Department of Mathematics
Faculty of Mathematics & Computer Science
M.Sc. (Applied Mathematics), 3rd Semester

Course Code	AM 303
Course Title	Cryptography
Course Credits	04

Course objective:

The objective of the course is to provide a basic understanding of the modern encryption system. The course provides an introduction to basic number theory, symmetric and asymmetric cryptosystem.

Minimum Pre-requisites:

Course structure:

Introduction and Mathematical Foundations
Introduction, Overview on Modern Cryptography, Number Theory, Probability and Information Theory.

Classical Cryptosystems
Classical Cryptosystems, Cryptanalysis of Classical Cryptosystems

Symmetric Key Ciphers
Symmetric Key Ciphers, Modern Block Ciphers (DES), Modern Block Cipher (AES), Cryptanalysis of Symmetric Key Ciphers, Linear Cryptanalysis, Differential Cryptanalysis

Asymmetric Key Ciphers
RSA, Diffie Hellman Key Exchange algorithm, ElGamal Encryption Algorithm, Elliptic Curve Cryptography, Digital Signatures.

Reading suggestions:

- Wenbo Mao, "Modern Cryptography, Theory& Practice", Pearson Education, 2003
- William Stalling, “Cryptography and network security: principles and practices”, prentice hall fourth edition 2005
- Behrouz A. Forouzan, “Cryptography & Network Security”, McGraw-Hill, 2008
- Bruce Schneier, “Applied CryptographyProtocols, Algorithms, and Source Code in C”, John Wiley & Sons,second edition, 1996.

- Johannes Buchmann,“Introduction to cryptography”, Springer Second Edition, 2004

Evaluation and weightage:

- Surprise Quiz / test – 15 Marks
- Assignments - 05 Marks
- Class attendance and interaction during class – 5 Marks
- Mid Semester Examination – 40 Marks
- End Semester Examination – 40 Marks