Abstract

This paper presents a different way for implementation of one-time pad. The one-time pad are known as the mother of all encryption schemes, since it is known to be information-theoretically secure in contrast to other encryption schemes used in practice, which are at most computationally secure. Our proposed way will make encryption impossible to crack if used correctly. We are implementing one-time pad encryption technique using both block cipher and one-way hash. In this proposed method each bit or character from the plaintext is encrypted by a modular addition with a bit or character from a secret random key of the same length as the plaintext, resulting in a cipher text. If the key is truly random and at least as long as the plaintext also never reused in whole or part and kept secret the cipher text will be impossible to decrypt or break without knowing the key.

Index Terms
Computer Science
Security

Keywords
One-Time Pad Encryption Block Cipher Randomness One–Way Hash Decryption