COMP90043 Cryptography and Security

Credit Points:	12.50
Level:	9 (Graduate/Postgraduate)
Dates & Locations:	This subject is not offered in 2011.
Time Commitment:	Contact Hours: 36 hours, made up of 24 one-hour lectures (two per week) and 12 one-hour workshops (one per week) Total Time Commitment: 120 hours
Prerequisites:	None
Corequisites:	None
Recommended Background Knowledge:	None
Non Allowed Subjects:	433-645 Software System Security 433-448 Applied Cryptography and Coding
Core Participation Requirements:	For the purposes of considering request for Reasonable Adjustments under the Disability Standards for Education (Cwth 2005), and Students Experiencing Academic Disadvantage Policy, academic requirements for this subject are articulated in the Subject Description, Subject Objectives, Generic Skills and Assessment Requirements of this entry. The University is dedicated to provide support to those with special requirements. Further details on the disability support scheme can be found at the Disability Liaison Unit website: http://www.services.unimelb.edu.au/disability/
Contact:	Professor Alistair Moffat email: **ammoffat@unimelb.edu.au (mailto:ammoffat@unimelb.edu.au)**
Subject Overview:	This subject covers fundamental concepts in information security on the basis of methods from modern cryptography, including encryption, signatures and hash functions. The subject will be made up of three parts: (1) cryptography, covering the essentials of public and private key cryptography, stream ciphers, digital signatures and cryptographic hash functions; (2) access control, covering essential elements of authentication and authorization; and (3) secure protocols which are obtained through cryptographic techniques. A particular emphasis will be placed on real-life protocols such as Secure Socket Layer (SSL) and Kerberos.
Objectives:	On completion of this subject students should be able to: # Identify security issues and objectives in computer systems and networks # Apply various security mechanisms derived from cryptography to computers and computer networks # Explain the workings of fundamental public key and symmetric key cryptographic algorithms like RSA, ElGamal, Diffie-Hellman schemes and stream ciphers # Explain the protocols which ensure security in contemporary networked computer systems # Describe the interaction between the underlying theory, including cryptography, and working computer security infrastructure
Assessment:	Two written assignments, due around weeks 3 and 7 of semester, of approximately 1000 words each (20%); a paper of about 10,000 words in the area of cryptography or security due at the end of semester, followed by a 15 minute in-class presentation during the second half of the semester (40%); and a 2-hour end-of-semester written examination (40%).
Prescribed Texts:	TBA
Breadth Options:	This subject is not available as a breadth subject.
Fees Information:	Subject EFTSL, Level, Discipline & Census Date, http://enrolment.unimelb.edu.au/fees

Generic Skills:	On completion of this subjects students should have: # Ability to undertake problem identification, formulation, and solution # Ability to utilise a systems approach to complex problems and to design for operational performance # Ability to manage information and documentation # Capacity for creativity and innovation # Ability to communicate effectively, with the engineering team and with the community at large
Related Majors/Minors/ Specialisations:	B-ENG Software Engineering stream Master of Engineering (Software)