INFO 3021 INFORMATION SECURITY (ADVANCED)

Credit Points 10

Description This subject introduces cryptography theory and application. It teaches cryptography algorithms and protocols in information security and the application of such knowledge in the design and implementation of secure computer and network systems. The contents include symmetric and asymmetric encryptions, signature, matrix, number theory, algebra, and security protocols. Students will learn the application of cryptography algorithm in current computer systems and information security management. This subject also provides practical exercises by security programming.

School Computer, Data & Math Sciences

Student Contribution Band HECS Band 2 10cp

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

Level Undergraduate Level 3 subject

Pre-requisite(s) MATH1006
COMP2030

Assumed Knowledge

Basic understanding of data structures and discrete mathematics
Basic programming skills in C, C++, Java, Python, etc.

Learning Outcomes

After successful completion of this Subject, students will 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
10. Investigate and apply advanced mathematical knowledges to security algorithms and implementations

Subject Content

1. Security, cyberattack and countermeasure, cryptography, and steganography
2. Conventional encryption and DES system
3. Number Theory and algebra, Modular arithmetic, and Euclid's algorithm
4. Public key encryption and RSA algorithm
5. Digital signature and authentication protocols
6. Key distribution and management
7. Security protocols and various applications in current computer systems
8. Information Security management
9. Conventional and public key decryption algorithms and implementation

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.

Type	Length	Percent	Threshold	Individual/ Group Task
Short Answer	2-5 pages	15	N	Individual
Practical	500 lines of program	20	N	Individual
Final Exam	2 hours	50	N	Individual
Report	5-10 pages	15	N	Individual

Prescribed Texts

Stallings, W. (2023). *Cryptography and network security: Principles and practice* (8th Global ed.). Pearson.

Teaching Periods

Spring (2024)

Penrith (Kingswood)

On-site

Subject Contact

View timetable (https://classregistration.westernsydney.edu.au/even/timetable/?subject_code=INFO3021_24-SPR_KW_1#subjects)

Parramatta - Victoria Rd

On-site

Subject Contact

View timetable (https://classregistration.westernsydney.edu.au/even/timetable/?subject_code=INFO3021_24-SPR_PS_1#subjects)