

## COURSE DESCRIPTION

Department and Course Number	<b>CS 336</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, 4th ed., by William Stallings, Pearson Prentice Hall, 2011.*

*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/participant authentication). Threats to wireless networks are included. Concepts presented in lectures are reinforced by the “hands-on” lab sessions.*

### Prerequisites by Topic

*Discrete Structures with “C” or better; Knowledge of basic TCP/IP recommended*

### Major Topics Covered in the Course

*Conventional Encryption,, Message Confidentiality, Public-Key Cryptography, Message and Participant Authentication, Authentication (Kerberos), Authentication (X.509), E-Mail Security (PGP), E-mail Security (S/MIME), 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, covering PGP, IPSec, SSL, and SSH/WEP.*

## 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/AES) and public-key (eg. RSA): theory of hash functions (eg. SHA); about 22% of course.*

## Problem Analysis

*10*

## Solution Design

*10*