ACADEMICIA: An International Multidisciplinary Research Journal
ISSN: 2249-7137 Vol. 11, Issue 11, November 2021 SJIF 2021 = 7.492
A peer reviewed journal

A REVIEW ON DIFFERENT TYPES OF CRYPTOGRAPHY TECHNIQUES

Vipin Jain*

*Teerthanker Mahaveer Institute of Management and Technology,
Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, INDIA
Email id: vipin555@rediffmail.com
DOI: 10.5958/2249-7137.2021.02568.4

ABSTRACT

Today, data communication is mostly based on digital data transmission, with data security as a top priority in order for data to reach the intended user. Cryptography is a technique of using codes to secure information and communications so that only those who are supposed to read and process it may do so. The prefix "crypt-" stands for "secret" or "vault," while the suffix "-graphy" signifies "writing." Cryptography and cryptology, as well as cryptanalysis, are closely linked sciences. Techniques such as microdots, combining words with pictures, and other methods of concealing information in storage or transit are included. However, in today's computer-centric world, cryptography is most often linked with scrambling plaintext (regular text, also known as cleartext) into ciphertext (a process known as encryption), then back again (known as decryption). Cryptographers are professionals who work in this area. As a result, various cryptography methods, such as symmetric and asymmetric algorithms, are used to provide data security. RSA (Rivest Shamir and Adleman), Diffie-Hellman, DSA (Digital Signature Algorithm), and ECC (Elliptic curve cryptography) are among the asymmetric encryption methods examined in this review article.

KEYWORDS: *Cryptography, Diffie-Hellman, DSA (Digital Signature Algorithm), ECC (Elliptic curve cryptography), RSA (Rivest Shamir and Adleman).*

1. INTRODUCTION

Every user needs a safe network while connecting so that data transmission is secure and no intruder may access their information. Cryptography is used in wireless and wired networks to provide secure data transmission, where cryptography transforms plain text to cipher text and cipher text to plain text(1). Encryption is the process of converting plain text into cipher text on the sender's side, while decryption is the process of converting cipher text back to plain text on the receiver's side. There are two types of encryption techniques: symmetric cryptography and asymmetric cryptography(2). Both parties utilize the same key in symmetric-key cryptography(3). The sender encrypts data using this key and an encryption method; the receiver decrypts the data with the same key and the matching decryption algorithm. There are two keys used in asymmetric or public-key cryptography: a private key and a public key(4). The recipient keeps the private key, while the public key is made public. Different researchers have also presented several forms of asymmetric cryptography. RSA (Rivest Shamir and Adleman), Diffie-Hellman, DSA (Digital Signature Algorithm), and ECC are some of the most widely used

asymmetric cryptographic methods (Elliptic curve cryptography). This paper will go through each of these techniques in detail(5,6)(7,8).

1.1. Rivest Shamir and Adleman (RSA) algorithm:

RSA is a public-key encryption method that is based on the factoring problem, which is thought to be difficult to solve. A user using RSA generates and then publishes their public key, which is the product of two big prime integers plus an auxiliary value. The most important elements must be kept hidden. Anyone can encrypt a message using the public key, but if the public key is big enough, only someone who knows the prime factors can decode the message using presently disclosed techniques(9)(10). Because WSN is an unsecured network that is susceptible to numerous assaults due to the broadcast nature of the transmission channel, the RSA method may be employed. Wireless sensor networks have certain security needs(11):

1. Confidentiality
2. Integrity
3. Authentication

Algorithm of RSA is shown in Figure 1:

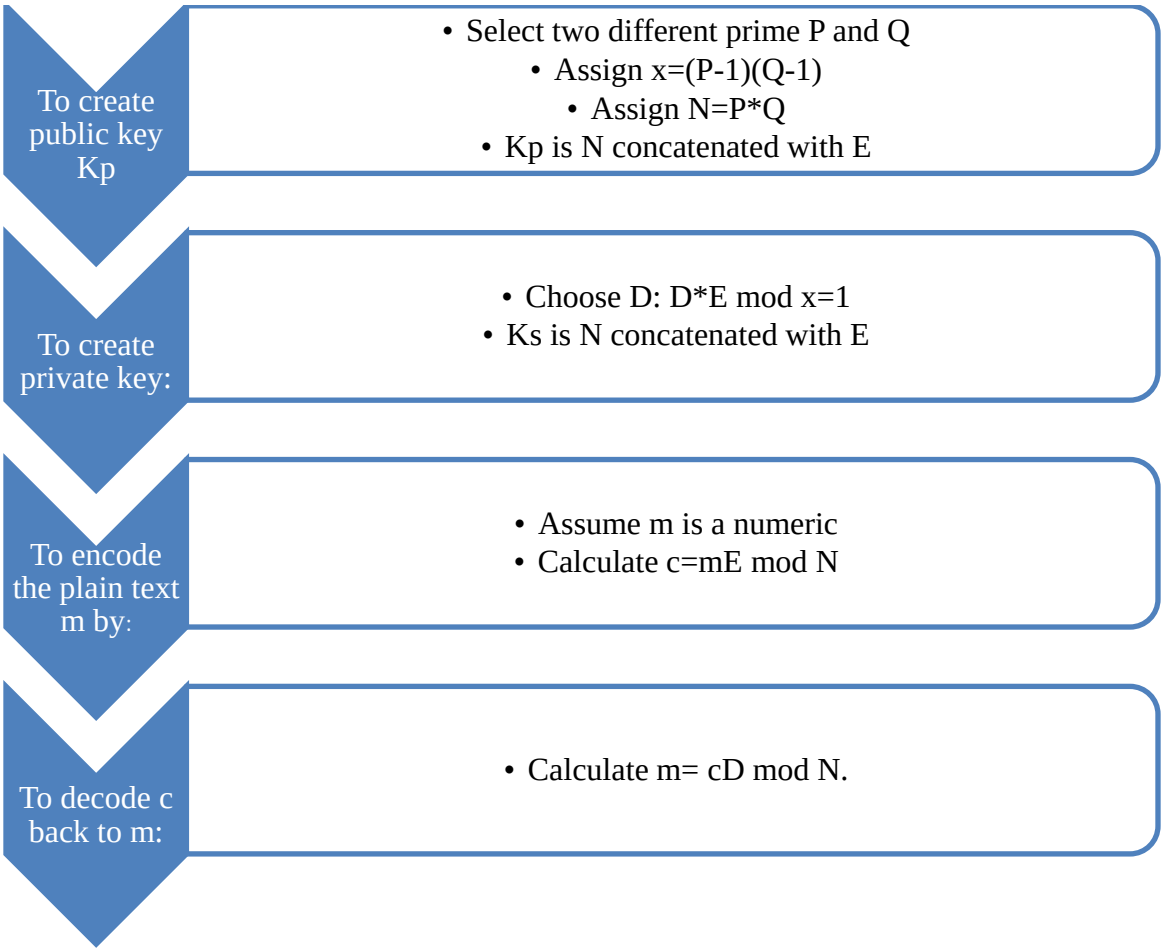

Figure 1: Illustrates the algorithm of Rivest Shamir and Adleman cryptography technique.

Because of its high time complexity and consumption requirement, RSA is not appropriate for WSN. In software, any encryption method, such as RSA, may be implemented. The speed, cost, and simplicity of customization are all drawbacks (or manipulation)(12). The benefits are in flexibility and mobility, as well as simplicity of use and upgradeability. The algorithms may be replicated and deployed on a large number of computers for a low cost(13).

1.2. Diffie-Hellman Algorithm:

This method is used when two users need to exchange cryptographic keys. Users have no knowledge of each other's keys, therefore they utilize a shared secret key via an unsecured communication channel, which is then used to encrypt future conversations using a symmetric key cipher(14,15).

In the asymmetric (public-key) situation, a new protocol is suggested for two goals: authenticated key agreement and authenticated key agreement with key confirmation(16). In this paper, they propose formal definitions of secure AK (Authenticated Key Agreement) and AKC (Authenticated Key Agreement with Key Confirmation) protocols within a formal model of distributed computing, as well as a unified model of key agreement, with several variants of this model demonstrating secure AK and AKC protocols in the random oracle model(17)(18). AK and AKC are rendered safe in this paper by first giving explicit, formal descriptions of the protocols' objectives, and then by offering practical, provably secure solutions in the random oracle model(19). In a nutshell, the process of providing security may be broken down into five steps:

a. Model specification
b. This model's objectives must be defined.
c. Assumptions statement
d. Protocol description
e. Demonstration that the protocol achieves its objectives within the mode

1.2.1. Properties of Key agreement algorithm:

a. Prior Session Key: This protocol has a previous session key saved.
b. (Perfect) Forward Secrecy: If the long-term secrets of one or more entities are exposed, the secrecy of the preceding key is unaffected.
c. Unknown Key Share: Assume there are two users, I and j. In this case, I cannot share the key with j without i's permission.
d. Key-Compromise Impersonation: If the value of I is revealed and intruders may copy it. However, the nature of I should be such that none of its other characteristics can be duplicated or modified.
f. Information Loss: The protocol's security is unaffected by the compromise of additional information that an adversary would not normally have access to.
g. Message Independence: This protocol is used by two different users.

In comparison to the presently utilized protocol, this method may be implemented with more security(20).

Another method for implementing the DiffieHellman algorithm over the internet is shown. It can be used in almost every encryption technique now in use on the Internet, including SSL, SSH, IPSec, PKI, and anything else that uses these protocols. In today's communication method, clients and servers exchange unencrypted messages via SSl (Secure Sockets Layer)(21).

The asymmetric key is utilized in the exchange procedure, and they each accept and prefer the compression choice. Client and server start the SSH (Secure Shell) procedure by negotiating parameters (e.g., preferred encryption and compression algorithms, and certain random numbers). In IPsec (Internet Protocol Security), certain preparatory data exchange is required before the data stream may be encrypted(22). Public key cryptography has two complimentary applications in PKI (Public Key Infrastructure). If one encrypts a message using another person's public key, that message can only be decrypted by that person since only that person knows his private key.

1.3. Digital Signature Algorithm (DSA):

It is used by the recipient of a communication to ensure that the message has not been tampered with during transit and that the sender's identity has been confirmed. A digital signature is an electronic counterpart of a written signature that may be used to prove to the receiver or a third party that the communication was signed by the sender in reality. For stored data and programs, digital signatures may be created so that the data and programs' integrity can be confirmed at any time. The “Hash function,” which is utilized in this technique and produces dynamic and lower sizes of bits based on each byte of data, is one way for transmitting low size and capacity data using DSA. Bitwise or and multiply functions are the most common hashing functions. If the hashed file is 4 percent the size of the original file in messages less than 1600 bytes. This method may be utilized in a variety of applications that need simple and quick procedures for creating digital signatures and have a small file size for transmitting(23,24).

Some characteristics of the hash function are listed below:

a. In the underlying public key cryptosystem, the hash function should destroy all homomorphism structures (be unable to compute hash value of 2 messages combined given their individual hash values).
b. The hash function should be applied to the whole message.
c. The hash function should be a one-way function, so that signatures do not reveal messages.
d. Given a message and its hash value, computing another message with the same hash value should be computationally infeasible.
e. The hash function should be able to withstand birthday assaults (finding any 2 messages with the same hash value, perhaps by iterating through minor permutations of two messages).

This method works with “.doc, .pdf, .txt” and other file formats, and the hash function may be used to handle data of varying sizes. The word "dynamic" refers to the fact that the hash function's output varies depending on the amount of the input.

1.4. Elliptic Curve Cryptography (ECC):

Elliptic curve cryptography is a relatively recent family of public-key algorithms that may offer lower key lengths and better performance over systems based on integer factorization and discrete logarithms, depending on the environment and application. Its security, benefits, and performance are described here. ECC's security issues are based on certain tough mathematical difficulties. Elliptic curves are based on a mathematical framework that allows for the definition of certain operations(25). These procedures result in a one-way function that may be utilized to create efficient cryptographic systems. This one-way function is known as the Elliptic Curve Discrete Logarithm Problem in ECC (ECDLP). Because the ECDLP is based on the same one-way function as DSA and Diffie-Hellman, elliptic curve analogs of each of these algorithms have been developed.

The security and benefits of utilizing elliptic curve-based cryptographic systems instead of integer factorization and discrete logarithm-based techniques are that they offer comparable levels of security with shorter key lengths. Most people believe that the security of integer factorization and discrete logarithm issues is about comparable. ECC's performance compared to other methods is 5 to 15, 20 to 60, and occasionally 400 times quicker, depending on the ECC bit.

Because it is quicker and uses less memory than RSA, the Elliptic Curve Cryptography method is also suited for smart card applications.

2. DISCUSSION

Table 1 shows the analysis of different type'scryptography techniques reviewed in this paper Rivest Shamir and Adleman (RSA) algorithm, Diffie-Hellman Algorithm, Digital Signature Algorithm.

TABLE 1: REPRESENT THE ANALYSIS ON DIFFERENT TYPES OF CRYPTOGRAPHY TECHNIQUES.

S. No.	Cryptography Technique	Analysis
1.	Rivest Shamir and Adleman (RSA) algorithm	Because mobile nodes are susceptible to numerous assaults owing to their broadcast nature, RSA may be employed in them. Because of its high time complexity and consumption requirement, RSA is not appropriate for WSN.
2.	Diffie-Hellman Algorithm	Keys are transferred between two users that are unaware of one other.

		In the asymmetric (public-key) situation, a suggested for two goals: authenticated key agreement and authenticated key agreement with key confirmation.
		It may be utilized on the Internet and in virtually every encryption technique now in use, such as SSL, SSH, IPSec, and PKI.
3.	Digital Signature Algorithm	Public-key algorithms that may offer lower key lengths and better performance over systems based on integer factorization and discrete logarithms, depending on the context and application in which they are employed.
		ECC's performance compared to other methods is 5 to 15, 20 to 60, and occasionally 400 times quicker, depending on the ECC bit.

3. CONCLUSION

Cryptosystems are generally believed to relate solely to mathematical processes and computer programs; nevertheless, they also involve human behavior control, such as selecting difficult-to-guess passwords, turning off unneeded systems, and not discussing sensitive operations with outsiders. Different kinds of encryption methods are discussed in this article, and after examining all of the above-mentioned cryptography techniques, it can be determined that ECC is quicker than RSA due to its short key. However, in comparison to RSA, its mathematical operation is more difficult. Secret keys are transferred between two users in the Diffie-Hellman cryptography method. In DSA, the receiver uses a digital signature to ensure that the signal received is unmodified.

REFERENCES:

1. Mian SM, Kumar R. Review on Intend Adaptive Algorithms for Time Critical Applications in Underwater Wireless Sensor Auditory and Multipath Network. In: 2019 International Conference on Automation, Computational and Technology Management, ICACTM 2019. 2019.

2. Rahul M, Kohli N, Agarwal R, Mishra S. Facial expression recognition using geometric features and modified hidden Markov model. Int J Grid Util Comput. 2019;

3. Agrawal T, Agrawal AK, Singh SK. An efficient key-accumulation cryptosystem for cloud. Int J Eng Adv Technol. 2019;

4. Agrawal T, Agrawal AK, Singh SK. Cloud sanctuary through effectual access control and cryptographic model. J Adv Res Dyn Control Syst. 2019;

5. Kumar V, Sharma A, Mitali VK, Sharma A. A survey on various cryptography techniques. Int J Emerg Trends Technol Comput Sci. 2014;

6. Sheth RK. Analysis of Cryptography Techniques. Int J Res Adv Eng. 2015;

7. Francis N, Monoth T. An Analysis of Hybrid Cryptographic Approaches for Information Security. Int J Appl Eng Res. 2018;

8. Morin O, Huang K, Liu J, Le Jeannic H, Fabre C, Laurat J. Remote creation of hybrid entanglement between particle-like and wave-like optical qubits. Nat Photonics. 2014;

9. Rouse M. RSA algorithm (Rivest-Shamir-Adleman). TechTarget. 2014;

10. Aryanti A, Mekongga I. Implementation of Rivest Shamir Adleman Algorithm (RSA) and Vigenere Cipher in Web Based Information System. In: E3S Web of Conferences. 2018.

11. Mishra S, Jain S, Rai C, Gandhi N. Security challenges in semantic web of things. In: Advances in Intelligent Systems and Computing. 2019.

12. Sharma TK. Enhanced butterfly optimization algorithm for reliability optimization problems. J Ambient Intell Humaniz Comput. 2021;

13. Dutta C, Singhal N. A cross validated clustering technique to prevent road accidents in VANET. In: Proceedings of the 2018 International Conference on System Modeling and Advancement in Research Trends, SMART 2018. 2018.

14. Tange H, Andersen B. SPDH - A secure plain diffie-hellman algorithm. J Cyber Secur Mobil. 2012;

15. Boni S, Bhatt J, Bhat S. Improving the Diffie-Hellman Key Exchange Algorithm by Proposing the Multiplicative Key Exchange Algorithm. Int J Comput Appl. 2015;

16. Singh P, Tyagi N. Radial Basis Function For Handwritten Devanagari Numeral Recognition. Int J Adv Comput Sci Appl. 2011;

17. Singh R, Singhal N. An enhanced vehicle parking management using artificial intelligence. In: Proceedings of the 2018 International Conference on System Modeling and Advancement in Research Trends, SMART 2018. 2018.

18. Awasthi Y, Sharma A, Pandey R. Image Watermarking Using APDCBT in Selected Pixel Blocks. In: Proceedings of the 2019 8th International Conference on System Modeling and Advancement in Research Trends, SMART 2019. 2020.

19. Sharma TK, Rajpurohit J, Prakash D. Enhanced Local Search in Shuffled Frog Leaping Algorithm. In: Advances in Intelligent Systems and Computing. 2020.

20. Tyagi VK, Goel R, Singh M, Kumar S. Modeling and analysis of a closed loop supply chain with uncertain lead time in the perspective of inventory management. Int J Sci Technol Res. 2020;

21. Rai DV, Kumar G. Soul and mind as quantum states of an embedded human system. Int J Sci Technol Res. 2020;

22. Sharma BK, Agarwal RP, Singh R. An efficient software watermark by equation reordering and FDOS. In: Advances in Intelligent and Soft Computing. 2012.

23. Pornin. Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA). Appl Microbiol Biotechnol. 2013;

24. Haddaji R, Bouaziz S, Ouni R, Mtibaa A. Comparison of Digital Signature Algorithm and Authentication Schemes for H.264 Compressed Video. Int J Adv Comput Sci Appl. 2016;

25. Jain N, Awasthi Y. WSN-AI based Cloud computing architectures for energy efficient climate smart agriculture with big data analysis. Int J Adv Trends Comput Sci Eng. 2019;