

**Department of Computer Engineering**

**LMS Assignment 8**

Q. 1 What is the principle behind One-Time-Pad (OTP). Why they are highly secure? [10 M]

In cryptography, the one-time pad (OTP) is an encryption technique that cannot be cracked if used correctly. In this technique, a plaintext is paired with a random secret key (also referred to as a one-time pad). Then, each bit or character of the plaintext is encrypted by combining it with the corresponding bit or character from the pad using modular addition. If the key is truly random, is at least as long as the plaintext, is never reused in whole or in part, and is kept completely secret, then the resulting ciphertext will be impossible to decrypt or break.[1][2][3] It has also been proven that any cipher with the perfect secrecy property must use keys with effectively the same requirements as OTP keys.[4] However, practical problems have prevented one-time pads from being widely used.