CS 11615: Network Security

Summer 2010

Instructor: Hicham G. Elmongui, Ph.D.

Required Textbooks:

- Cryptography and Network Security: Principles and Practice, Fourth Edition by William Stallings, Prentice Hall.

Pre-requisite:
Undergraduate-level knowledge in Programming, Computer Network, and Probability Theory.

Recommended References:

- Handbook of Applied Cryptography by Alfred Menezes (Editor), Paul van Oorschot (Editor), and Scott Vanstone (Editor).
- Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition by Bruce Schneier.
- Cryptography: Theory and Practice, Second Edition by Douglas R. Stinson

Course Description:
This is an in-depth course to both the principles and practice of cryptography and network security. In particular, we will focus on applied cryptography protocols and algorithms followed by up-to-date applications of network security.

Topics Covered (Tentative):

- Introduction to computer security concepts
- Classical encryption techniques
- Block Ciphers and the Data Encryption Standard
- Concepts in Number Theory
- Advanced Encryption Standard
- Block Cipher Operation
- Stream Ciphers
- Public-Key Cryptography
- Cryptographic Hash Functions
- Digital Signatures
- Key Management and Distribution
- User Authentication Protocols
- Transport-Level Security
- Wireless Network Security
- Electronic Mail Security
- IP Security

Policies:
The course follows the Academic Regulations for VT-MENA graduate students.

Grading (Tentative):

- 6 homework assignments: 60%
- 1 seminar on a network security practice: 20%
- Final exam: 20%