

EE 560 – Computer Network Security

Spring 2009

Class Meets M-W-F 8:30-9:20 in T&B 307
14 January - 1 May 2009
Final Exam Period: 8:00 – 10:00

Instructor E.E. Johnson
Thomas & Brown 211
Office Hours: M-W-F 9:30–10:00, or by appointment
e-mail: ejohnson@nmsu.edu

Text *Cryptography and Network Security* (4th edition), W. Stallings
Cryptol Reference Manual
available for download at <http://www.ece.nmsu.edu/ee560/references.html>

Reference *Handbook of Applied Cryptography*, Menzes *et al.*
available for download at <http://www.cacr.math.uwaterloo.ca/hac/>

Course Objectives

- Learn the terminology and fundamental concepts of security in computing and communications systems
- Study and practice the mathematical techniques developed to provide security.
- Apply these techniques in protocols that provide the mathematical security of cryptographic algorithms to network tasks.
- Analyze the security of key Internet protocols.
- Develop presentation skills through teaching technical material to your classmates.

Outline	<u>Topic</u>	<u>Time (approx.)</u>
	Overview of network security	1 week
	Mathematical background	2 weeks
	Cryptographic algorithms	4 weeks
	————— Midterm Exam — 2 March —————	
	Public-key cryptography	2 weeks
	Cryptographic procedures and protocols	3 weeks
	Internet security	2 weeks

Grading	Class Participation (incl homework and presentations)	25 %
	Exams (2)	50 %
	Project(s)	25 %