SHODH SAMAGAM

ISSN : 2581-6918 (Online), 2582-1792 (PRINT)

A Comparative Study of Encryption Techniques

Vikas Sharma, Ruchi Sharma, Vaibhav Kumar Ingle, Computer Science Department
Agrasen Mahavidyalaya, Raipur, Chhattisgarh , INDIA

ORIGINAL ARTICLE

Authors

Vikas Sharma
Ruchi Sharma
Vaibhav kumar Ingle

shodhsamagam1@gmail.com

Received on : 15/04/2023
Revised on : -----
Accepted on : 24/04/2023
Plagiarism : 08% on 15/04/2023

ABSTRACT

Data security is very important during internet-based communication and for this encryption plays a vital role which means "Keyed writing". In Cryptography encryption decryption of data is done by using secret key to maintain confidentiality, data integrity and data authentication. This paper provides a comparative study between symmetric key and asymmetric key encryption techniques, so that one can choose right one for his/her purpose to achieve secrecy in communication.

KEY WORDS

Encryption, Symmetric, Public Key, Private Key, Asymmetric, Cryptography.

INTRODUCTION

Data encryption is a way to protect data by encoding it so that it cannot be directly accessed by unauthorized parties. Encrypted data appears scramble or unreadable. In technical terms it is the process of converting human readable data to incomprehensible text also called cipher text.

Encryption technique requires formulas and keys which are used to encode and decode messages; such formulas are called encryption algorithms.

In the modern era a huge amount of private data is shared around the internet everyday which may include confidential and non-shareable things like personal lives, emails, chat-records, passwords, financial documents etc, that we upload answer hours such confidential data elements are also sent via the same routes (network paths) as other ordinary data sent. Hackers figured out such ways to steal the data packets from these roots. To stop unauthorized access of private data and the next level security mechanism

that can be adopted is encryption. Overall it can be said that the following are the reasons behind practicing encryption:

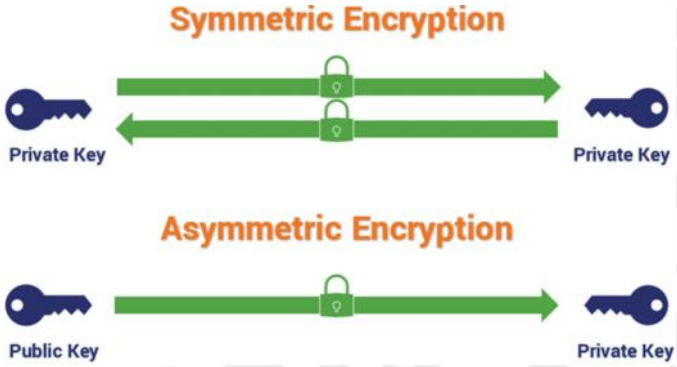
1. **Authentication:**With the help of encryption and decryption keys it can be ensured that messages sent would be received by authentic receivers.
2. **Privacy:** Encryption guarantees that no third parties can read our access to the data except the sender and receiver.
3. **Regulatory Compliance:** Many after industries and Government departments have made rules to secure personal information while sharing it on the internet through encryption.
4. **Security:** Encryption helps to enhance the security of the information whether the data is at rest or in transit.

Encryption also helps us to protect data against malicious activities and let's the parties communicate without any issues.

Types of Encryption Techniques

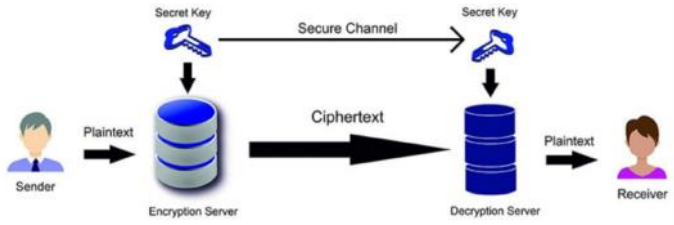
Based on the keys the encryption technique has applied, it can be categorized as:

1. Symmetric encryption/decryption
2. Asymmetric encryption/decryption



What is Symmetric Encryption?

Symmetric encryption which is also known as symmetric key cryptography uses one single key (Private Key) to encrypt as well as decrypt data. You have to share this key with the recipient, i.e. in this encryption technique, the message is encrypted with a key, and the same key is used for decrypting the message.

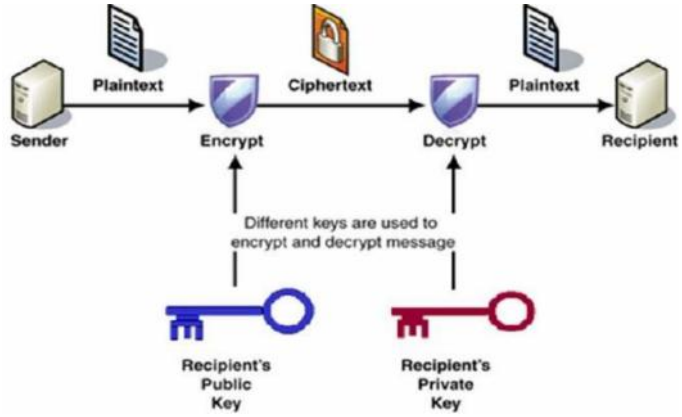


Symmetric Cryptography

What is Asymmetric Encryption?

Asymmetric method requires two different keys public key and private key. The public key and the private key are not the same thing, but they are related. You write your message, and then encrypt it with the recipient's public key. After that, if the recipient wants to decrypt your message, they would have to do it with their private key.

.



Comparative Analysis of Encryption Methods

Factors	Symmetric Encryption	Asymmetric Encryption
Key Used	Uses a single key to encrypt and decrypt data	Uses a public key to encrypt data and a private key to decrypt data
Speed	Faster encryption process	Slower encryption process
Key Length	128 or 256 bits longer	1024 bits or longer
Resources	Requires less resources comparatively	More resources required
Security	More secure comparatively	Higher risk factors involved
Cost of Implementation	Simple and Cheaper comparatively	Complex and Costlier comparatively
Data Handling	Better at handling and transferring large amounts of data	Better at handling and transferring smaller amounts of data
Example algorithms	AES, DES, IDEA and Blowfish	RSA, ECC, DSA and ElGamal
Usage	Banking: Encrypting customer sensitive data.	Digital signing: need private and public keys

CONCLUSION

"A comparative study of encryption techniques" explains symmetric key and asymmetric key encryption techniques comparatively. Analysis concludes that symmetric key algorithms can be chosen in case of high-speed, simple implementation, lower cost and security required with fewer resources like banking. On other hand asymmetric key algorithms is more efficient with public authentication mechanisms like digital signature but it requires higher cost, more recourses and complex implementation with risk factors involved.

REFERENCES

1. https://docs.oracle.com/cd
2. www.thesslstore.com/blog
3. *International Journal of Innovative Research in Science,* Engineering and Technology "A Comparative Study of Some Symmetric and Asymmetric Key Cryptography Algorithms"
4. https://www.tutorialspoint.com/cryptography/public_key_encryption.htm
5. https://www.trentonsystems.com/blog
6. https://blog.mailfence.com/symmetric-vs-asymmetric-encryption

****