

ICS 454 - Principles of Cryptography

Term: 171

Section: 01



INSTRUCTOR: Sultan Almuhammadi

OFFICE: 22-316

PHONE: 860-1625

E-MAIL: muhamadi (@ kfupm.edu.sa)

COURSE SITE: www.almuhammadi.com/sultanm/ics454 (see also Blackboard)

DESCRIPTION

Classical cryptography; Secret Key Encryption; Perfect Secrecy. Cryptanalysis; Block and Stream cipher; Data Encryption Standard (DES) and Advanced Encryption Standard (AES); Public Key Encryption; Diffie-Hellman Key Exchange; RSA, ElGamal and Rabin's Cryptosystems; Authentication and Digital Signatures; One-time signatures; Randomized Encryption; Rabin and ElGamal signature schemes; Digital Signature Standard (DSS)' Cryptographically Secure Hashing; Message Authentication Codes; Network Security; Secure Socket Layer (SSL); IPsec.

PREREQUISITES ICS 254 and ICS 353.

COURSE OBJECTIVES

1. To study the basic number theory concepts and integer algorithms related to cryptography.
2. To study variety of existing cryptosystems and their cryptanalysis.
3. To develop problem-solving skills for cryptographic applications.

COURSE LEARNING OUTCOMES

After completion of this course, the student should be able to:

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

TEXTBOOK

B. Forouzan, Cryptography and Network Security, 2008.

CONTENTS

The following list is tentative and subjected to changes. Any change will be announced in the course website/Blackboard.

- Classical cryptography, Secret Key Encryption
- Integer Algorithms, Modular Arithmetic and Linear Congruence.
- Cryptanalysis, Perfect Secrecy
- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)
- Algebraic Structures, Group Theory
- Public Key Encryption: RSA, Diffie-Hellman, ElGamal and Rabin's Cryptosystems
- Authentication, Digital Signatures, and Digital Signature Standard (DSS)
- Cryptographically Secure Hashing

EVALUATION

Coursework	25%
Major Exam I	20%
Major Exam II	25%
Final Exam (comprehensive)	30%

Course Policies

- **Coursework includes** participation, online/in-class discussions and activities, attendance, homework assignments, and quizzes. Active learning is implemented in this class. Students are expected to be positively engaged in the learning process.
- **Course Website & Participation:** 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.
 - [Blackboard](#) will be used for communication and interaction, posting and submitting assignments, posting grades, posting sample exams, etc.
 - It is expected that you get benefit of the discussion board by raising questions or answering questions put by others.
- **Attendance:** Regular attendance is a university requirement.
 - Attendance will be checked at each lecture.
 - Missing 20% of the classes will result in an automatic DN grade (without warning).
 - Late arrivals will disrupt the class session, and may be counted as a miss if repeated.
 - If you find yourself unable to attend a class, email the instructor ahead of time for better planning and management of the class. If you fail to do so, send your email as soon as you get a chance and provide your excuses if any.
 - Every unexcused absence may lead to a loss of 0.5% of total grade.
- **Late assignments:** are subjected to late-penalty. See late submission policy on the course website/ Blackboard under the Assignments page.
- **Re-grading policy:** If you have a complaint about any of your grades, discuss it with the instructor no later than 3 days of distributing the grades (except for the final). Only legitimate concerns on grading should be discussed.
- **Office Hours:**
 - Students are encouraged to use the office hours to clarify any part of the material that is not clear. Use the Blackboard (Bb) for quick points and homework questions.
 - For urgent issues, use emails instead of Bb-mails, please indicate ICS454 in the "Subject" field of your email (e.g. ICS454: Quiz1 score is missing).
- **Academic honesty:**
 - Students are expected to abide by all the university regulations on academic honesty.
 - Cheating will be reported to the Department Chairman.
 - 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.
- **Courtesy:**
 - Students are expected to be courteous toward their classmates and the instructor throughout the duration of this course (in-class and online).
 - Side-talks and text-messages during the class are prohibited.