# Course Outline
# Cryptography and its Applications

| | | | |
|---|---|---|---|
| **Schedule** | As per Time Table | **Website** | ssc.umt.edu.pk |
| **Instructor** | Dr. Sohail Zafar | **Contact** | Sohail.zafar@umt.edu.pk |
| **Course Description** | This course is an introduction to the basic theory and practice of cryptographic techniques. It is self contained, however a basic understanding of number theory and probability theory will be helpful. The course is intended for master's students. | | |
| **Textbooks** | Introduction to Cryptography by Johannes Buchmann | | |
| **Reference Material** | Introduction to Modern Cryptography by J. Katz and Y. Lindell. | | |

## Course Outline:

1. **Cryptosystem**

- Basic Definitions and Notations

2. **Historical Cryptosystems and their Cryptanalysis**

- Caesar Cryptosystem
- Subsitution Cryptosystem
- Vigenere Cryptosystem
- Four square Cryptosystem
- Hill Cryptosystem

3. **Criteria to secure your cryptosystem**

- Perfect security in Cryptosystem
- Verman one Time pad
- Shanon's Theorem and its applications

4. **Discrete Logrithm Problem and some techniques to solve it**

- Key exchange Problem
- Diffie-Helleman problem and Key exchange Algorithm
- Shank's Algorithm
- Pohilg- Helleman Algorithm

## 5. Modern Cryptosystems and their Cryptanalysis

- Public key Cryptosystem
- Elgamal Cryptosystem
- Naive, Fermat and Millar-Rabin Test
- RSA Cryptosystem
- Hastad’s Broadcast Attack
- Common Modules Attack
- Wiener’s Attack
- Merkle–Hellman Knapsack Cryptosystem

## 6. Elliptic curves and Cryptosystem

- Basics on Elliptic curves
- Cryptosystems using Elliptical curves

## 7. Applications

- Image encryption technicques using Matlab
- Computer security