IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, February 2023

Exploring Number Theory Applications in Cryptography and Security Analysis

Pramod Kumar[1] and Dr. Vineeta Basotiya[2]
Research Scholar, Department of Mathematics[1]
Assistant Professor, Department of Mathematics[2]
Shri J. J. T. University, Rajasthan, India

Abstract: *Number theory a subject of pure mathematics is essential to security applications and cryptography. This study examines number theory's underlying ideas and practical applications to ensure data privacy, soundness, and correctness in current cryptographic systems. Primordial numbers, modular arithmetic, and integer characteristics are introduced in the essay. This research clearly explores how prime numbers aid key exchange methods and cryptographic key creation. Modular exponentiation, which underpins many encryption and decryption algorithms, is also addressed in modular arithmetic. The paper also considers using number theory to create digital signatures that verify data. It studies the mathematical foundations of digital signature algorithms like the Elliptic Curve Digital Signature Algorithm (ECDSA) and the RSA signature scheme, which use modular arithmetic and prime numbers to verify digital document authenticity and integrity. The limits and uses of number theory-based encryption are also examined. Advances in computer hardware and computational complexity affect system security. The paper examines post-quantum cryptography, which seeks to create cryptographic algorithms that are secure even with quantum computers.*

Keywords: Modular arithmetic, Prime numbers, Factorization.

REFERENCES

[1]. Hoffstein, J., Pipher, J., Silverman, J.H.. "An Introduction to M athem atical Cryptography," Springer. 2010.
[2]. Analysis of Number Theory for Cryptography and Security Applications Koblitz, Neal. "A Course in Number Theory and Cryptography," Springer-Verlag, 1987.
[3]. Luma, A., Raufi, B. "Relationship between Fibonacci and Lucas Sequences and Their Application in Symmetric Cryptosystem s," Latest Trends on Circuits, Systems and Signals, 2010.
[4]. Matousesk, Radomil. "Knapsack Cipher and Cryptanalyst Using Heuristic M ethods,"
[5]. Institute of Autom ation and Com puter Science, Brno University of Technology, Menezes, A., Vanstone, S., "Elliptic Curve Cryptosystems and Their Im plem entation," Journal of Cryptology, 1993.
[6]. Paterson, Kenneth G. "Cryptography from Pairings: A Snapshot of Current Research," Information Security Group, University of London. November, 2002.
[7]. Raphael, A. Joseph, Sundaram, Dr. V., "Secured Communication through Fibonacci Numbers and Unicode Symbols," International Journal of Scientific and Engineering Research, Vol. 3, Iss.4, April, 2012
[8]. S. Chandra, "A comparative survey of symmetric and asymmetric key cryptography", file:///C:/Users/deepanshu/Desktop/workingpaper/working paper/Analysis and Comparison of Substitution and Transposition Cipher.pdf, pp. 83-93, 2014.
[9]. K. Renuka and G.N. Harshini, "Analysis and Comparison of Substitution andTransposition Cipher", vol. 6, no. 2, pp. 549-555, 2019.
[10]. P. Security, "Recent Parables in Cryptography", vol. 2, no. file:///C:/Users/deepanshu/Desktop/working paper/working paper/Understanding Cryptography by Christof Paar.pdf, pp. 82-86, 2014.
[11]. M. Mushtaq Faheem, S. Jamel, A. Hassan Disina, Z. A. Pindar, N. Shafinaz Ahmad Shakir and M. Mat Deris, "A survey on the cryptographic encryption algorithms", Int. J. Adv. Comput. Sci. Appl, vol. 8, no. 11, pp. 333-344, 2017.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, February 2023

[12]. B. Purnama and A. H. H. Rohayani, "A New Modified Caesar Cipher Cryptography Method with LegibleCiphertext from a Message to Be Encrypted", Procedia Comput. Sci, vol. 59, no. Iccsci, pp. 195-204, 2015.

[13]. Jain and A. K. Pandey, "Modeling And Optimizing Of Different Quality Characteristics In Electrical Discharge Drilling Of Titanium Alloy (Grade-5) Sheet", Material Today Proceedings, vol. 18, pp. 182-191, 2019

[14]. A. Jain, A. K. Yadav and Y. Shrivastava, "Modelling and Optimization of Different Quality Characteristics In Electric Discharge Drilling of Titanium Alloy Sheet", Material Today Proceedings, vol. 21, pp. 1680-1684, 2019

[15]. M. Mushtaq Faheem, S. Jamel, A. Hassan Disina, Z. A. Pindar, N. Shafinaz Ahmad Shakir and M. Mat Deris, "A survey on the cryptographic encryption algorithms", Int. J. Adv. Comput. Sci. Appl, vol. 8, no. 11, pp. 333-344, 2017.

[16]. Jain and A. K. Pandey, "Multiple Quality Optimizations In Electrical Discharge Drilling Of Mild Steel Sheet", Material Today Proceedings, vol. 8, pp. 7252-7261, 2019

[17]. Chung-Ping Wu, C.-C. Jay Kuo, "Design of integrated multimedia compression and encryption systems", IEEE Transactions on Multimedia, vol.7, no. 5, 2005, pp. 828

[18]. Vikram Jagannathan, Aparna Mahadevan, Hariharan R., Srinivasan E., "Simultaneous color image compression and encryption using number theory", Proceedings of ICIS 05, 2005, pp. 1.

[19]. Mehmet Utku Celika, Gaurav Sharma, A. Murat Tekalp, "Gray-level- embedded lossless image compression", Signal Processing: Image Communication 18, 2003, pp. 443-454.

[20]. Said and W. A. Pearlman, "A New, Fast and Efficient Image Codec Based on Set Partitioning in Hierarchical Trees," IEEE Trans. on Circuits and Systems for Video Technology, Vol. 6, No. 3, June 2000, pp. 243.