Course Outline

MTH-728 Mathematical Cryptography

|  |  |  |  |
| --- | --- | --- | --- |
| **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**  **Reference Material** | Introduction to Cryptography by Johannes Buchmann  I[ntroduction to Modern Cryptography](http://www.cs.umd.edu/~jkatz/imc.html) by J. Katz and Y. Lindell. | | |

|  |  |
| --- | --- |
| **Course Outline:** | 1. **Cryptosystem**  * Basic Definitions and Notations  1. **Historical Cryptosystems and their Cryptanalysis**  * Caesar Cryptosystem * Subsitution Cryptosystem * Vigenere Cryptosystem * Four square Cryptosystem * Hill Cryptosystem  1. **Criteria to secure your cryptosystem**  * Perfect security in Cryptosystem * Verman one Time pad * Shanon’s Theorem and its applications  1. **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  1. **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  1. **Elliptic curves and Cryptosystem**  * Basics on Elliptic curves * Cryptosystems using Elliptical curves  1. **Applications**  * Image encryption technicques using Matlab * Computer security |