

# ICS 562 – Quantum Cryptography

Term: 231

Section: 01



**INSTRUCTOR:** Sultan Almuhammadi  
**OFFICE:** 22-316  
**PHONE:** 860-1625  
**E-MAIL:** sultan (@ almuhammadi.com)  
**COURSE SITE:** [www.almuhammadi.com/sultanm/ics561](http://www.almuhammadi.com/sultanm/ics561) (see also Blackboard)

## DESCRIPTION

Review on Number Theory, Symmetric-key cryptography, Shannon Theory, Commitment scheme and coin-flipping, Public Key Encryption: RSA, Diffie-Hellman Protocol, ElGamal Cryptosystem, Quantum information processing, Quantum cryptanalysis, Post-quantum cryptography, Quantum money, the quantum one-time pad, Key distribution protocols.

**PREREQUISITES** ICS 561 and Math 570.

## COURSE OBJECTIVES

1. To provide the students with foundational principles of modern cryptosystems.
2. To introduce advanced concepts, tools and protocols used in quantum cryptography.

## COURSE LEARNING OUTCOMES

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

1. Describe the setups and the security issues of some existing cryptosystems.
2. Explain foundational concepts in quantum information security and their applications.
3. Apply number theory concepts in modern and quantum cryptography.
4. Apply advanced cryptanalysis techniques using quantum computers.
5. Design and analyze a cryptoscheme that achieves some security requirements.
6. Search and utilize information on conventional and quantum algorithms from a variety of sources.

## CONTENTS

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

1. Introduction to cryptography and cybersecurity	1 week
2. Number theory, Modular arithmetic	2 weeks
3. Symmetric-key Cryptography, Block ciphers, DES, AES	2 weeks
4. Public Key Encryption: RSA, Diffie-Hellman protocol, ElGamal cryptosystem	1 week
5. Hash functions, Digital signatures	1 week
6. Quantum information processing, Quantum cryptanalysis	2 weeks
7. Quantum key distribution protocols	2 weeks
8. Post-quantum cryptography	2 weeks
9. Quantum money, Quantum one-time pad	1 week

## TEXTBOOKS

1. B. Forouzan, Cryptography and Network Security, 2015
2. N. Yanofsky, M. Mannucci, Quantum Computing for Computer Scientists, 2008

## REFERENCES

1. W. Stallings, "Cryptography and Network Security," 7th Edition, 2018
2. M. Nielsen and I. Chuang, Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge: Cambridge University Press, 2010.

## EVALUATION

Coursework:	30%
Project	20%
Midterm Exam	20%
Final Exam (comprehensive)	30%

## 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 ICS562 in the "Subject" field of your email (e.g. ICS562: 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.