Title (Units): **COMP4017 Computer and Network Security (3,3,0)**

Course Aims: To introduce the fundamental concepts and techniques in computer and network security, including basic encryption techniques, cryptographic algorithms, authentication and digital signature, public key infrastructure, security models, network security, as well as their applications (e.g., IP security, Web security, trusted operating systems). Popular cryptographic standards and libraries will be introduced. Other advanced topics in computer security will also be discussed (e.g., intrusion detection, access control, secure programming, computer virus).

Prerequisite: COMP2015 Data Structure and Algorithm
COMP3015 Data Communications and Networking

Course Intended Learning Outcomes (CILOs):
Upon successful completion of this course, students should be able to:

No.	Course Intended Learning Outcomes (CILOs)
	Knowledge
1	Describe fundamental concepts of computer security
2	Explain the basic concepts of symmetric, asymmetric cryptography & various digital signature schemes
3	Identify security weaknesses in different networking environments
	Professional Skill
4	Identify the appropriate cryptographic scheme & security mechanism for different computing environments and information systems
5	Analyze the security of different computer systems & networks
	Attitude
6	Critically evaluate the security of computer systems

Calendar Description: This course introduces fundamental concepts and techniques in computer and network security. Topics include basic encryption techniques, cryptographic algorithms, authentication and digital signature, public key infrastructure, security models, network security, as well as their applications (e.g., IP security, Web security, trusted operating systems). Popular cryptographic standards and libraries will be introduced. Other advanced topics in computer security will also be discussed (e.g., intrusion detection, access control, secure programming, computer virus).

Teaching and Learning Activities (TLAs):

CILOs	Type of TLA
1 - 6	Lectures. Students will be shown the fundamental concepts of computer and network security, their relevant mathematic theories, and examples of computer systems
2, 4, 6	Computational exercises. Students will perform different encryption algorithms and investigate various cryptographic techniques by performing some exercises.
3, 5, 6	Programming exercises. Students will read the source code and implement some software to analyze the security of different computer systems and networks and to exploit the security weakness of some computer systems.

Assessment:

No.	Assessment Methods	Weighting	CILOs to be addressed	Description of Assessment Tasks
1	Continuous Assessment	30%	1-6	Continuous assessments are designed to measure how well the students have learned the material. Projects and/or assignments are designed to give students hands-on experience in the subject matter.
2	Examination	70%	1-5	Final examination questions are designed to evaluate students' understanding of the course

				material, and how far students have achieved the intended learning outcomes. Questions will primarily be analysis and skills based to assess the students’ ability to analyze the security of different computer systems.

Assessment Rubrics:

Excellent (A)	• Achieve the six CILOs, demonstrating a good mastery of both the theoretical and practical aspects of computer security • Have a solid understanding of computer security fundamental concepts, and be able to explain and highlight the key points of these concepts • Able to conduct security analysis on computer systems, and possibly highlighting security vulnerabilities with detailed explanation and proper reasoning • Able to recommend suitable cryptographic technologies and security mechanisms to different situations and computing environments, and be able to design and develop, with competence, high quality computer security systems using these technologies
Good (B)	• Achieve the six CILOs, demonstrating a good understanding of both the theoretical and practical aspects of computer security • Have a good understanding of computer security fundamental concepts • Able to conduct security analysis on computer systems with sound reasoning • Able to apply cryptographic technologies and security mechanisms to different situations and computing environments, and be able to design and develop computer security systems using these technologies
Satisfactory (C)	• Achieve most of the six CILOs, demonstrating a basic level of understanding of the theoretical and practical aspects of computer security • Have a basic understanding of computer security fundamental concepts • Able to conduct a basic security analysis on most computer systems • Demonstrate an adequate level of ability of applying cryptographic technologies and security mechanisms to different situations and computing environments
Marginal Pass (D)	• Achieve most of the six CILOs, with a minimal level of understanding of the theoretical and practical aspects of computer security • Have a minimal level of understanding of computer security fundamental concepts • Ability to conduct security analysis on computer systems under a limited number of typical situations • Ability to apply some of the cryptographic technologies and security mechanisms to a limited number of computing environments
Fail (F)	• Achieve less than three of the CILOs, and have little understanding of the theoretical and practical aspects of computer security • Unable to provide solutions to simple problems which require basic understanding of computer security fundamental concepts • Unable to conduct security analysis on computer systems • Have little understanding of cryptographic technologies and security mechanisms and have difficulty in applying these technologies to computing environments

Course Content and CILOs Mapping:

Content		**CILO No.**
I	Overview	1, 3, 6
II	Basic Encryption Techniques	1, 2, 3, 6

III	Secret-Key Cryptography	1, 2, 3, 4, 6
IV	Public-Key (Asymmetric) Cryptography	1, 2, 3, 4, 6
V	Message Authentication and Digital Signature	1, 2, 3, 4, 6
VI	Network Security Practice	1, 3, 5, 6

References:

- William Stallings, Computer Security: Principles and Practice, 3rd Edition, Prentice Hall, 2014.
- William Stallings, Cryptography and Network Security: Principles and Practice, 7th Edition, Pearson, 2016
- Behrouz A. Forouzan, Introduction to Cryptography and Network Security, McGraw Hill, 2008.
- Eric Maiwald, Network Security – A Beginner′ s Guide, 2nd Edition, McGraw Hill, 2003.
- Charles P. Pfleeger, Shari Lawrence Pfleeger, Security in Computing, 4th Edition, Prentice Hall, 2007.
- Nestler, Conklin, White, and Hirsch, Computer Security Lab Manual, McGraw-Hill Irwin, 2006.
- Atul Hahate, Cryptography and Network Security, McGraw Hill, 2003.
- B. Schneier, Applied Cryptography, 2nd Edition, John Wiley & Sons, 1996.
- Niels Ferguson, Bruce Schneier, Cryptography Engineering: Design Principles and Practical Applications, Wiley, 2010.
- J. Pieprzyk, T. Hardjono, and J. Seberry, Fundamentals of Computer Security, Springer, 2003.

Course Content:

Topic

I. Overview

II. Basic Encryption Techniques
   A. Substitution
   B. Transposition
   C. Steganography

III. Secret-Key Cryptography
   A. Block cipher
   B. Stream cipher
   C. Different encryption standards
   D. Key distribution

IV. Public-Key (Asymmetric) Cryptography
   A. Principles of public-key cryptosystems
   B. The RSA algorithm
   C. Key management
   D. Other public-key cryptosystems

V. Message Authentication and Digital Signature
   A. Message authentication code (MAC)
   B. Hash functions and algorithms
   C. Digital signature
   D. Authentication protocols

VI. Network Security Practice
   A. Threats in networks
   B. E-mail security
   C. IP security
   D. SSL/TSL, and OpenSSL
   E. Web security
   F. Firewall
   G. Intrusion detection