ICS 440 –
Cryptography and Blockchain Applications

Term: 201

Section: 01

INSTRUCTOR: Sultan Almuhammadi
OFFICE: 22-316
PHONE: 860-1625
E-MAIL: muhamadi (@ kfupm.edu.sa)
COURSE SITE: www.almuhammadi.com/sultanm/ics440 (see also Blackboard)

DESCRIPTION

Secret key encryption; Block and stream ciphers, Encryption standards; Number theory: Divisibility, Modular arithmetic, Group theory and Finite fields; Public key encryption: RSA, ElGamal and Rabin cryptosystems; Diffie-Hellman key exchange; Cryptographically secure hashing; Authentication and digital signatures; Digital signature standard (DSS), Randomized encryption; Cryptocurrency, Blockchain models and applications. Security issues and their solutions in Blockchain models and applications. Blockchain payment networks.

PREREQUISITES Math 208 and Stat 319.

COURSE OBJECTIVES

- To provide a practical introduction to the cryptography field
- To introduce students to cryptographic algorithms and their applications such as Blockchain

COURSE LEARNING OUTCOMES

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

1. Describe the mathematical background behind cryptosystems.
2. Explain the setups, the protocols, and the security issues of some existing cryptosystems.
3. Design a simple crypto scheme for a given security goal.
4. Utilize cryptographic algorithms implementations to secure systems.

CONTENTS

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

1. Divisibility, Modular arithmetic, Prime numbers, Euclidean algorithm, Linear congruence, Chinese remainder theorem)	2 weeks
2. Introduction to cryptography, Secret key encryption, Ideal block cipher, Data Encryption Standard (DES), Advanced Encryption Standard (AES)	1 week
3. Group Theory: Cyclic groups, Permutation groups; Finite fields	2 weeks
4. Public-key encryption: RSA, ElGamal cryptosystems; Diffie-Hellman key-exchange scheme	1.5 weeks
5. Quadratic residues, Rabin's Cryptosystem	1.5 weeks
6. Cryptographically secure hashing, Authentication, Digital signatures, and Digital Signature Standard (DSS), Randomized encryption, One-time and ring signatures	2 weeks
7. Blockchains: Blockchain characteristics, Cryptocurrencies, Smart contracts	2 weeks
8. Blockchain implementations, Blockchain models, Proof-of-work alternatives, Tangle and Hash graph	1 week
9. Blockchain Business models	1 week
10. Blockchain Security and their countermeasures	1 week

TEXTBOOK

W. Stallings, "Cryptography and Network Security," 7Th Edition, 2018

REFERENCES

1. A. Banafa, "Blockchain Technology and Applications," River Publishers, 2020.
2. B. Forouzan, Cryptography and Network Security, 2008.
3. B. Schneier, "Applied Cryptography: Protocols, Algorithms and Source Code in C," 20th Anniversary Edition, Wiley, 2015.
4. Bitcoin and Blockchain: The Ultimate Guide to Discover Blockchain, Investing, Mining and Cryptocurrencies like Bitcoin, Ethereum, Litecoin, Ripple and All Altcoins by Brian Lain, 2020.

EVALUATION

Coursework:	30%
Major Exam I	20%
Major Exam II	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 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.