School of Information Technology
International Business College

7 Greenfield Parade
Bankstown 2200 NSW Australia

Cryptography and Network Security

Subject Coordinator and Lecturer: Professor Minh Hung Le
School of Information Technology
International Business College
7 Greenfield Parade
Bankstown 2200 NSW Australia
Tel: (02) 9645 3126
Fax: (02) 9790 3302
Emails: m.le@sece-unsw.org or minhle@ieee.org

Aim of Unit:

This unit covers the theory and practice of cryptography and network security, including authentication, electronic mail security, web security, firewalls. In this age of viruses and hackers, of electronic eavesdropping and electronic fraud, security is paramount. The disciplines of cryptography and network security have matured, more practical, readily available applications to enforce network security have developed. The basic issues to be addressed by a network security capability are explored through a tutorial and survey of cryptography and network security technology. The practice of network security is explored via practical applications that have been implemented and are in use today.

Unit Outline:

- Describe Symmetric Ciphers, Encryption.
- Determine Finite Fields, Number Theory.
- Explain Public-Key Encryption, RSA and Hash Functions.
- Demonstrate Network Security Practice.
- Express Authentication, Electronic Mail Security, IP Security, Web Security.
- Describe System Security, Intruders, Malicious Software, Firewalls.

Mode of Delivery:

Two hours lecture per week.
One hour tutorial per week.

Unit Assessment:

Assignments	20 %
Mid-Semester Test	20 %
Final Examination	60 %

Assessment Requirements:

Students must receive 50% or more for each part of Unit Assessment in order to pass the subject.

Student Workload:

Students will have 3 hours per week face-to-face learning during semester.
Students are expected to work at least 5 hours per week out of class.

Text Book:

1. William Stallings, "Cryptography and Network Security", 4th edition, Prentice Hall, 2006

Recommended References:

1. Bruce Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C", 2nd edition, Wiley, 1995
2. Doug Stinson, "Cryptography: Theory and Practice", 2nd edition, CRC Press, 2002
3. Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vanstone, "Handbook of Applied Cryptography", CRC Press, 2001, (free download available online: http://www.cacr.math.uwaterloo.ca/hac/)
4. Charlie Kaufman, Radia Perlman, Mike Speciner, "Network Security: Private Communication in a Public World", Prentice Hall, 2nd edition, 2003

Subject Schedule

Weeks	Lecture/Tutorial Topics	Assignments	Reading from Text Book
1	Overview, Classical Encryption Techniques	Assignment #1	Chapters 1,2
2	Block Ciphers and The Data Encryption Standard, More on Symmetric Ciphers	Assignment #2	Chapters 3,6
3	Introduction to Finite Fields, Introduction to Number Theory	Assignment #3	Chapters 4,8
4	Advanced Encryption Standard, Confidentiality Using Symmetric Encryption	Assignment #4	Chapters 5,7
5	Public-Key Cryptography and RSA	Assignment #5	Chapter 9
6	Key Management; Other Public-Key Cryptosystems	Assignment #6	Chapter 10
7	**Mid-Semester Test**		
8	Message Authentication and Hash Functions, Hash and Mac Algorithms	Assignment #7	Chapters 11,12
9	Digital Signatures and Authentication Protocols, Authentication Applications	Assignment #8	Chapters 13,14
10	Electronic Mail Security, IP Security	Assignment #9	Chapters 15,16
11	Web Security, Intruders	Assignment #10	Chapters 17,18
12	Malicious Software, Firewalls	Assignment #11	Chapters 19,20
13	Revision		
14	**Final Examination**		