433-448 Applied Cryptography and Coding

Credit Points:	12.50
Level:	4 (Undergraduate)
Dates & Locations:	This subject is not offered in 2009.
Time Commitment:	Contact Hours: Twenty-four hours of lectures, 11 hours of workshops Total Time Commitment: Not available
Prerequisites:	Study at level 3 in at least four of the following areas: artificial intelligence, computer design, database systems, graphics, interactive system design, networks and communications, operating systems, programming languages, software engineering, and theory of computation.
Corequisites:	None
Recommended Background Knowledge:	None
Non Allowed Subjects:	None
Core Participation Requirements:	For the purposes of considering request for Reasonable Adjustments under the Disability Standards for Education (Cwth 2005), and Student Support and Engagement Policy, academic requirements for this subject are articulated in the Subject Overview, Learning Outcomes, Assessment and Generic Skills sections of this entry. It is University policy to take all reasonable steps to minimise the impact of disability upon academic study, and reasonable adjustments will be made to enhance a student's participation in the University's programs. Students who feel their disability may impact on meeting the requirements of this subject are encouraged to discuss this matter with a Faculty Student Adviser and Student Equity and Disability Support: http://services.unimelb.edu.au/disability
Subject Overview:	Topics covered include public key systems, stream ciphers, discrete logarithms based schemes, digital signatures, error correcting and detecting codes, and Hamming and BCH codes.
Objectives:	On completion of this subject students should understand the fundamentals of cryptographic and coding principles, be able to implement cryptographic algorithms, and be familiar with various coding schemes in communications and computers.
Assessment:	A half-hour mid-semester test (10%); two assignments (20%); one term project (35%); and a 2-hour end-of-semester written examination (35%). To pass the subject, students must obtain at least 50% overall, 10/20 in the assignments, 17.5/35 in the term project, and 17.5/35 in the written examination.
Prescribed Texts:	None
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 successful completion students should: # be able to explain workings behind fundamental public key and symmetric key cryptographic algorithms like RSA, ElGamal, Diffie-Hellman schemes and stream ciphers; # be able to implement some fundamental cryptographic algorithms like RSA, ElGamal and Diffie-Hellman schemes; and # be able explain the basic principles of cryptanalysis; # be able to undertake problem identification, formulation and solution; # have a capacity for independent critical thought, rational inquiry and self-directed learning; and # have a profound respect for truth and intellectual integrity, and for the ethics of scholarship.
Related Course(s):	Bachelor of Computer Science (Honours) Bachelor of Engineering (Computer Engineering)

	Bachelor of Engineering (Electrical Engineering) Bachelor of Engineering (Software Engineering)