MATH-471 Cryptography

Credit Hours: 3-0

Prerequisite: MATH-274 Elementary Number Theory

Course Objectives: Cryptography is the practice and study of techniques for secure communication in the presence of third parties. The focus of the course is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity and authentication.

Detailed Course Contents: Overview of cryptology, Cryptanalysis, Module arithmetic and integer rings, Symmetric Cryptography, Shift Ciphers and affine Ciphers, Introduction to stream ciphers, Random numbers and unbreakable stream ciphers, Shift register based stream ciphers, Introduction to data encryption standards (DES), Overview of DES algorithm, Internal structure of DES, Key Schedule, Decryption of DES, Advanced encryption standard, Galois field, Encryption with Block-Ciphers: Modes of Operation, Increase the Security of Block Ciphers, Symmetric vs Asymmetric Cryptology, Practical Aspects of Public-Key Cryptology, Essential Number Theory for Public-Key Algorithms

Course Outcomes:

- To understand the concept and importance of Information security and its applications in computer security and Financial Markets.
- Student's must understand and be able to understand the classical ciphers and their cracking by using elementary number theory

Text Book: C. Paar and J. Pelzl, Understanding Cryptography, Springer, 2nd Edition, 2010.

Reference Books:

1. J. Katz, Y. Lindell, Introduction to Modern Cryptography, Chapman and Hall, 2007.
2. J. Hoffstein, J. Pipher, J. H. Silverman, An Introduction to Mathematical Cryptography, Springer, 2008.
3. Buchmann, J., Introduction to Cryptography, Springer, 2004
4. J. Menezes, P. C. van Oorschot, S. A. Vanstone, Handbook of Applied Cryptography,CRC Press; 1st edition, 1996.

Weekly Breakdown		
Week	***Section***	***Topics***
1	1.1-1.3	Overview of cryptology, symmetric cryptography, Cryptanalysis,

2	1.4	Module arithmetic and integer rings, Shift ciphers and affine ciphers
3	2.1	Introduction to stream ciphers (stream ciphers vs block ciphers; Encryption and decryption with stream ciphers)
4	2.2-2.3	Random numbers and unbreakable stream ciphers, Shift register based stream ciphers
5	3.1-3.2	Introduction to data encryption standards (DES), Overview of DES algorithm
6	3.3	Internal structure of DES • Initial and final permutation The f-function
7	3.3 (Contd.), 3.4	Key Schedule, Decryption of DES
8	4.1-4.2	Introduction to Advanced encryption standard (AES), Overview of AES algorithm
9	**Mid Semester Exam**	
10	4.3	Existence of finite fields; Prime fields, Extension fields $GF\ (2^m)$
11	4.3 (Contd.)	Addition and subtraction in $GF\ (2^m)$, Multiplication in $GF\ (2^m)$, Inversion in $GF\ (2^m)$
12	4.4	Byte substitution layer, Diffusion layer, Key addition layer
13	4.4 (Contd.), 4.5	Key schedule, Decryption of AES
14	5.1	Encryption with Block-Ciphers: Modes of Operations
15	5.3	Increase the Security of Block Ciphers
16	6.1-6.2	Symmetric vs Asymmetric Cryptology, Practical Aspects of Public-Key Cryptology
17	6.3	Essential Number Theory for Public-Key Algorithms
18	**End Semester Exam**	