

COURSE IMPLEMENTATION DATE: []  
 COURSE REVISED IMPLEMENTATION DATE: [January 2004]  
 COURSE TO BE REVIEWED: [Nov 2007]  
 (Four years after implementation date)

## OFFICIAL COURSE OUTLINE INFORMATION

Students are advised to keep course outlines in personal files for future use.  
 Shaded headings are subject to change at the discretion of the department and the material will vary - see course syllabus available from instructor

FACULTY/DEPARTMENT: <b>COMP 490</b>	<b>Computer Information Systems</b>	<b>3</b>
	FORMER COURSE NUMBER	UCFV CREDITS
<b>Network Security and Cryptography</b>		
COURSE DESCRIPTIVE TITLE		

**CALENDAR DESCRIPTION:**

This course provides students with an understanding of important concepts in network security and cryptography. A practical technological survey of cryptography and network security will be given. This includes conventional encryption algorithms such as DES and IDEA, public-key design and algorithms such as RSA and elliptic curve, digital signatures and authentication protocols, key managements, and applications of authentication such as Kerberos and X.509. IP security and web security will also be covered. Network security plans and procedures will be formulated at the end.

**PREREQUISITES:** MATH 106, CIS 390 with a grade of C or better. Acceptance to CIS degree program. (Students accepted to a CIS or Computing Science minor may register with permission of the department.)  
**COREQUISITES:**

SYNONYMOUS COURSE(S)	<b>SERVICE COURSE TO:</b>
(a) Replaces: _____ (Course #)	(Department/Program)
(b) Cannot take: _____ For further credit. (Course #)	(Department/Program)

TOTAL HOURS PER TERM: <b>45</b>	TRAINING DAY-BASED INSTRUCTION
<b>STRUCTURE OF HOURS</b>	LENGTH OF COURSE: _____
Lectures: <b>45</b> Hrs	HOURS PER DAY: _____
Seminar: Hrs	
Laboratory: Hrs	
Field Experience: Hrs	
Student Directed Learning: Hrs	
Other (Specify): Hrs	

MAXIMUM ENROLLMENT:	<b>35</b>
EXPECTED FREQUENCY OF COURSE OFFERINGS:	<b>Once per year</b>
<b>WILL TRANSFER CREDIT BE REQUESTED? (lower-level courses only)</b>	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>WILL TRANSFER CREDIT BE REQUESTED? (upper-level requested by department)</b>	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
<b>TRANSFER CREDIT EXISTS IN BCCAT TRANSFER GUIDE:</b>	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No

**AUTHORIZATION SIGNATURES:**

Course Designer(s): <b>Edward Lo</b>	Chairperson: _____ (Curriculum Committee)
Department Head: <b>Paul Franklin</b>	Dean: <b>Karen Evans</b>
PAC Approval in Principle Date: _____	PAC Final Approval Date: <b>December 03, 2003</b>

**COMP 490**  
COURSE NAME/NUMBER

---

---

**LEARNING OBJECTIVES / GOALS / OUTCOMES / LEARNING OUTCOMES:**

Students will explore network security and cryptography. At the end of this course, the student will have gained knowledge of:

- I. Conventional encryption algorithms
- II. Public-key encryption
- III. Digital signatures and authentication protocols
- IV. E-mail security
- V. IP and web security
- VI. Network security practices
- VII. Identification of security issues in an IT deployment plan
- VIII. Intrusion detection and responses
- IX. Various network security attacks and violations
- X. Network security plans and procedures

This will provide the student with the basic skills required in the network security industry.

**METHODS:**

Lecture

**PRIOR LEARNING ASSESSMENT RECOGNITION (PLAR):**

Credit can be awarded for this course through PLAR

Yes

No

**METHODS OF OBTAINING PLAR:**

Course challenge with departmental approval

**TEXTBOOKS, REFERENCES, MATERIALS:**

[Textbook selection varies by instructor. An example of texts for this course might be:]

*Cryptography and Network Security: Principles and Security*, 3<sup>rd</sup> Edition, William Stallings, Prentice-Hall, 2002.

*Network Security Essentials: Applications and Standards*, William Stallings, Prentice-Hall, 2000.

*The CERT Guide to System and Network Security Practices*, Julia H. Allen, Addison-Wesley, 2001.

*Linux System Security*, Scott Mann and Ellen L. Mitchell, Prentice-Hall, 2000.

*Windows 2000 Security: Technical Reference*, Internet Security Systems, Inc., Microsoft Press, 2000.

**SUPPLIES / MATERIALS:**

**STUDENT EVALUATION:**

[An example of student evaluation for this course might be:]

Participation	10%
Assignments and a project	30%
Mid term exam	20%
Final exam (comprehensive)	40%

**COURSE CONTENT:**

[Course content varies by instructor. An example of course content might be:]

- Various types of security attacks.
- The network access security model.
- Classical and modern conventional encryption techniques.
- Algorithms of conventional algorithms
- Public-key encryption
- Digital signatures and authentication protocols
- Applications of authentication
- Email security
- IP and Web security
- System and network security procedures
- Security issues and requirements
- Intrusion detection and response preparation
- Detecting intrusions
- Responding to intrusions