A Hybrid Cryptosystem that Uses the Vigenère Cipher and the Columnar Transposition Cipher

Shivani Anil Mahajan

Lecture, Department of Computer Application

Dr. Varsha Patil Women's College of Computer Application, Jalgaon, India

Abstract: *One of the main concerns that information security addresses is privacy. One can stop a third party from deciphering transmitted raw data by using cryptographic encryption techniques. Data over an unprotected channel while a signal is being transmitted. In the modern era, cryptographic techniques for improving the security of digital content have become increasingly important. Information security aims to address two major issues: security breaches and the misuse of private data that has been intercepted by unauthorized parties.*

By creating a novel hybrid method of plaintext encryption, this paper aims to advance the general corpus of knowledge in the field of classical cryptography. The columnar transposition cipher is used to encrypt the plaintext, and the cryptosystem then uses the cipher text to use the Vigenère cipher to re-encrypt the plaintext. Finally, the cipher text was subjected to cryptanalysis. Java programming will be used for the implementation.

Keywords: columnar transposition, Vigenère, encryption, cryptography, and key