# COMP90043 Cryptography and Security

| | |
|---|---|
| **Credit Points:** | 12.50 |
| **Level:** | 9 (Graduate/Postgraduate) |
| **Dates & Locations:** | This subject is not offered in 2013. |
| **Time Commitment:** | Contact Hours: 3 hours per week Total Time Commitment: 120 hours |
| **Prerequisites:** | None |
| **Corequisites:** | None |
| **Recommended Background Knowledge:** | None |
| **Non Allowed Subjects:** | 433-645 Software System Security<br>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: <a href="http://services.unimelb.edu.au/disability">http://services.unimelb.edu.au/disability</a> |
| **Contact:** | Dr Udaya Parampalli<br>email: **udaya@unimelb.edu.au (mailto:udaya@unimelb.edu.au)** |
| **Subject Overview:** | 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 analyze 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.<br>This subject is an elective subject in the Master of Engineering (Software). It can also be taken as a advanced elective in Master of Information Technology. |
| **Objectives:** | On completion of this subject students should be able to:<br># Identify security issues and objectives in computer systems and networks<br># Apply various security mechanisms derived from cryptography to computers and computer networks<br># Explain the workings of fundamental public key and symmetric key cryptographic algorithms like RSA, ElGamal, Diffie-Hellman schemes and stream ciphers<br># Explain the protocols which ensure security in contemporary networked computer systems<br># Describe the interaction between the underlying theory, including cryptography, and working computer security infrastructure<br># Analyze security of network protocols and systems |
| **Assessment:** | Project work: It involves two components: Two equally weighted homework assignments done individually with a total of about 1000 words for both the assignments due around Week 4 and Week 8 (20%). A 10-minute presentation given by a group working in pairs due around week 11 (8%) and a 3000-word report about a current security research topic written by a group working in pairs (32%) due in week 12. A 2-hour written examination at the end of the semester (40%). To pass the subject, students must obtain at least:50% overall.10/20 in the |

| | |
|---|---|
| | homework assignments20/40 in the group-based work.20/40 in the end-of-semester written examinationILOs 1 to 4 are addressed in the examination and the two assignments. ILO 1, 5-6 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 subjects students should have:<br># Ability to undertake problem identification, formulation, and solution.<br># Ability to utilise a systems approach to solving complex problems and to design for operational performance<br># Ability to manage information and documentation<br># Capacity for creativity and innovation<br># Ability to communicate effectively, with the engineering team and with the community at large |
| **Related Course(s):** | Master of Engineering in Distributed Computing<br>Master of Information Technology<br>Master of Information Technology<br>Master of Information Technology<br>Master of Philosophy - Engineering<br>Master of Science (Computer Science)<br>Master of Software Systems Engineering<br>Ph.D.- Engineering |
| **Related Majors/Minors/ Specialisations:** | B-ENG Software Engineering stream<br>Computer Science<br>Master of Engineering (Software) |