

University of Puerto Rico
 Mayagüez Campus
 College of Engineering
 Department of Electrical and Computer Engineering
 Bachelor of Science in Computer Engineering

Course Syllabus

| | |
|---|----------------------|
| 1. General Information: | |
| Alpha-numeric codification: ICOM 5018 Course Title: Network Security and Cryptography Number of credits: 3 Contact Period: 3 hours of lecture per week Elective in ICOM | |
| 2. Course Description: | |
| English: Theoretical and practical aspects of Computer System and Network Security. Threat models and vulnerabilities of Computers Systems and Networks to attacks: hackers, malicious code, Trojan Horses, Viruses, and Worms. Methods and techniques to defend against attacks and minimize their damage. Cryptographic techniques, physical and operational security policies, and management related issues. | |
| Spanish: Aspectos teoricos y practicos de seguridad de Computacion y Redes. Modelos de amenazas a la Seguridad, descripcion y de cuan vulnerables son los sistemas de redes a ataques: Hackers,Codigo Malicioso, Caballos de Troya, Virus y "worms". Metodos y tecnicas para defender los sistemas de ataques y minimizar su potencial impacto. Tecnicas criptograficas, politicas operacionales de seguridad y temas relacionados sobre la administracion de sistemas. | |
| 3. Pre/Co-requisites and other requirements: | |
| Prerequisite ICOM5007, INEL4307 or equivalent experience | |
| 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: | |
| <input checked="" type="checkbox"/> conference <input type="checkbox"/> discussion <input checked="" type="checkbox"/> computation <input type="checkbox"/> laboratory <input checked="" type="checkbox"/> seminar with formal presentation <input type="checkbox"/> seminar without formal presentation <input type="checkbox"/> workshop <input type="checkbox"/> art workshop <input type="checkbox"/> practice <input type="checkbox"/> trip <input type="checkbox"/> thesis <input type="checkbox"/> special problems <input type="checkbox"/> tutoring <input type="checkbox"/> research <input type="checkbox"/> other, please specify: | |
| 6. Minimum or Required Resources Available: | |
| Students will use 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 (Suggested): The faculty member teaching the course will provide the student with the evaluation strategy he/she will be using throughout the semester. This will be done within the first week of classes.

| | Quantity | Percent |
|--|----------|---------------------|
| <input checked="" type="checkbox"/> Exams | 3 | 60% |
| <input checked="" type="checkbox"/> Final Exam | 1 | 20% |
| <input type="checkbox"/> Short Quizzes | | 0% |
| <input checked="" type="checkbox"/> Oral Reports | 3 | Included in project |
| <input type="checkbox"/> Monographs | | |
| <input type="checkbox"/> Portfolio | | |
| <input checked="" type="checkbox"/> Projects | | 20% |
| <input type="checkbox"/> Journals | | |
| <input type="checkbox"/> Other, specify: | | |
| TOTAL: | | 100% |

10. Bibliography:

William Stallings, Cryptography and Network Security, 4th Ed. Prentice Hall, 2005.

Niels Ferguson, Bruce Schneier, Practical Cryptography , John Wiley and Sons, 2003.

11. 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 (Chemistry Building, room 019) at (787)265-3862 or (787)832-4040 extensions 3250 or 3258.

12. Contribution of Course to meeting the requirements of Criterion 5:

| Math | Basic Science | General | Engineering Topic |
|------|---------------|---------|-------------------|
| | | | √ |

13. Course Outcomes

Map to Program Outcomes

- | | |
|--|-----|
| 1. Understand and contrast various symmetric algorithms | (a) |
| 2. Understand computational complexity aspects of cryptographic and cryptoanalytic methods | (a) |
| 3. Apply modern algebra and number theory to understanding of cryptographic algorithms and vulnerabilities | (a) |
| 4. Analyze attacks, such as person-in-the-middle, on cryptosystems | (b) |
| 5. Understand and analyze functionality and weaknesses of signature and authentication protocols | (b) |
| 6. Describe and analyze key exchange protocols | (a) |
| 7. Understand and analyze functionality and weaknesses of security layer protocols | (c) |
| 8. Relate hacking and intrusion techniques to OS and network characteristics | (a) |
| 9. Relate current legal and social issues to cryptographic applications and usage | (j) |
| 10. Define, implement and test a significant project relating to cryptography or its application | (e) |
| 11. Coordinate group accomplishment of the project | (d) |
| 12. Prepare and give oral and written project reports | (g) |

13.

Person (s) who prepared this description and date of preparation: Thomas Noack.
Submitted by: Manuel Rodríguez, March 2007