Abstract

Cryptography is a science of converting clear message into secret message "unreadable message", where message was encrypted at sender side then decrypted at receiver side. Vigenere is an example of substitution cipher, it has various limitations, in this paper we propose an advanced encryption algorithm which improves the security of Vigenere method by combining it with modern cipher method like Stream cipher, Stream cipher relatively regards as unbreakable method, and it uses binary form (instead of characters) where the Plaintext, Ciphertext and the Key are strings of bits. When applying the proposed algorithm, we see that the mentioned above combination cipher has a high degree of security, where cipher based on just Vigenere method is not secure. Also, the proposed algorithm makes the cryptanalysis, using frequency attack, more difficult.

References

- Menezes A. J., Oorschot P. C. and Vanstone S. A. handbook of applied
cryptography, CRC Press, 1996.
- http://www.simonsingh.net/The_BlackChamber/cracking_tool.
- Albrecht Beutelspacher: "Cryptography: an introduction to the art and science of enciphering";

Index Terms

Computer Science  Security

Keywords

Plaintext  Ciphertext  Key  Cipher  Substitution  Vigenere  Stream cipher