

## COURSE DESCRIPTION

Department and Course Number	<b>CS 336 (formerly CS 437)</b>	Course Coordinator	<b>Barnard</b>
Course Title	<b>Computer Network Security</b>	Total Credits	<b>3</b>

### Current Catalog Description

*Conventional and public-key cryptography. Message encryption and authentication. Secure communication between computers in a hostile environment, including E-mail (PGP), virtual private networks (IPSec), remote access (SSH), and E-commerce (SSL). Firewalls. Mandatory weekly Linux-based lab.*

### Textbooks

*Network Security Essentials, 2<sup>nd</sup> ed., by William Stallings, Prentice Hall, 2003.*

*Lab manual locally written and duplicated*

References *None*

### Course Goals

*Thorough understanding of the threats facing transmission of information over internets, especially the global Internet, and the protective measures that are available (especially encryption and message authentication). Threats to wireless networks are included. Concepts presented in lectures are reinforced by the “hands-on” lab sessions.*

### Prerequisites by Topic

*Discrete Structures and Object-Oriented Design with “C” or better in both*

### Major Topics Covered in the Course

*Conventional Encryption, Encryption, Message Confidentiality, Public-Key Cryptography, Message Authentication, Authentication (Kerberos), Authentication (X.509), E-Mail Security (PGP), E-mail Security (S/MIME), IP Security, IP Security (Authentication), IP Security (Confidentiality), WWW Security (SSL), SSH, IEEE 802.11 WEP, Firewalls, IEEE 802.11 WPA*

### Laboratory projects (specify number of weeks on each)

*There are four lab sessions, one per week during the second half of the course.*

Estimate CSAB Category Content

	CORE	ADVANCED		CORE	ADVANCED
Data Structures	_____	_____	Computer Organization and Architecture	_____	_____
Algorithms			Concepts of Programming Languages	_____	_____
Software Design	_____	8			

Oral and Written Communications

*None*

Social and Ethical Issues

*None*

Theoretical Content

*Theory of encryption, both secret-key (eg. Rijndael) and public-key (eg. RSA): theory of hash functions (eg. SHA); about 22% of course.*

Problem Analysis

*None*

Solution Design

*None*