Comparison of Symmetric Key And Asymmetric Key Algorithm

Dr. C. Thiyagarajan[1], M. Suresh Babu[2]
[1]Associate Professor,Dept of MCA
[2]Dept of MCA
[1, 2] PSG College of Arts and Science, Coimbatore, Tamil Nadu, India

Abstract- *Symmetric and asymmetric key cryptography, fundamental methods for data protection, are compared in this research study. We examine their guiding ideas, working methods, advantages, and disadvantages while taking efficiency and key distribution into account. Applications in the real world and security issues are covered, along with the implications of cutting- edge innovations like quantum computing. We also highlight current innovations and hybrid strategies that combine the benefits of both techniques. This study provides stakeholders with knowledge for efficient data protection and cryptographic system design in the digital era.*

Keywords- Cryptography, Encryption, Decryption, RSA, DSA, Diffie-Hellman, DES, AES.

I. INTRODUCTION

Modern digital security is built on cryptography, which makes it possible to protect sensitive data and conversations. Two main techniques in the field—symmetric key cryptography and asymmetric key cryptography—offer various strategies for reaching this objective.

We compare and contrast these two key cryptography paradigms in this research article. The effectiveness of symmetric key cryptography, which uses a single shared key for both encryption and decryption, comes at the expense of key distribution security issues. Asymmetric key cryptography, in contrast, addresses the distribution issue but adds computational complexity by using a pair of keys, public and private.

Our investigation will cover the fundamental ideas, computational procedures, and real-world applications of both approaches, highlighting their advantages and disadvantages. By doing this comparative research, we hope to arm readers with the information they need to choose the best cryptographic strategy for their unique security requirements in the ever-changing digital environment.

II. OVERVIEW OF SYMMETRIC KEY

One shared secret key is used for both data encryption and decryption in symmetric key cryptography, a crucial idea in the area of cryptography. By converting plaintext into ciphertext and vice versa, this method, also known as secret- key cryptography, ensures the secrecy and integrity of data. Symmetric key cryptography's main advantage is that it is computationally quick, which makes it perfect for quickly encrypting massive amounts of data. The difficulty of securely preserving and disseminating the shared secret key, however, continues to be of primary concern [1].

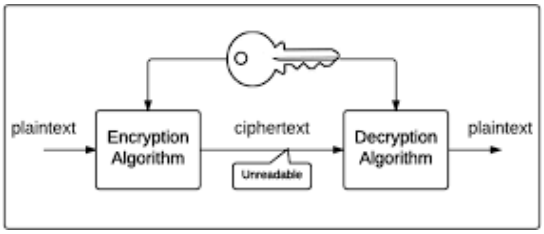

Figure 2.1 Symmetric Key Flow Diagram

A. SOME GENERAL ALGORITHM FOR SYMMETRIC KEY

For symmetric key cryptography, there are many different algorithms available. We have discussed some fundamental symmetric key methods in this section.

- AES
- DES
- Blowfish

1) ADVANCED ENCRYPTION STANDARDS(AES):

One of the most used symmetric key encryption methods is called Advanced Encryption Standard (AES). The National Institute of Standards and Technology (NIST) of the United States chose it as the encryption standard in 2001. Applications for AES include data encryption, secure communications, and disk encryption. AES provides high security and efficiency.

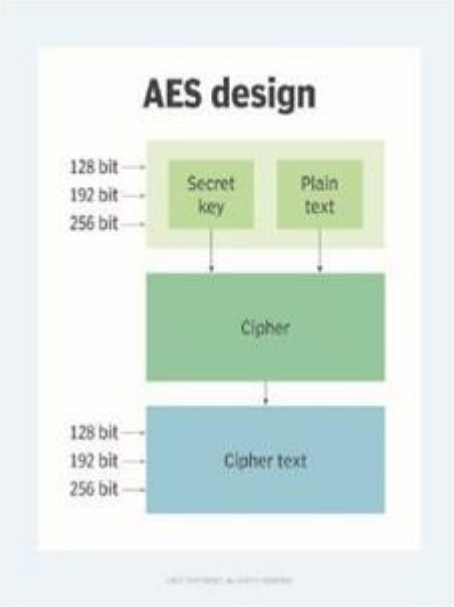

Figure 2.1.1 Diffie-Hellman Flow Diagram

2) DATA ENCRYPTION STANDARDS(DES):

An important part of the early development of cryptography was the symmetric key encryption technique known as the Data Encryption Standard (DES). It served as the basis for later cryptographic research and development after the US government accepted it as a federal standard in the 1970s [2]

.

3) BLOWFISH:

A symmetric key block cipher created for quick encryption and decoding is called Blowfish. It has been used in many applications, including secure communications and information encryption, and is renowned for being straightforward and effective [3].

III. OVERVIEW OF ASYMMETRIC KEY

A fundamental method in contemporary information security is asymmetric key cryptography, sometimes referred to as public-key cryptography. Asymmetric cryptography employs a pair of mathematically related keys, a public key and a private key, as opposed to symmetric key cryptography, which uses a single shared secret for encryption and decoding. This strategy offers special benefits for protecting key exchange mechanisms, digital signatures, and communications [4].

Figure 3.1 Asymmetric Key Flow Diagram

A. SOME GENERAL ALGORITHM FOR ASYMMETRIC KEY

For symmetric key cryptography, there are many different algorithms available. We have discussed some fundamental symmetric key methods in this section.

- RSA
- DH
- DSA

1) RIVEST-SHAMIR-ADLEMAN (RSA):

One of the best-known and most often used asymmetric encryption techniques is RSA. It is heavily used to secure digital signatures, key exchange protocols, and online communication. It is based on the mathematical features of large prime numbers [5].

2) DIFFIE-HELLMAN:

Key exchange protocol Diffie-Hellman enables two parties to concur on a shared secret key over an unreliable channel. In numerous encryption schemes, it serves as the foundation for secure key negotiation [6].

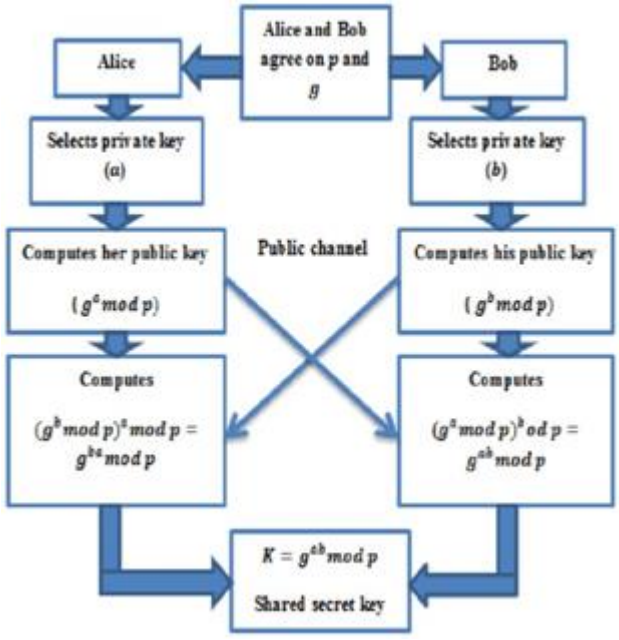

Figure 3.1.1 Diffie-Hellman Flow Diagram

3) DIGITAL SIGNATURE ALGORITHM (DSA):

The DSA algorithm is a popular one for producing digital signatures. It frequently makes use of secure email communication and document verification to guarantee the integrity and validity of messages or documents [7].

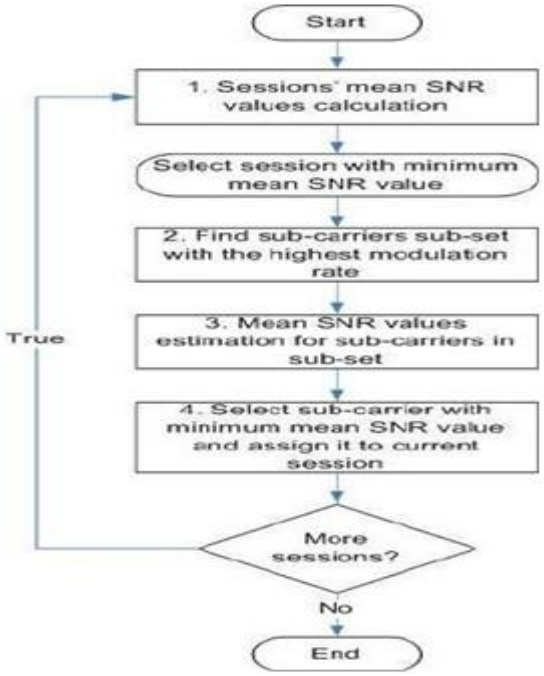

Figure 3.3.1 DSA Flow Diagram

IV. COMPARISON OF SYMMETRIC KEY AND ASYMMETRIC KEY ALGORITHMS

Algorithm	Symmetric Key			Asymmetric Key		
	BlowFish	DES	AES	RSA	DSA	Diffie-Hellman
Encryption and Decryption Key	Same [3,5,6]	Same [1,2,3,4,5,6]	Same [2,3,5,6,7]	Different [1,2,4,5,7]	Different [3,4]	Different [2,3,5]
Key Length	32 bits 'till 448 bits [3,5,6]	56 bits [1,2,3,4,5,6]	128,192 or 256 bits [2,3,5,6,7]	>1024 bits [1,2,4,5,7]	5012 'till 1024 bits [3,4]	>1024 bits [2,3,5]
Encryption Strength	High [3,5,6]	Medium [1,2,3,4,5,6]	High [2,3,5,6,7]	High [1,2,4,5,7]	High [3,4]	High [2,3,5]
Tunability	Yes [3,5,6]	No [1,2,3,4,5,6]	No [2,3,5,6,7]	Yes [1,2,4,5,7]	Yes [3,4]	Yes [2,3,5]
Operating Speed	Fast [3,5,6]	Fast [1,2,3,4,5,6]	Fast [2,3,5,6,7]	Fast [1,2,4,5,7]	Fast [3,4]	Slow [2,3,5]
Cost	Expensive [3,5,6]	Expensive [1,2,3,4,5,6]	Cheap [2,3,5,6,7]	Expensive [1,2,4,5,7]	Expensive [3,4]	Depend on key [2,3,5]
Power Consumption	Very Low [3,5,6]	Higher than AES [1,2,3,4,5,6]	Higher thanBlow Fish [2,3,5,6,7]	High [1,2,4,5,7]	High [3,4]	High [2,3,5]

V. CONCLUSION

The comparison of symmetric key and asymmetric key algorithms highlights, in the end, the significance of choosing the appropriate cryptographic strategy depending on particular use cases and security requirements. Both types of algorithms have advantages and disadvantages, so selecting one over the other requires careful consideration of a number of different factors.

Symmetric key algorithms are the best choice in situations when fast encryption and decryption are required because of their efficiency and speed. They perform best in circumstances where a shared secret key can be safely distributed among parties, like in secure device-to-device communication or inside a closed network. However, managing and distributing these secret keys in a secure manner presents a hurdle.

Asymmetric key algorithms, on the other hand, use public and private key pairs to provide a reliable solution to key distribution issues. They are especially well suited for circumstances in which secure key exchange and authentication are essential, such as in the protection of online communications and digital signatures. Although slower and more computationally intensive than their symmetric equivalents, asymmetric algorithms offer a higher level of security due to the separation of keys.

Hybrid encryption, which combines both symmetric and asymmetric cryptography, is frequently used in practise to take advantage of each type's advantages. The effectiveness of symmetric encryption for large amounts of data is combined in this method with the safety of asymmetric encryption for secure key exchange. Hybrid encryption creates a balance between performance and security by utilising the benefits of both systems.

In conclusion, the decision between symmetric and asymmetric key methods is based on the application's environment, performance needs, and individual security requirements. A well-informed choice should take into account things like key distribution, processing capacity, and the necessary level of security. To preserve the security and integrity of digital communication and data protection, researchers and practitioners must keep up with the most recent advances as cryptographic technologies continue to improve.

REFERENCES

[1] Stinson, D. R. (2005). "Cryptography: Theory and Practice." CRC Press. Schneier, B. (2015). "Applied Cryptography: Protocols, Algorithms, and Source Code in C." Wiley. Paar, C., & Pelzl, J. (2009). "Understanding Cryptography: A Textbook for Students and Practitioners." Springer.

[2] National Institute of Standards and Technology (NIST). (2001). "Announcing Approval of the Advanced Encryption

[3] Standard (AES)." Federal Information Processing Standards Publication 197 (FIPS PUB 197).

[4] Schneier, B. (1993). "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)." Fast Software Encryption, 191-204.

[5] Stallings, W. (2017). "Cryptography and Network Security: Principles and Practice." Pearson.

[6] Rivest, R. L., Shamir, A., & Adleman, L. (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems." Communications of the ACM, 21(2), 120- 126.

[7] Diffie, W., & Hellman, M. E. (1976). "New Directions in Cryptography." IEEE Transactions on Information Theory, 22(6), 644-654.

[8] National Institute of Standards and Technology (NIST). (1994). "Digital Signature Standard (DSS)." FIPS PUB 186.