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

FACULTY OF APPLIED SCIENCES
BACHELOR OF SCIENCE IN COMPUTING
LEARNING MODULE OUTLINE

Academic Year	2023/2024	Semester	1
Module Code	COMP412		
Learning Module	Computer Security		
Pre-requisite(s)	Nil		
Medium of Instruction	English		
Credits	3	Contact Hours	45 hrs
Instructor	Dr. Amang Kim	Email	amang@mpu.edu.mo
Office	A320 Chi Un Building	Office Phone	8599.6455

MODULE DESCRIPTION

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 INTENDED LEARNING OUTCOMES (ILOS)

On completion of this learning module, students will be able to:

M1.	Analyze threats in distributed computer systems and design the methods of providing protection; (SM1p)
M2.	Utilize the main cryptographic primitives for encryption and authentication; (EA1p, EA4p, D1p)
M3.	Contrast the conventional and modern cryptographic techniques; (SM1p, EA1p)
M4.	Justify the role of key management systems; (SM1p)
M5.	Analyze main types of security protocols and security needs of scenarios; (EA4p, ET4p, EP1p)
M6.	Design security services based on user needs in uncertainty. (D1p, ET4p, EP1p, EP8p)

These ILOs aims to enable students to attain the following Programme Intended Learning Outcomes (PILOs):

PILOs	M1	M2	M3	M4	M5	M6
P1. Select and apply proven methods, tools and techniques to the effective and efficient implementation of information systems;	✓					
P2. Evaluate computer systems in a local area network, and understand the additional requirements for connection to other					✓	

networks through wide area networks;						
P3. Be competent in system development in the Internet and the web platform;						
P4. Work independently to design and implement a relational database, with an emphasis on how to organise, maintain and retrieve information from a DBMS;						✓
P5. Acquire essential knowledge in specific fields of computing disciplines including multimedia, security and artificial intelligence;		✓				
P6. Acquire the perceptive skills needed to understand information presented in the form of UML diagram, flow chart or other industry standard formats;						
P7. Understand the need for and use of the necessary mathematical techniques;	✓					
P8. Work independently to develop an understanding of, and the knowledge and skills associated with the general support of computer systems and networks;		✓				
P9. Work as an effective member of a team in the analysis, design and development of software systems;						
P10. Use project planning and management techniques in systems development;						
P11. Understand the fundamental and operational issues of computer systems in business environments;			✓			
P12. Equip with adequate written, oral communication and interpersonal skills;						
P13. Build the capacity and desire for lifelong learning and to learn advanced and emerging technologies on one's own;				✓		
P14. (For Enterprise Information Systems specialisation) Gain an in-depth understanding of the information technology related to enterprise information systems, with an emphasis on development of such systems to support business processes;						
P15. (For Gaming Technology specialisation) Acquire the general and advanced knowledge of current technologies and operating environment in the gaming industry;						
P16. (For Computer Education specialization) Acquire the general and practical knowledge of computer education and its practicing environment in secondary education.						

MODULE SCHEDULE, COVERAGE AND STUDY LOAD

Week	Content Coverage	Contact Hours
1-2	1. Introduction to Cryptography	6
	1.1. Services, Mechanisms and Attacks	
	1.2. Network Security Models	
	1.3. Classical Ciphers	
3-4	2. Modern Block Ciphers	6

	2.1. SDES, DES, Double DES and Triple DES	
5-8	3. Public Key Cryptography Algorithms	12
	3.1. Modulo Arithmetic and related theorems	
	3.2. Public Key Theorem	
	3.3. RSA and its security	
	3.4. Diffie-Hellman Key Exchange	
9-11	4. Authentication	9
	4.1. Hash Functions	
	4.2. Message Authentication Code	
	4.3. Digital Signature	
12-13	5. Key Management	5
	5.1. X.509 Certificate	
	5.2. Secure Socket Layer	
13-15	6. Network Security Applications	6
	6.1. Availability and Disaster Recovery	
	6.2. Pretty Good Privacy	
	6.3. Wireless Security	
	6.4. IP Security	
	6.5. Software Security	
15	7. Cyber-Security and Government	1
	7.1. Macao Network Security Law	

TEACHING AND LEARNING ACTIVITIES

In this learning module, students will work towards attaining the ILOs through the following teaching and learning activities:

Teaching and Learning Activities	M1	M2	M3	M4	M5	M6
T1. Class teaching and lecture	✓	✓	✓			✓
T2. Literature review				✓	✓	
T3. Test	✓	✓	✓	✓		✓

ATTENDANCE

Attendance requirements are governed by the Academic Regulations Governing Bachelor's Degree Programmes of the Macao Polytechnic University. Students who do not meet the attendance requirements for the learning module shall be awarded an 'F' grade.

ASSESSMENT

In this learning module, students are required to complete the following assessment activities:

Assessment Activities	Weighting (%)	AHEP3 LOs	ILOs to be Assessed
A1. Popup quiz	5%	EP1p	P1, P2, P11
A2. Assignments	20%	D1p, ET4p, EP8p	P7, P8, P11
A3. Test	25%	SM1p, EA1p, EA4p	P1, P2, P4, P5
A4. Exam	50%	SM1p, EA1p, EA4p	P1, P2, P4, P5, P13

The assessment will be conducted following the University's Assessment Strategy (see www.mpu.edu.mo/teaching_learning/en/assessment_strategy.php). Passing this learning module indicates that students will have attained the ILOs of this learning module and thus acquired its credits.

Students with an overall score of less than 35 in the coursework must take the re-sit examination even if the overall score for the module is 50 or above.

Students with a score of less than 35 in the final examination must take the re-sit examination even if the overall score for the module is 50 or above.

Students with an overall final grade of less than 35 are NOT allowed to take the re-sit examination.

REQUIRED READINGS

1. Stallings, W. (2017). Cryptography and Network Security (7th ed.). New Jersey: Pearson.

REFERENCES

1. Stallings, W. (2006). Network Security Essentials, Applications and Standards (3rd ed.). New Jersey: Prentice Hall.
2. Trappe, W. and Washington, L. (2005). Introduction to cryptography with coding theory (2nd ed.). New Jersey: Prentice Hall.

STUDENT FEEDBACK

At the end of every semester, students are invited to provide feedback on the learning module and the teaching arrangement through questionnaires. Your feedback is valuable for instructors to enhance the module and its delivery for future students. The instructor and programme coordinators will consider all feedback and respond with actions formally in the annual programme review.

ACADEMIC INTEGRITY

The Macao Polytechnic University requires students to have full commitment to academic integrity when engaging in research and academic activities. Violations of academic integrity, which include but are not limited to plagiarism, collusion, fabrication or falsification, repeated use of assignments and cheating in examinations, are considered as serious academic offenses and may lead to disciplinary actions. Students should read the relevant regulations and guidelines in the Student Handbook which is distributed upon the admission into the University, a copy of which can also be found at www.mpu.edu.mo/student_handbook/.