IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 5, June 2022
Impact Factor: 6.252

The Hill Cipher Algorithm for Data Encryption and Decryption

Ayush Gupta
Student, Department of Computer Science & Information Technology
Dronacharya College of Engineering, Gurugram, India

Abstract: *The science of encoding and decoding signals is known as cryptography. Cryptography is frequently used in people's daily life to keep sensitive data, such as Mastercard data, safe. Many regular exercises can be easily viewed by unintentional outsiders via the Internet. Hill cipher is a simple linear transformation represented by a matrix that is a traditional cryptography based on linear algebra. It is one of the symmetric key algorithms with various data encryption advantages. However, the inverse of the plaintext encryption key matrix is not always available. The encrypted text cannot be decoded if the key matrix is not invertible. The key matrix employed for encryption in the Involutory matrix generation method is invertible. As a result, we do not need to find the inverse of the key matrix during decryption.*

Keywords: Symmetric Key Algorithms

REFERENCES

[1]. H. Ming dan S. LiZhong, "A New System Design of Network Invasion Forensics," in 2009 Second International Conference on Computer and Electrical Engineering, 2009, hal. 596–599.
[2]. A. Lubis dan A. P. U. Siahaan, "Network Forensic Application in General Cases," IOSR J. Comput. Eng., vol. 18, no. 6, hal. 41–44, 2016.
[3]. F. H. Khan, R. Shams, F. Qazi, dan D.-E.-S. Agha, "Hill Cipher Key Generation Algorithm by using Orthogonal Matrix," Int. J. Innov. Sci. Mod. Eng., vol. 3, no. 3, hal. 5–7, 2015.
[4]. A. P. U. Siahaan, "Three-Pass Protocol Concept in Hill Cipher Encryption Technique," Int. J. Sci. Res., vol. 5, no. 7, hal. 1149–1152, 2016.
[5]. W. Stallings, Cryptography and Network Security Principles and Practices, 4th ed. Prentice Hall, 2005.
[6]. A. P. U. Siahaan, How to Code: Advanced Encryption Standard in C#. Medan: Fakultas Ekonomi Universitas Panca Budi, 2018.
[7]. A. Putera Utama Siahaan, E. Elviwani, dan B. Oktaviana, "Comparative Analysis of RSA and ElGamal Cryptographic Public-key Algorithms," in Proceedings of the Joint Workshop KO2PI and The 1st International Conference on Advance & Scientific Innovation, 2018.
[8]. X. Liu, Z. Wei, and C. J. Carter, A novel image encryption approach using block based transformation and random phase encoding,.
[9]. S. Muttoo, D. Aggarwal, and B. Ahuja, "A Secure Image Encryption Algorithm Based on Hill Cipher System," Bulletin of Electrical Engineering and Informatics, vol. 1, no. 1, 2012.
[10]. M. A. Aljanabi, N. A. Shnain, and S. F. Lu, "An image similarity measure based on joint histogram — Entropy for face recognition," in Proceedings of the 3rd IEEE International Conference on Computer and Communications (ICCC '17), pp. 1626–1631, Chengdu, December 2017.
[11]. B.M.Verdiana, Coverage 6, 2020, Retrieved from liputan6.com: https://www.liputan6.com/global/read/4214488/who-unjukkan-corona-covid-19-tak-menular-kapalair-ini-pelaksanaannya
[12]. H. Anton, C. Rorres, Elementary Linear Algebra, America, Wiley, 2004
[13]. Melvin Steven Hernández, Dr. Alfredo Cruz (Advisor, Study of the Hill Cipher Encryption/Decryption Algorithm, 28-08-2012