Roll #.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Nothing should be written on question paper)

**IQRA NATIONAL UNIVERSITY, PESHAWAR, PAKISTAN**

# Advance Network Security

## Program: MSCS Final Term Exam Semester: Summer-2020

## Maximum Marks: 50 Time Allowed: 4 Hour

* 1. **What is meant by DES? Describe its history with Encryption Techniques Overview. Also describe its DES Round structure with substitution boxes overview. (10)**
  2. **Distinguish between Differential and Linear Cryptanalysis techniques. Explain their features with design characteristics alongwith diagram. (10)**
  3. **Apply the following 3 codes to the given text:**

**Monoalphabetic Cipher**

**Playfair Cipher**

**Vigenere Cipher**

**Step by step process should be mentioned when performing the activity.**

1. **The sections on quantum cryptography, quantum proper ties of squeezed light, and experimental efforts to measure gravitational waves provide adequate introduction to these exciting applications of quantum optics.**
2. **The implementation of a public key cryptography package needs to ensure that the random number object used in the generation of key pairs cannot be accessed by clients of the package.**
3. **Components for these systems are now commercially available, and it seems very likely that quantum cryptography will be an important technology long before quantum computers of useful size are constructed.**

**(10+10+10)**