



PURE MATHEMATICS 329 "INTRODUCTION TO CRYPTOGRAPHY"

Calendar Description: H(3-1T)

Description and analysis of cryptographic methods used in the authentication and protection of data. Classical cryptosystems and cryptanalysis, information theory and perfect security, the Data Encryption Standard (DES) and Public-key cryptosystems.

Prerequisite: Mathematics 271 or 273 or Pure Mathematics 315.

Syllabus

| <u>Topics</u> | <u>Number of hours</u> |
|---|------------------------|
| Basic Ideas and substitution Ciphers, Cryptanalysis and n-gram Ciphers | 6 |
| Polyalphabetic Substitution Ciphers Statistical Attacks on Polyalphabetic Ciphers | 6 |
| Cipher Machines | 3 |
| Elementary Information Theory Entropy and Unicity distance | 6 |
| Transposition Ciphers and Product Ciphers | 3 |
| The Data Encryption Standard (DES), Triple DES Modes of Operation and Authentication | 6 |
| The Advanced Encryption Standard (AES) | 3 |
| One Way Functions and Cryptographic Key Agreement Public-Key Cryptography | 6 |
| TOTAL HOURS | 39 |

* * * * *