COMP90043 Cryptography and Security

Credit Points:	12.5
Level:	9 (Graduate/Postgraduate)
Dates & Locations:	2015, Parkville This subject commences in the following study period/s: Semester 2, Parkville - Taught on campus.
Time Commitment:	Contact Hours: 3 hours per week Total Time Commitment: 200 hours
Prerequisites:	<table><tr><th>Subject</th><th>Study Period Commencement:</th><th>Credit Points:</th></tr><tr><td>COMP90041 Programming and Software Development</td><td>Semester 1, Semester 2</td><td>12.50</td></tr><tr><td>COMP90038 Algorithms and Complexity</td><td>Semester 1, Semester 2</td><td>12.50</td></tr><tr><td>COMP90007 Internet Technologies</td><td>Semester 1, Semester 2</td><td>12.50</td></tr></table> **Or Equivalent subject.**
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 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
Coordinator:	Assoc Prof Udaya Parampalli
Contact:	email: **udaya@unimelb.edu.au (mailto:udaya@unimelb.edu.au)**
Subject Overview:	**AIMS** The subject will explore foundational knowledge in the area of cryptography and information security. The overall aim is to gain an understanding of fundamental cryptographic concepts like encryption and signatures and use it to build and analyse security in computers, communications and networks. This subject covers fundamental concepts in information security on the basis of methods of modern cryptography, including encryption, signatures and hash functions. This subject is an elective subject in the Master of Engineering (Software). It can also be taken as an advanced elective in Master of Information Technology. **INDICATIVE CONTENT** The subject will be made up of three parts: # Cryptography: the essentials of public and private key cryptography, stream ciphers, digital signatures and cryptographic hash functions

	# Access Control: the essential elements of authentication and authorization; and # 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. Topics drawn from: # Symmetric key crypto systems # Public key cryptosystems # Hash functions # Authentication # Secret sharing # Protocols # Key Management.
Learning Outcomes:	**INTENDED LEARNING OUTCOMES (ILO)** On completion of this subject the student is expected to: 1 Identify security issues and objectives in computer systems and networks 2 Apply various security mechanisms derived from cryptography to computers and computer networks 3 Explain the workings of fundamental public key and symmetric key cryptographic algorithms including RSA, ElGamal, Diffie-Hellman schemes and stream ciphers 4 Explain the protocols which ensure security in contemporary networked computer systems 5 Describe the interaction between the underlying theory and working computer security infrastructure 6 Analyse security of network protocols and systems
Assessment:	Two equally weighted homework assignments done individually with a total of about 1000 words for both the assignments, each requiring 25 - 30 hours of work, due around Week 4 and Week 8 (20%). ILOs 1 to 4 are addressed in this assessment, due in week 4 and week 8. The assessment tests the knowledge of the core modules of the subject topic introduced in lectures. They are generally extensions of tutorial questions One 10-minute presentation given by a group working in pairs due around Week 11 (8%), requiring approximately 10 -11 hours of work, due in week 11. ILOs 1, 5 and 6 and generic skills are addressed in the group project work One 3000-word report about a current security research topic written by a group working in pairs (32%), each member committing approximately 45-50 hours of work, due in Week 12. ILOs 1, 5 and 6 and generic skills are addressed in the group project work One 2-hour written examination held during the end of semester exam period (40%). ILOs 1 to 4 are addressed in the examination. Hurdle requirement: To pass the subject, students must obtain at least: 50% overall. 10/20 in the homework assignments 20/40 in the group-based work 20/40 in the end-of-semester written examination. Intended Learning Outcomes (ILOs) 1 to 4 are addressed in the examination and the two assignments. ILOs 1, 5 and 6 and generic skills are addressed in the group project work. Assignment 1 and 2 tests the knowledge of the core modules of the subject topic introduced in lectures. They are generally extensions of tutorial questions. The knowledge earned during the semester is finally tested in 2 hour examination The group work, done in a group of two students, tests research and presentation skills.
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 subject, students should have the following skills: # Ability to undertake problem identification, formulation, and solution. # Ability to utilise a systems approach to solving 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.
Notes:	**LEARNING AND TEACHING METHODS** Each week there will be student centred activities planned within two lectures and a workshop. In workshops, tutorial questions illustrating the main concepts taught in the lectures will be discussed. **INDICATIVE KEY LEARNING RESOURCES** Students will have access to lecture notes and lecture slides. The subject LMS site also contains links to recommended textbook and resources on security and cryptography. **CAREERS / INDUSTRY LINKS** The concepts of security, trust and privacy are very much essential in a range of disciplines in computing and software engineering. This knowledge and skills learned in the subject also forms a basis of many professional careers such as practicing engineers, consultants and Information Technology specialists. Guest lectures by experts from Industry on specific topics from network security and cryptography will be organized.
Related Course(s):	Master of Information Technology Master of Philosophy - Engineering Master of Science (Computer Science) Master of Software Systems Engineering Ph.D.- Engineering
Related Majors/Minors/ Specialisations:	Approved Masters level subjects from other departments B-ENG Software Engineering stream Computer Science Computer Science MIT Computing Specialisation MIT Distributed Computing Specialisation Master of Engineering (Software)