Cryptography

(CSC 421)

Assignment 1

Submitted By-

Your Name
University Number: 123456

Submitted To-

Dr. Mohammad Shoab
Department of Computer Science
Shaqra University

Instructions:

- Draw diagrams wherever relevant. Explain your notations explicitly and clearly.
- An incomplete assignment is NOT acceptable for submission.
- Once you submit your assignment, you will be expected to answer all the questions there INDEPENDENTLY. You may be asked to answer any question of the assignment in the class.

Q1. Define Cryptography and Cryptanalysis. Draw and explain conventional cryptosystem.

Q2. List and explain various types of attacks on encrypted messages.

Q3. What is the objective of attacking an encryption system? Write two approaches to attack a conventional encryption scheme.

Q4. Define Caesar Cipher and Cryptography.

Q5. Explain Rail fence technique.