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

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).*

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;