key Infrastructure framework bring about anotherstep for authenticating and validating the sender thereby making data transfer moresecure and tamper proof.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VII July 2022- Available at www.ijraset.com

REFERENCES

[1] V. Esther Jyothi, Dr. BDCN Prasad, Dr.Ramesh Kumar Mojjada, "Analysis ofCryptography Encryption for Network Security", IOP Conference Series: MaterialsScience and Engineering,DOI:10.1088/1757-899X/981/2/022028, 2020.
[2] Mariam O. Alrashidi, MaherKhemakhem, "A Framework andCryptography Algorithm for Protecting Sensitive Data on Cloud Service Providers",Computing and Information Technology Sciences 8(2):69-92, 2019.
[3] Santhosh Kumar R, Shashidhar R, "Design of High Speed AES System for Efficient Data Encryption and DecryptionSystem", The IEEE Seminar on Quantum Cryptography: Secure Communications for Business (Ref. No. 2005/11310), 2019.
[4] Hamid Nejatollahi, Nikil Dutt , Rosario Cammarota," Trends, Challenges and Needsfor Cryptography Implementations", International Conference on Hardware/Software Codesign and System Synthesis (CODES+ISSS), 2019.
[5] Ye Yuan,Yijun Yang, Liji Wu, Xiangmin Zhang, "A High Performance Encryption System Based on AES Algorithm", IEEE International Conference on ElectronDevices and Solid State Circuits (EDSSC), 2018.
[6] E. Thambiraja, G. Ramesh, Dr. R. Umarani, "A Survey on Various Most Common Encryption Techniques" International Journal of Advanced Research in Computer Science and SoftwareEngineering, VOL. 2, Issue 7 July 2018, Page226-233.
[7] F. Mallouli, A. Hellal, N. Sharief Saeed and F. Abdulraheem Alzahrani, "A Survey on Cryptography: Comparative Study between RSA vs ECC Algorithms, and RSA vs El-Gamal Algorithms," 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud), Paris, France, pp. 173-176, 2017
[8] Dr. Sandeep Tayal et al., "A Review paper on Network Security and Cryptography", Advances in Computational Sciences and Technology, Volume 10, Number 5 (2017)pp.763-770.
[9] Mohit, "Performance Evaluation of Cryptographic Algorithms", International Journal of Computer Applications, Vol. 41, No.7, 2017.
[10] Abhishek et. al "Cryptography inNetwork Security", International Journal of Engineering and Technology, Volume 07 Issue: 04 , Apr 2017.



10.22214/IJRASET

INDEX COPERNICUS

45.98

IMPACT FACTOR: 7.129

TOGETHER WE REACH THE GOAL

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY