King Fahd University of Petroleum & Minerals

College of Computer Sciences and Engineering
Information and Computer Science Department

ICS 555: Data Security and Encryption (3-0-3)

Syllabus – Fall Semester 2009-2010 (091)

Website: Blackboard (WebCT) & http://faculty.kfupm.edu.sa/ICS/alfy/files/teaching/091-ics555/index.htm

Class Time, Venue and Instructor Information:

Sec.	Time	Venue	Instructor	Office Hours
01	SMW 8:00-9:15pm	22-119	**Dr. EL-SAYED EL-ALFY** Office: 22-108 Phone: 03-860-1930, E-mail: alfy@kfupm.edu.sa, http:faculty.kfupm.edu.sa/ics/alfy	SMW 11:00:11:59am SM 9:15-10:00pm Or by appointment

Course Catalog Description

Mathematical principles of cryptography and data security. A detailed study of conventional and modern cryptosystems. Zero knowledge protocols. Information theory, Number theory, complexity theory concepts and their applications to cryptography.

Pre-requisites: Consent of Instructor.
Recommended: ICS 353 or any course on principles of algorithms

Course Objectives

- Introduce students to the basic concepts of number theory and algorithms underlying cryptography and data security.
- Explore a variety of existing cryptosystems and develop problem-solving skills for cryptographic problems.

Course Learning Outcomes

Upon completion of the course, you should be able to:

1. understand basic concepts in number theory and apply modular arithmetic in problem solving
2. explain the setups, protocols, and security issues of some conventional and modern cryptosystems
3. design secure crypto-schemes to achieve simple tasks and explain their security issues.

Required Material

- B. A. Forouzan, Cryptography and Network Security, McGraw Hill 2007. (Available at the bookstore)
- W. Stallings, Cryptography and Network Security: Principles and Practice, (4th Edition, Prentice-Hall, 2006). 5th Edition is upcoming in Dec. 2009. The The book's online website contains numerous useful resources. URL: http://williamstallings.com/Crypto/Crypto4e.html (Available at KFUPM Library)
- Lecture notes and some pointed websites and papers

Other Recommended References

- S. Goldwasser and M. Bellare, Lecture Notes on Cryptography. MIT, 1996-2008 *
- M. Bellare & P. Rogaway, Introduction to Modern Cryptography, UCSD, 2005. *
- Christof Paar, Applied Cryptography and Data Security. Ruhr-Universitat Bochum, Germany, 2005. *
- D. Stinson, Cryptography: Theory and Practice, 3rd Edition, CRC Press, 2005.
- A. Menezes, P. Oorschot, & S. Vanstone, Handbook of Applied Cryptography, 2001. *
- N. Koblitz, A Course in Number Theory and Cryptography, 2nd edition, 1994. *
- N. Ferguson & B. Schneier, Practical Cryptography, John Wiley & Sons, 2003. (Based on Applied Cryptography: Protocols, Algorithms, and Source Code in C, by B. Schneier, 2nd Edition, John Wiley & Sons, 1996.)
- M. Welschenbach, Cryptography in C and C++, Apress, 2001.

  * softcopy is available online

Assessment Plan

Assessment Tool	**Weight**
Class work - attendance and class participation - in-class presentations and online discussions - homework assignments - quizzes - project - paper (optional)	40 %
Midterm Exam (Date: Nov. 16, Room: in-class)	25 %
Final Exam (Date and venue as announced by the registrar)	35 %

Tentative Major Topics

1. Introduction to Data Security and Cryptography
2. Basics of Number Theory and Algebraic Structures Related to Cryptography
3. Symmetric-Key Cryptography and Cryptosystems: Conventional and Modern Block and Stream Symmetric-Key Ciphers, DES, 3DES, AES
4. Public-Key Cryptography: RSA, Diffie-Hellman, Massey-Omura, Rabin, ElGamal
5. Message Integrity and Cryptographic Hash Functions
6. Digital Signature, Authentication and Key Management

Additional Course Policies

- ***Course Website***: Students are required to periodically check the course website and download course material as needed. Several resources will be posted through the website as well. Keys to quizzes and exams are generally discussed during class as time permits but solutions will not be posted. Blackboard CE 8 will be used for communication and interaction, posting and submitting assignments, posting grades, posting sample exams, etc.
- ***Class Attendance***: Regular attendance is a university requirement; hence attendance will be checked at the beginning of each class. Late arrivals will disrupt the class session. Hence, two late attendances (more than 10 minutes) will be considered as one absence. Missing more than 6 lectures will result in a DN grade without prior warning. To avoid being considered as absent, an official excuse must be shown no later than one week of returning to classes. Unexcused absences will also reduce your class work score unless acceptably justified. In case you have emergency and won't be able to attend, please let me know either by email or phone.
- ***Class Work and Participation:*** Students are expected to be active and positively engaged in the learning process. Get benefit of the discussion board by raising questions or answering those put by others. Also you can prepare and give a short presentation on a related tool or some interesting topic. Late submission of assigned work within the allowed period will be subject to penalty.
- ***No makeup of homework, quizzes or exams will be given.***
- ***Re-grading policy***: If you have a complaint about any of your grades, discuss it with the instructor no later than a week of distributing the grades (except for the final, an office hour will be announced in Blackboard after grading in which complains can be raised, if any). Only legitimate concerns on grading should be discussed.
- ***Term Project***: Each student is required to be exposed to research. A term project is a venue for demonstrating that. A student can select a topic, review it and write a survey report on related published material. He can choose to develop a cryptosystem and write a report, or he can analyze the security of an existing cryptosystem and report that. He can also design a cryptosystem, or an enhancement for an existing system. There could be other possibilities and ideas that you need to discuss first with the instructor. For example, it could be an application of using existing systems in designing a secure architecture for a real-world problem such as online shopping, banking, wireless communication, video encryption, etc.
- ***Academic honesty***: Students are expected to abide by all the university regulations on academic honesty. Cheating will be reported to the Department Chairman and will be severely penalized. Although collaboration and sharing knowledge is highly encouraged, copying others' work without proper citation, either in part or full, is considered plagiarism. Whenever in doubt, review the university guidelines or consult the instructor. Cheating in whatever form will result in F grade.
- ***Courtesy***: Students are expected to be courteous toward the instructor and their classmates throughout the duration of this course. Talking while someone else is speaking will not be tolerated. Furthermore, all cell phones must be turned off during class and exams. In addition, students are expected to be in class on time. To contact your instructor, please keep all communications, except in urgent matters, through Blackboard and avoid using phone calls, university emails or written notes. When sending an email through the university email system, please indicate 091-ICS555 in the "Subject" field of your email, e.g. 091-ICS555: Question about homework 1. Not following properly these guidelines may result in late or no response of your email.

⊙⊙⊙ **Best of luck!!** ⊙⊙⊙