This Week

Overview Lecture

Subject Overview

Lecture 1

Introduction to cr

Lecture 2

Introduction to Numbers

Workshops start from Week 2

Quiz 1

Overview

Instructors and Tutors

Instructors

- Udaya Parampalli, Udaya@unimelb.edu.au
- Joseph Bonneau, joseph.bonneau@unimelb.edu.au

Tutors

- William Troiani, william.a.troiani@gm tutor)
- Ms Wenjun Zhou(aarenzhou81@gmail.com)
- Mr Guang Hu(ghu1@student.unimelb.edu.au)
- Dr Omar Al-Boridi(omarnori81@gmail.com)

A little bit of myself

- Udaya Parampalli,
  - Professor and Reader, Leader-Quantum Computing Research, School of Computing and Information Systems
- Research Interests:
  - Quantum comput hy
  - Steganography or
  - Cryptography for Networks and Com
  - Sequence design for Radar and Comm
  - Coding theory for Storage and DNA
- Publications:
  - http://people.eng.unimelb.edu.au/udaya/

How to contact me?

- Preferably at the end of lectures
- Email: udaya@unimelb.edu.au (Include the word COMP90043 in subject field)
- Expect 48 hours turn around on occasions!
- Level 2, Melbourne
- Consultation: Time nd also by appointment.

Subject Structure

- 12 Weeks of Lectures
  - 2 lectures (maximum of 3 hours per week) + 1 hour of tutorial (in parallel sessions)
- Assessment:
  - 40% Final exami
  - 2 Hour Final exa
  - Mid-Semester Test (10%)[Tentative d
- 50% Project/Assignment
  - 2 Assignments (7.5% each individual work)
    - Weekly Quiz
    - 2 bonus marks for completing 8 out of 10 quizzes (80%).
  - 1 Research project (35% Total) a group project-details will be released soon)
    - Part A: Presentation in Week 10 (10%)
    - Part B: Research Report due in Week 12 (25%)

Bonus applies to the Assignment component not exceeding max cap of 15

Research Project

- Group Project, group size of maximum 3, we would prefer groups of 3 people.
- Project should be based on a topic that involves Cryptography.
  - A list if suggested topics will be available.
  - You should organize your groups preferably with members from same tutorial group
  - Your tutor will be the first point of contact for any discussion on the project
- You need to choose a esearch project. The proposal should detail st group members.
- The Body of the work:
  - Implementations:
  - Problem Identification
  - Analysis
  - Conclusion
- Marks breakdown:
  - Part A: Presentation in Week 10 or 11 (10%)
  - Part B: Research Report (25%) due in Week 12

Hurdle Requirements

- To pass the subject, students must obtain at least:
  - 50% overall.
  - 50% in the homework assignments
    - Note that b quizzes you can earn 2 bonus mark
- 50% in the research project
- 50% in the end-of-semester written examination
- No hurdle for the mid-semester test component

Intended Learning Outcomes (ILO)

- ILO1: Identify security issues and objectives in computer systems and networks.
- ILO2: Apply various security mechanisms derived from cryptography to computers and computer networks.
- ILO3: Explain the c key and symmetric key cryptographic algo l, Diffie-Hellman schemes and strea
- ILO4: Explain the protocols which en n contemporary networked computer systems.
- ILO5: Describe the interaction between the underlying theory and working computer security infrastructure.
- ILO6: Analyze security of network protocols and systems.

Lecture Times

COMP90043: Cryptography and Security

- Two lectures per week, total time maximum of 3 hours*.
  - Monday 15:15 to 17:15, Delivered through LMS
  - Thursday, 17:1 gh LMS

- Note that in the subject you are ex k on programs on departmental servers. There will no ial laboratory workshops. You will need to work yourselves. We will provide consultations.

- We may have some guest lectures and revisions in some lectures. The contents in some of these guest lectures are examinable

Subject Resources

- Textbook: Cryptography and Network Security: Principles and Practice, 7/E by William Stallings

References:

- Douglas R Stinson, Cryptography, Theory and Practice, Chapman & Hall/CRC, 2006.
- Richard E. Smith, I Y, ADDISON WESLEY, 1997.

- Andrew S. Tanenbaumm , COMPUTE S, Fourth Edition, Prentice-Hall lnternational, Inc. 2003.

- Alfred J. Menezes, Paul C. van Oorsch . Vanstone, Handbook of Applied Cryptography, CRC Press, October 1996.
- Wenbo Mao, ``Modern cryptography Theory and Practice",www.hp.com/hpbooks, Pearson Education, Prentice Hall, 2004.
- Articles from Lecture Notes in Computer Science series covering security and cryptography

Subject Outline

- This subject covers fundamental concepts in information security on the basis of methods from modern cryptography. We will concentrate on topics which are of current interest as well as the more `classic' topics which underlay this discipline.

Topics drawn from:

- symmetric key an
- hash functions,

- authentication
- secret sharing
- Protocols
- Key Management

There will be some guest lectures in specialized topics.

Subject Description

The objective of this subject is for students

- to understand the fundamentals of security principles in modern networks and computer systems,
- to be able to explai curity in contemporary networked computer systems;
- to study various cryptographic primitives like encryption, hashing and signature functions which are used in theory and practice of network security.

Course Plan (Dates to be Confirmed)

Topics by week:

- 1. Introduction to Cryptography and Security (Ch 1), Introduction to Numbers,
- 2. Symmetric Ciphers, Classical Ciphers,. (Group Formation) (Assignment 1 handed out)
- 3. Modern Symmetric Ciphers: Block and Stream Ciphers (Ch 2,3,6,7)
- 4. Basics from Numb
- 4. Public Key Crypto nt 1 due)
- 5. Hash functions (Ch Assignment 2 handed out)
- 6. Message Authentication Codes (Ch 12)
- 7. Digital Signatures (Ch 13) (Mid Semeste ent 2 due)
- 8. Key management,
- 9. Key management cont., Secret Sharing (Ch 14)
- 10. Guest Lecture/Project Presentations
- 11. Application/Advanced Topics (Part 5)
- 12. Review, Report Due

Generic Skills

- GS1: Ability to undertake problem identification, formulation, and solution.
- GS2: Ability to utilise a systems approach to solving complex problems and to design for operational performance
- GS3: Ability to ma tation
- GS4: Capacity for creativity and innov
- GS5: Ability to communicate effectively, with the engineering team and with the community at large

Academic Standards

From your canvas home page access **Academic integrity module**

- https://catalog.lms.unimelb.edu.au/browse/communities/student-induction/

- Even if you have e, you should listen to the talks and com again. This will take less than 15 minutes. The experien ou to realize the importance of academic honesty w y progress in your studies.