ICS 439 – Cryptography in Quantum Era

Term: 202

Section: 01

INSTRUCTOR: Sultan Almuhammadi
OFFICE: 22-316
PHONE: 860-1625
E-MAIL: muhamadi (@ kfupm.edu.sa)
COURSE SITE: www.almuhammadi.com/sultanm/ics439 (see also Blackboard)

DESCRIPTION

The difference between quantum cryptography and existing conventional cryptography, Integer Algorithms, Modular Arithmetic , Symmetric-key Cryptography, Perfect Secrecy, Stream and Block cipher, Group Theory, Public Key Cryptography, Quantum cryptography and cryptanalysis, Key distribution protocols, Quantum money, quantum one-time pad.

PREREQUISITES

COE 466.

COURSE OBJECTIVES

- To provide basic concepts of modern cryptography
- To explain the impact of quantum computers on modern cryptography
- To introduce quantum cryptographic tools and protocols, and their cryptanalysis

COURSE LEARNING OUTCOMES

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

1. Identify the difference between conventional and quantum cryptography protocols.
2. Apply basic number theory concepts in modern cryptography.
3. Describe the setups and the security issues of some existing cryptosystems.
4. Explain basic concepts in quantum information security and their applications.
5. Describe cryptanalysis techniques using quantum machines.

CONTENTS

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

1. An overview on modern cryptography and quantum cryptography (1 week)
2. Integer Algorithms, Modular Arithmetic and Linear Congruence. (2 weeks)
3. Symmetric- key cryptography, Perfect Secrecy, Stream and Block cipher (1 week)
4. Introduction to Group Theory (2 weeks)
5. Public Key Encryption: RSA, Diffie-Hellman Protocol, ElGamal Cryptosystem (1 week)
6. Quantum machines and cryptanalysis (2 weeks)
7. Quantum information security (2 weeks)
8. Key distribution protocols (2 week)
9. Quantum money, the quantum one-time pad (1 week)
10. Commitment scheme and coin-flipping (1 week, if time permits)

TEXTBOOKS AND REFERENCES

1. B. Forouzan, Cryptography and Network Security, 2015
2. N. Yanofsky, M. Mannucci, Quantum Computing for Computer Scienctists, 2008
3. W. Stallings, “Cryptography and Network Security,” 7Th Edition, 2018

EVALUATION

Coursework:	40%
Midterm Exam	25%
Final Exam (comprehensive)	35%

Course Policies

- ***Coursework includes*** participation, online/in-class discussions and activities, attendance, homework assignments, quizzes, and projects. 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 (on MS Teams) to clarify any part of the material that is not clear. Use the Blackboard/MS Teams for quick points and homework questions.
  - For urgent issues, use emails (or MS Teams), please indicate ICS439 in the "Subject" field of your email (e.g. ICS439: 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.