INFO 3006 INFORMATION SECURITY

Credit Points 10

Legacy Code 300128

Coordinator Yun Bai (https://directory.westernsydney.edu.au/search/name/Yun Bai/)

Description Information Security is concerned with the protection and privacy of information in computer systems. The focus is primarily on introducing cryptography concept, algorithm and protocol in information security and applying such knowledge in the design and implementation of secure computer and network systems. The unit also addresses conventional and public key encryption, number theory and algebra and their application in public key encryption and signature. Students will learn the application of cryptography algorithm in current computer systems and information security management. This unit also provides students with the practical experience around security programming.

School Computer, Data & Math Sciences

Discipline Security Science

Student Contribution Band HECS Band 2 10cp

Check your HECS Band contribution amount via the Fees (https://www.westernsydney.edu.au/currentstudents/current_students/fees/) page.

Level Undergraduate Level 3 subject

Pre-requisite(s) MATH 1006 AND
COMP 2009 OR
COMP 2015 OR
COMP 2016

Assumed Knowledge

Basic understanding of data structures, number theory and probability theory. Basic programming skills in C, C++, java, etc.

Learning Outcomes

On successful completion of this subject, students should be able to:

1. Describe fundamentals in computer security and basic knowledge in cryptography;
2. Explain conventional encryption/decryption methods and the concepts of symmetric keys;
3. Design and implement block ciphers and stream ciphers;
4. Explain principles of public key cryptosystems and public key algorithms;
5. Summarize the number theory used in the RSA algorithm, Diffie-Hellman key exchange and digital signatures;
6. Apply authentication functions and hash functions in message authentication;
7. Illustrate Kerberos authentication protocols;
8. Apply security requirements and design in electronic mail systems and in electronic commerce.
9. Explain principles and mechanisms of security management.

Subject Content

Security, cyberattack and countermeasure, cryptography and steganography
Conventional encryption and DES system
Number Theory and algebra, Modular arithmetic and Euclid's algorithm
Public key encryption and RSA algorithm
Digital signature and authentication protocols
Key distribution and management
Security protocols and various applications in current computer systems
Information Security management

Assessment

The following table summarises the standard assessment tasks for this subject. Please note this is a guide only. Assessment tasks are regularly updated, where there is a difference your Learning Guide takes precedence.

Item	Length	Percent	Threshold	Individual/ Group Task
Short Answer	2-5 pages	25	N	Individual
Practical	500 lines of program	25	N	Individual
Final Exam	2 hours	50	Y	Individual

Prescribed Texts

- Stallings, W. (2017). Cryptography and network security : principles and practice (7th ed.). Boston: Pearson.

Teaching Periods

Spring

Penrith (Kingswood)

Day

Subject Contact Yun Bai (https://directory.westernsydney.edu.au/search/name/Yun Bai/)

View timetable (https://classregistration.westernsydney.edu.au/even/timetable/?subject_code=INFO3006_22-SPR_KW_D#subjects)

Parramatta - Victoria Rd

Day

Subject Contact Yun Bai (https://directory.westernsydney.edu.au/search/name/Yun Bai/)

View timetable (https://classregistration.westernsydney.edu.au/even/timetable/?subject_code=INFO3006_22-SPR_PS_D#subjects)