澳門理工大學
Universidade Politécnica de Macau
Macao Polytechnic University

COMP412: Computer Security

Course Introduction

Dr. Kim, Song-Kyoo (Amang)
Associate Professor,

Computer Science Program
MACAO POLYTECHNIC UNIVERSITY
Macau, SAR

Module Descriptions

- This module explains the theoretical foundations, and current state, of modern cryptographic algorithms and trusted computers used to provide various computer security services.
- Cryptographic encryption algorithms, including DES, RSA, and Diffie-Hellman, are discussed.
- Additional topics are classical ciphers, modern private key block ciphers, public key ciphers, authentication and integrity, key management and modern application systems.

Module Outline (1/2)

- Introduction to Cryptography
  - Services, Mechanisms and Attacks
  - Network Security Models
  - Classical Ciphers
- Modern Block Ciphers
  - SDES, DES, Double DES and Triple DES
- Public Key Cryptography Algorithms
  - Modulo Arithmetic and related theorems
  - Public Key Theorem
  - RSA and its security
  - Diffie-Hellman Key Exchange

Module Outline (2/2)

- Authentication (Ch. 11-13)
  - Hash Functions
  - Message Authentication Code
  - Digital Signature
- Key Management (Ch. 14)
  - X.509 Certificate
  - Secure Socket Layer
- Network Security Applications (Ch. 18- 20)
  - Pretty Good Privacy
  - Wireless Security
  - IP Security

Grading System (1/2)

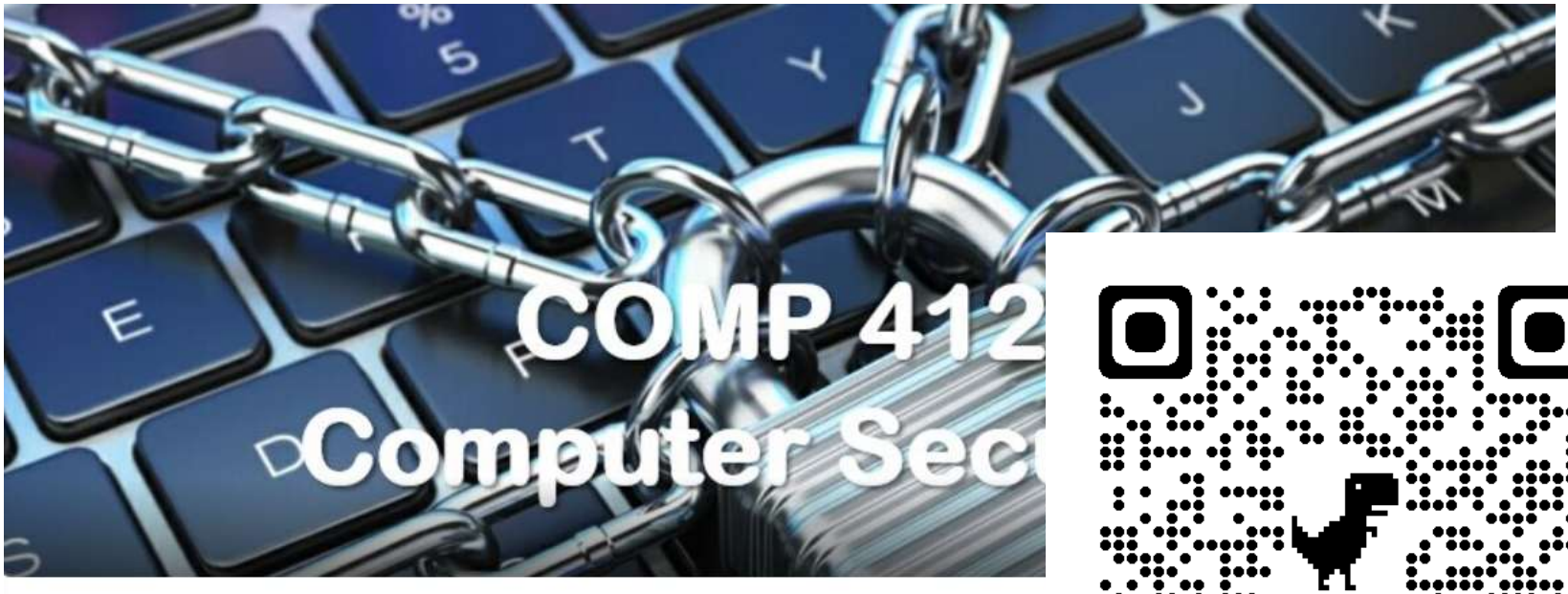
- **Popup Quiz …… 5 %**
  - (Almost) every session will have a quiz.
  - Based on the previous session.
- **Take-home assignments …… 20 %**
  - 2 Literature (research) review.
- **Test (Mid-term exam) …… 25 %**
- **Exams (Final)…… 50 %**

Grading System (2/2)

- Popup Quiz
  - Couple of questions that students have leant on the last session.
- Take-home assignments
  - 2 Research papers – Literature review (freely selected)
  - 10 % per each assignment
  - The forms will be provided.
- 2 Exams
  - Mid term exam (test) – 25 %
  - Final exam – 50 %
    - Following the MPU regulations.

Student Conduct

- Facebook Pages:
  - https://www.facebook.com/amang.mpi.7
  - https://www.facebook.com/groups/732227351335968



COMP412-202223-1st

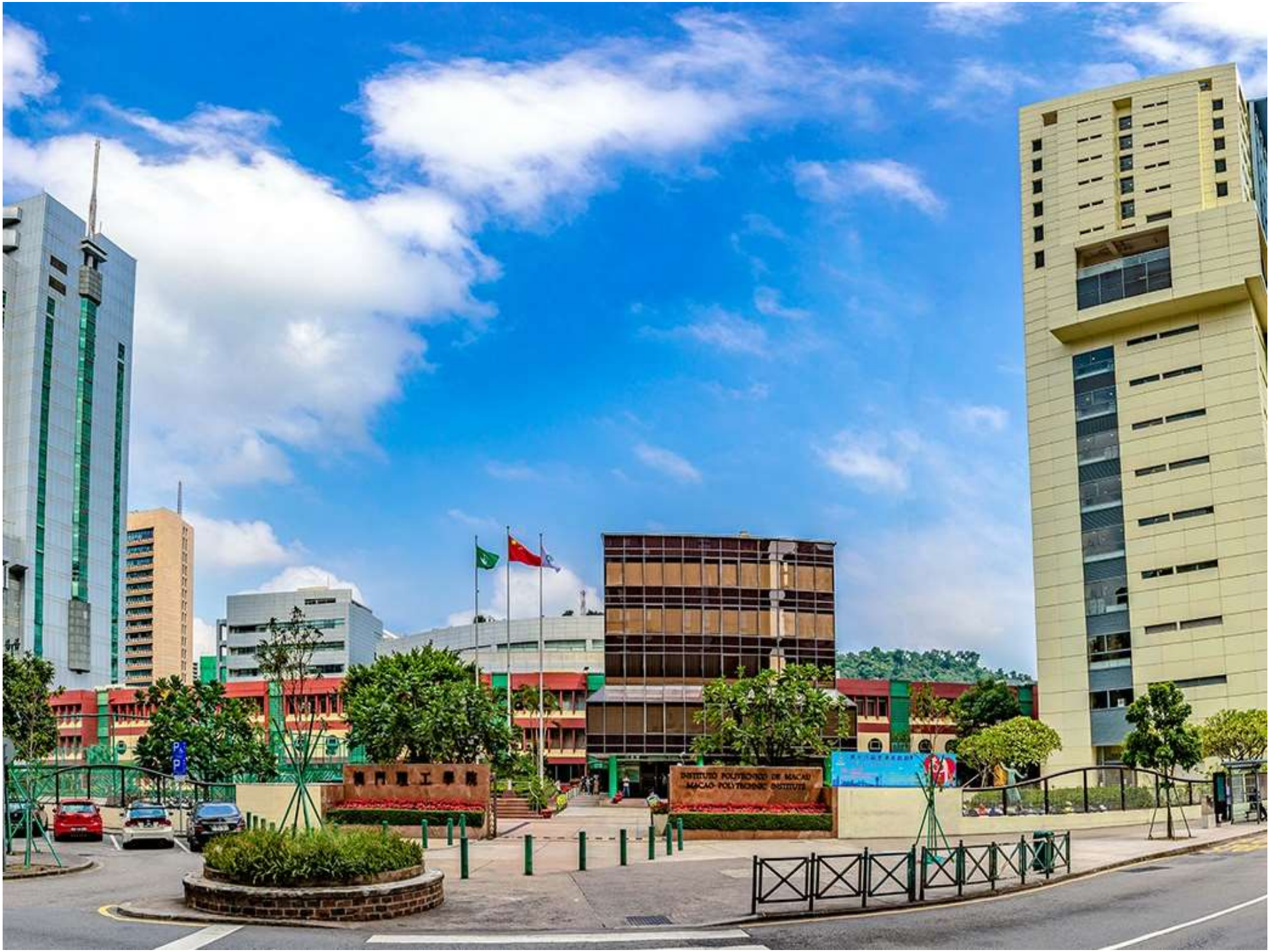
Private group · 1 member

Student Conduct (2/2)

- Canvas:
  - Sec-1 (411): https://canvas.mpu.edu.mo/courses/1449
  - Sec-2 (412): https://canvas.mpu.edu.mo/courses/1320

Section-1 (411)

Section-2 (412)


澳門理工學院
INSTITUTO POLITÉCNICO DE MACAU
MACAO POLYTECHNIC INSTITUTE