

## 433-448 Applied Cryptography and Coding

<b>Credit Points:</b>	12.500
<b>Level:</b>	Undergraduate
<b>Dates &amp; Locations:</b>	2008, This subject commences in the following study period/s: Semester 1, - Taught on campus.
<b>Time Commitment:</b>	Contact Hours: Twenty-four hours of lectures, 11 hours of workshops Total Time Commitment: Not available
<b>Prerequisites:</b>	Study at the third-year level 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.
<b>Corequisites:</b>	None
<b>Recommended Background Knowledge:</b>	None
<b>Non Allowed Subjects:</b>	None
<b>Core Participation Requirements:</b>	<p>&lt;p&gt;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.&lt;/p&gt;         &lt;p&gt;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: &lt;a href="http://services.unimelb.edu.au/disability"&gt;http://services.unimelb.edu.au/disability&lt;/a&gt;&lt;/p&gt;</p>
<b>Subject Overview:</b>	<p>The objectives of this subject are for students to understand the fundamentals of cryptographic and coding principles, to be able to implement cryptographic algorithms, and to be familiar with various coding schemes in communications and computers.</p> <p>Topics covered include public key systems, stream ciphers, discrete logarithms based schemes, digital signatures, error correcting and detecting codes, and Hamming and BCH codes.</p>
<b>Assessment:</b>	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.
<b>Prescribed Texts:</b>	None
<b>Recommended Texts:</b>	Information Not Available
<b>Breadth Options:</b>	This subject is not available as a breadth subject.
<b>Fees Information:</b>	Subject EFTSL, Level, Discipline & Census Date, <a href="http://enrolment.unimelb.edu.au/fees">http://enrolment.unimelb.edu.au/fees</a>
<b>Generic Skills:</b>	Information Not Available
<b>Related Course(s):</b>	Bachelor of Computer Science (Honours) Bachelor of Engineering (Computer Engineering) Bachelor of Engineering (Electrical Engineering) Bachelor of Engineering (Software Engineering)