

Faculty of Computer Science and Information Technology Universiti Putra Malaysia

POSTGRADUATE PROGRAMME BY COURSEWORK

MASTER OF INFORMATION SECURITY



PROGRAMME BY COURSEWORK

Faculty of Computer Science and Information Technology, UPM

Introduction

The Master of Information Security is a 40 credits postgraduate program by coursework at the Faculty of Computer Science and Information Technology, Universiti Putra Malaysia (UPM). This programme offers an opportunity for advanced studies and career development for students to success in the field of information security.

Entrance Requirements

- An applicant should have a Bachelor's degree or equivalent, in computing, science and technology or related to computing, with a minimum CGPA 2.75; or
- Bachelor's degree or equivalent, in computing, science and technology or related to computing with a CGPA of 2.500 – 2.749 may be considered based on a minimum of 1 year of work experience in the related field; or
- Bachelor's degree or equivalent, in computing, science and technology or related to computing with a CGPA of 2.00 – 2.49 may be considered based on a minimum of 5 year of work experience in the related field;
- For a candidate who do not have a Computing Degree, the candidate must take a prerequisite course in computing.

English Language Requirement

International applicants must have obtained a minimum score of 550 for the TOEFL Paper-based Test (Academic Version) or Band 6.0 for IELTS (Academic Training), or 79-80 for TOEFL Internet-based Test (Academic Version) or Level 109 for CIEP at ELS Language Centre.

Programme Offered by Semester

First and Second Semester of every year.

Programme Requirements

In order to graduate, students must complete at least **40 credits**. The minimum cumulative average is **3.000**. The minimum credit distribution for this program is as follows:

Core modules	24 credits
Project paper	10 credits
Field Elective	6 credits
Total	40 credits

A. CORE MODULES (COMPULSORY)

Code	Course Name	Credits
SSK5090	Research Methods in Computer Science	3(3+0)
SSK5207	Cyber Ethics and Law	3(3+0)
SSK5511	Security in Computing	3(3+0)
SSK5506	Information Security Management	3(3+0)
SSK5502	Penetration Testing	3(3+0)
SSK5505	Internet and Cloud Computing Security	3(3+0)
SSK5503	Cryptography and Security Protocol	3(3+0)
SSK5508	Computer Forensic and Investigation	3(3+0)
	TOTAL	24

B. PROJECT PAPER

Code	Course Name	Credits
SSK 5991	Project	10(0+10)
	TOTAL	10

C. FIELD ELECTIVES (choose 2)

Code	Course Name	Credits
SSK5511	Software Security	3(3+0)
SSK5509	Trusted Computing	3(3+0)
SSK5512	Steganography and Digital Watermarking	3(3+0)
SSK5514	Intrusion Detection System	3(3+0)
SSK5513	Public Key Cryptography	3(3+0)
SSK5529	Cryptanalysis	3(3+0)
SSK5537	Blockchain Technology	3(3+0)
SSK5800	Special Topic in Information Security	3(3+0)
	TOTAL	6

Tuition Fees

The fee structure for this programme consists of basic fee and credit-based fee:

a) Basic Fee

Semester	Local	International
First Semester	RM 1,425.00	RM2,475.00
Second and Subsequent Semesters	RM 1,175.00	RM2,225.00

b) Credit-based Fee

Student	Amount	Credit	Total Amount
Local	RM250.00 per credit	40	RM10,000.00
International	RM400.00 per credit		RM16,000.00

NOTE: The fee amount is subject to change from time to time WITHOUT prior notice by the University. Prospective and current students are advised to check the SGS website for any fee changes not earlier than one (1) month before the start of each semester/new students' registration. All fees must be paid upon registration.

OTHER COST: Please refer to School of Graduate Studies website at http://www.sgs.upm.edu.my

COURSE SYNOPSIS

SSE5101 Programming and Computer-based Problem Solving

This course covers problem-solving technique using computer programming. Programming elements and algorithms to produce effective program are discussed.

SSK5090 Research Methods in Computer Science

This course introduces students to the research methods in computer science and gives ideas on how to plan, organize and use the available resources efficiently in helping them in their research.

SSK5207 Cyber Ethics and Law

This course covers the fundamentals of cyberlaw and computer ethics. It emphasizes ethical attitude and practice in matter relating to cyber law and ethics, and accountability towards the actions taken.

SSK5500 Security in Computing

This course covers protection methods against various attacks on legitimate users, including necessary actions to track, document, and prevent the threats. Awareness on security threats and vulnerabilities as well as best practices in computer security are discussed.

SSK5502 Penetration Testing

This course includes supporting theory in understanding the ways in which computer systems can be attacked and invaded by bypassing security or exploiting system vulnerabilities. Several principles and methods are used to ethically assess and evaluate computer security.

SSK5503 Cryptography and Security Protocol

This course covers the concept of cryptography and its applications. Two categories of cryptography techniques, namely symmetric ciphers and public-key are discussed. Message authentication and appropriate cryptography techniques are used in constructing security protocol for application systems.

SSK5505 Internet and Cloud Computing Security

This course covers advanced topics in cloud network security that emphasizes the network security practices and practical applications that have been adopted to ensure the security of the Internet and cloud is guaranteed. Secure design and deployment are also discussed.

SSK5506 Information Security Management

This course covers the techniques being used in managing information security. A pragmatic approach that manages the entire information security process within a large organisation shall be introduced.

SSK5508 Computer Forensic and Investigation

This course covers the principles of forensic evidence, criminal investigations, evidence collection and handling procedures that can be admissible in court. The search methods, documentations, forensic toolkits, acquisition and data analysis methods, data examination, evidence collection, fraud and forensic accounting, writing computer forensic reports, as well as legal, ethical and policies are also discussed.

SSK5509 Trusted Computing

This course covers the underlying mechanisms and technologies needed for trusted computing, which include hardware and trust models, attestation protocols such as

Direct Anonymous Attestation and Single Sign-On to make authorization decisions. Some of the applications discussed include certificate management, conditional access for mobile recipients and peer-to-peer (P2P) networks in protecting the security and privacy of information providers and end users.

SSK5511 Software Security

This course covers the common software security problems, their underlying causes, and solutions to the problems. Techniques to prevent and detect the software security level shall be discussed in this course.

SSK5512 Steganography and Digital Watermarking

This course covers steganography and digital watermarking technics that can be adapted for information security problems in industry or specific domains. Emphasis on current trends and practices in the real world also discussed.

SSK5513 Public Key Cryptography

This course covers cryptographic techniques and algorithms with their implementations in different situations. Limitations of cryptography will be identified before implementation of the cryptosystems.

SSK5514 Intrusion Detection System

This course focuses on the concepts and issues related to intrusion detection system (IDS). IDS functions, detection approaches, analysis schemes and deployment of IDS are also discussed.

SSK5529 Cryptanalysis

This course covers various techniques of cryptanalysis starting from cryptanalysis for classic ciphers, linear cryptanalysis, differential cryptanalysis and current cryptanalysis. Limitation of cryptanalysis will be identified before execution.

SSK5537 Blockchain Technology

This course covers the concepts, technologies, and impacts of blockchain technology in society. The architecture, consensus, application and security of decentralized blockchain by maintaining transparency, anonymity, security, variability, and history in the open domain are also discussed.

SSK5580 Special Topic in Information Security

This course focuses on selected issues and trends related to the field of information security. Exploration of key issues and new direction is conducted through analysis of critical issues and problems to recommend solutions.

SSK 5991 Project

The student will carry out a detailed study to evaluate the significant method and develop a research project related to information security under a supervision of a lecturer. Students will perform the study according to a suitable methodology for the project that will be implemented. A proposal report needs to be prepared at the beginning of the study. At the end of the project, the student will submit a complete project report for evaluation. The student will also be required to present the project in a seminar organised by the department.

Application for Admission:

School of Graduate Studies Zone 4, Off Jalan Stadium Universiti Putra Malaysia 43400 UPM Serdang Selangor Darul Ehsan MALAYSIA Tel: (603) 9769 4218 / 4223 / 4165 / 4169 / 4225 Website: http://www.sgs.upm.edu.my

For further information on academic programmes, please contact:

Faculty of Computer Science and Information Technology Universiti Putra Malaysia 43400 UPM Serdang Selangor Darul Ehsan MALAYSIA Tel: (603) 9769 1742/ 1744/ 1787 /3091 Website: http://www.fsktm.upm.edu.my

Master Programme Coordinator (by coursework) Faculty of Computer Science and Information Technology Universiti Putra Malaysia 43400 UPM Serdang Selangor Darul Ehsan MALAYSIA. Tel: (603) 9769 1757/ 3091 Email: ifah@upm.edu.my