



The University of Southern Queensland

Course specification

The current and official versions of the course specifications are available on the web at <http://www.usq.edu.au/coursespecification/current>.
Please consult the web for updates that may occur during the year.

Description: Cryptography and Security

Subject	Cat-nbr	Class	Term	Mode	Units	Campus
CSC	8419	86862	1, 2009	ONC	1.00	Toowoomba

Academic group:	FOSCI
Academic org:	FOS003
Student contribution band:	2
ASCED code:	020113

STAFFING

Examiner: Hua Wang
Moderator: Ron Addie

REQUISITES

Pre-requisite: Students must be enrolled in one of the following Programs: MCOP or MPIT

OTHER REQUISITES

Pre-requisite: Know basics of programming in C, C++, Java, or other high level language, or possess basic knowledge of any field related to cryptology.

RATIONALE

Security has become an important and challenging goal in the design of computer systems. A number of security techniques such as signature, multi-signature, blind signature and access control have been published and have been adopted by researchers and industry applications. This course will provide students with key knowledge about the nature and challenges of computer security, especially the relationship between policy and security, the role and application of cryptography, the methodologies and technologies for assurance, vulnerability analysis and intrusion detection and building secure systems.

SYNOPSIS

The course gives a broad overview of methods of implementing security services based on cryptography in today's communication networks. Topics to be covered include the fundamentals of contemporary cryptography and its application to network services, such as confidentiality, integrity, authentication, and non-repudiation. We show new ideas in cryptology, such as public key cryptography and zero-knowledge protocols, permit the efficient solutions to the problems of digital signature, electronic cash, key exchange, and access control. We analyse the strength of today's ciphers and their implementations, and discuss the best known crypto analytical techniques used to break security systems. We analyse the most popular implementations of cryptography used on the Internet, including systems for electronic mail protection, secure WWW, and electronic

payment protocols. We discuss the ongoing work on the development of American and international standards for secure communications and present the most recent research trends in cryptology.

OBJECTIVES

On successful completion of this course should be able to:

1. Analyse and address a number of situations in which security can be compromised (Project Proposal, Final Research Report);
2. Understand and apply selected protocols used to ensure security (Project Proposal);
3. Apply the algorithms behind some current cryptographic protocols (Project Implementation);
4. Demonstrate understanding of how insecure systems can be attacked (Final Research Report);
5. Understand public key systems and their applications (Project Implementation);
6. Demonstrate detailed knowledge of the RSA algorithm (Final Research Report);
7. Demonstrate detailed knowledge of the PGP system (Project Implementation);
8. Design and develop techniques and algorithms that are used to implement these protocols (Project Implementation, Final Research Report).

TOPICS

Description	Weighting (%)
1. Review of pre-computing cryptography.	5.00
2. Single key and public key cryptography.	9.00
3. Key management and attacks on public key systems.	9.00
4. Secrecy and digital signatures.	9.00
5. The RSA public key algorithm	9.00
6. Knapsack algorithms and ways to break them.	9.00
7. Authentication and the Kerberos algorithm.	9.00
8. Hash functions and birthday attacks.	9.00
9. Multiple key cryptography: secret splitting and sharing.	9.00
10. Mental poker and anonymous distribution.	9.00
11. The PGP package.	9.00
12. The attitude of public bodies to security.	5.00

TEXT and MATERIALS required to be PURCHASED or ACCESSED

ALL textbooks and materials are available for purchase from USQ BOOKSHOP (unless otherwise stated). Orders may be placed via secure internet, free fax 1800642453, phone 07 46312742 (within Australia), or mail. Overseas students should fax +61 7 46311743, or phone +61 7 46312742. For costs, further details, and internet ordering, use the 'Textbook Search' facility at <http://bookshop.usq.edu.au> click 'Semester', then enter your 'Course Code' (no spaces).

Gollmann, Dieter 2006, *Computer security*, 2nd edn, Wiley, New York.

REFERENCE MATERIALS

Reference materials are materials that, if accessed by students, may improve their knowledge and understanding of the material in the course and enrich their learning experience.

Finally, there are many relevant and interesting resources on the web, from newsgroups such as sci.crypt.research and comp.risks through hacker and CERT sites to organisations involved in crypto policy and, of course, researchers' home pages (<http://www.swcp.com/~mccurley/cryptographers/cryptographers.html>).

Bishop, Matt 2004, *Introduction to computer security*, Addison Wesley, Boston.

Cheswick, WR & Bellovin, SM 2003, *Firewalls and internet security*, 2nd edn, Addison-Wesley Professional,

Ferguson, N & Schneier, B 2003, *Practical cryptography*, John Wiley & Sons, New York.

Garfinkel, S & Spafford, G 2003, *Practical unix and internet security*, 3rd edn, O'Reilly & Associates,

(Online from Library)

STUDENT WORKLOAD REQUIREMENTS

ACTIVITY	HOURS
Lectures	24.00
Private Study	54.00
Project Work	80.00
Tutorials	12.00

ASSESSMENT DETAILS

Description	Marks out of	Wtg (%)	Due date
PROJECT PROPOSAL	20.00	20.00	20 Mar 2009
PROJECT IMPLEMENTATION	30.00	30.00	01 May 2009
FINAL RESEARCH REPORT	50.00	50.00	19 Jun 2009

IMPORTANT ASSESSMENT INFORMATION

1 Attendance requirements:

It is the students' responsibility to attend and participate appropriately in all activities (such as lectures, tutorials and practical work) scheduled for them, and to study all material provided to them or required to be accessed by them to maximise their chance of meeting the objectives of the course and to be informed of course-related activities and administration.

2 Requirements for students to complete each assessment item satisfactorily:

To satisfactorily complete an assessment item a student must achieve at least 50% of the marks. Students do not have to satisfactorily complete each assessment item to be awarded a passing grade in this course. Refer to Statement 4 below for the requirements to receive a passing grade in this course.

- 3 Penalties for late submission of required work:
If students submit assignments after the due date without (prior) approval of the examiner then a penalty of 5% of the total marks gained by the student for the assignment may apply for each working day late up to ten working days at which time a mark of zero may be recorded.
- 4 Requirements for student to be awarded a passing grade in the course:
To be assured of receiving a passing grade a student must achieve at least 50% of the total weighted marks available for the course.
- 5 Method used to combine assessment results to attain final grade:
The final grades for students will be assigned on the basis of the aggregate of the weighted marks obtained for each of the summative assessment items in the course.
- 6 Examination information:
There is no examination in this course.
- 7 Examination period when Deferred/Supplementary examinations will be held:
As there are no examinations in this course, there will be no deferred or supplementary examinations.
- 8 University Regulations:
Students should read USQ Regulations 5.1 Definitions, 5.6. Assessment, and 5.10 Academic Misconduct for further information and to avoid actions which might contravene University Regulations. These regulations can be found at the URL <http://www.usq.edu.au/corporateservices/calendar/part5.htm> or in the current USQ Handbook.

ASSESSMENT NOTES

- 9 The due date for an assignment is the date by which a student must despatch the assignment to the USQ. The onus is on the student to provide proof of the despatch date, if requested by the Examiner.
- 10 Students must retain a copy of each item submitted for assessment. This must be produced within five days if required by the Examiner.
- 11 The due date for an assignment is the date by which a student must despatch the assignment to the USQ. The onus is on the student to provide proof of the despatch date, if requested by the Examiner.
- 12 In accordance with University Policy, the Examiner may grant an extension of the due date of an assignment in extenuating circumstances.
- 13 Students who have undertaken all of the required assessments but who have failed to meet some of the specified objectives within the normally prescribed time may be awarded the temporary grade: IM (Incomplete - Make up). An IM grade will only be awarded when, in the opinion of the examiner, a student will be able to achieve the remaining objectives of the course after a period of non directed personal study.
- 14 Students who, for medical, family/personal, or employment-related reasons, are unable to complete an assignment may apply to defer an assessment in a course. Such a request must be accompanied by appropriate supporting documentation. The following temporary grade IDM (Incomplete Deferred Make-up) may be awarded.