CIIC 5018 - Course Syllabus

1. General Information:

Alpha-numeric codification: CIIC 5018
Course Title: Cryptography and Network Security
Number of credits: 3
Contact Period: 3 hours of lecture per week

Equivalent Course: ICOM 5018

2. Course Description:

English: Theoretical and practical aspects in computing system and network security; thread models; system vulnerability to attacks such as: hackers, malicious code, Trojan horses, viruses, and worms; cryptographic techniques used to defend systems from such attacks.

Spanish: Aspectos teóricos y prácticos de seguridad en sistemas de computadoras y redes; modelos de amenazas; vulnerabilidad a ataques tales como: "hackers", código malicioso, caballos de Troya, virus y gusanos; técnicas criptográficas para defender los sistemas de dichos ataques.

3. Pre/Co-requisites and other requirements:

Prerequisites: CIIC 4050 or ICOM 5007

4. Course Objectives:

Students will learn to identify security threats and the cryptographic algorithms used to protect computer data and network communications. Then, students will use these algorithms to develop schemes to protect computer systems against typical security threads.

5. Instructional Strategies:

□conference □discussion □computation □laboratory

□seminar with formal presentation □seminar without formal presentation □workshop

□art workshop □practice □trip □thesis □special problems □tutoring

□research □other, please specify:

6. Minimum or Required Resources Available:

Students will use the Departmental computer laboratories to complete course projects.

7. Course time frame and thematic outline

Outline	**Contact Hours**
Introduction to cryptography	3
Modern algebra and private-key cryptography	3
Contemporary symmetric ciphers	6
Number theory and public-key algorithms	6
Key management and distribution	3
Authentication, signature, and electronic commerce protocols	3
Secure layers in the protocol stack	6
Security in applications, mail and web, Malware and countermeasures	6
Legal and Social Issues - Current legislation	3
Project presentations	3
Exams and discussions	3
Total hours: (equivalent to contact period)	45

8. Grading System

Quantifiable (letters) Not Quantifiable

9. Evaluation Strategies

	Quantity	**Percent**
Exams	**3**	**50%**
Final Exam	**1**	**20%**
Short Quizzes		

Oral Reports		
Monographies		
Portfolio		
Projects	**1**	**30%**
Journals		
Other, specify:		
TOTAL:		**100%**

10. Bibliography:

1. William Stallings, *Cryptography and Network Security*, 6th ed., Prentice Hall, 2013.
2. Niels Ferguson, Bruce Schneier, *Cryptography* Engineering: *Design Principles and Practical Applications*, John Wiley and Sons, 2010.
3. Matt Bishop, *Computer Security: Art and Science*, 2nd ed., Addison-Wesley, 2014.
4. Tom St. Denis, and Simon Johnson, *Cryptography for Developers*, Syngress, 2007. [Available via EBSCO eBooks, UPRM General Library Databases]

11. Course Outcomes

Upon completion of this course the student will be able to:	Program Student Outcomes Impacted
1. apply modern algebra and number theory to the understanding of cryptographic algorithms and vulnerabilities	a, b
2. understand and analyze modern encryption/decryption algorithms	a, b, l
3. understand and analyze digital signature, key exchange, and authentication protocols	a, b, l
4. understand and analyze secure layer protocols	a, b, l
5. analyze security attacks on cryptosystems	a, b, h, i, l
6. understand ethical, legal, and social issues related to security attacks and cryptographic applications	e, g, l
7. define, implement, and evaluate a cryptographic system	c, f, i, j, k

12. According to Law 51

Students will identify themselves with the Institution and the instructor of the course for purposes of assessment (exams) accommodations. For more information please call the Student with Disabilities Office which is part of the Dean of Students office (Office #4) at (787)265-3862 or (787)832-4040 extensions 3250 or 3258.

13. Academic Integrity

-The University of Puerto Rico promotes the highest standards of academic and scientific integrity. Article 6.2 of the UPR Students General Bylaws (Board of Trustees Certification 13, 2009-2010) states that academic dishonesty includes, but is not limited to: fraudulent actions; obtaining grades or academic degrees by false or fraudulent simulations; copying the whole or part of the academic work of another person; plagiarizing totally or partially the work of another person; copying all or part of another person answers to the questions of an oral or written exam by taking or getting someone else to take the exam on his/her behalf; as well as enabling and facilitating another person to perform the aforementioned behavior. Any of these behaviors will be subject to disciplinary action in accordance with the disciplinary procedure laid down in the UPR Students General Bylaws.–