Vigenere cipher is one of the earliest known polyalphabetic cipher which was considered secure for a very long time until 1917 when friedman and kasiski were able to break it by determining repeating segments of the ciphertext and using it to determine the length of the key. Once the length of the key is known, the ciphertext could be grouped in columns and treated as a separate caesar cipher which can be solved. Over the years, a lot of modification has been done to improve the security of the vigenere cipher. This paper presents a review of the vigenere cipher and also discusses various existing modifications.

References


Index Terms

Computer Science

Information Systems

Keywords
Cipher, Cryptography, Encryption, Substitution, Vigenere.