

---

---

# SCSSE

School of Computer Science and Software Engineering  
Faculty of Informatics

---

---

## CSCI971 Advanced Computer Security Subject Outline Spring Session 2009

---

Head of School –Professor Willy Susilo, Student Resource Centre, Tel: (02) 4221 3606

### GENERAL INFORMATION

**Subject Coordinator**

Telephone Number:

Email:

Location:

Associate Professor Yi Mu

02 4221 5228

ymu@uow.edu.au

3.218

Professor Mu's consultation times during session:

Day

Wednesday

Friday

Time

13:30 – 15:30

13:30 – 15:30

**Lecturer**

Telephone Number:

Email:

Location:

Dr Tianbing Xia

02 4221 3076

txia@uow.edu.au

3.205

Dr Xia's consultation times during session:

Day

Monday

Wednesday

Time

13:30 – 15:30

13:30 – 15:30

**Subject Organisation**

Session:

Credit Points

Contact hours per week:

Lecture Times &amp; Location:

Tutorial Day, Time and Location can be found at:

Spring Session, Wollongong Campus

6 credit points

2 hours lectures

15:30– 17:30 Thurs, 3-121

<http://www.uow.edu.au/student/timetables/index.html>

Students should check the subject's web site regularly as important information, including details of unavoidable changes in assessment requirements will be posted from time to time via e-Learning space <http://www.uow.edu.au/student/>. Any information posted to the web site is deemed to have been notified to all students.

**Subject Description**

This subject provides a review of computer security. Topics include: digital signatures, elliptic curve cryptography, El Gamal public key methods, the Advanced Encryption Standard (AES), Security Standards, Security Evaluation Standards, Linear Cryptanalysis, Differential Cryptanalysis.

---

## Subject Objectives

At the completion of this subject students will be able to:

- i) understand and use modern cryptographic techniques;
- ii) access appropriate technique to be used in specific conditions;
- iii) undertake rudimentary cryptanalysis of a cryptalgorithm or hash algorithm;
- iv) understand what is required to get a certified security evaluation.

## Graduate Qualities

This subject will continue to the following graduate qualities:

Informed  
Independent Learners  
Problem Solvers  
Effective Communicators  
Team Work  
Innovation & Design

Further information can be found at:

<http://www.uow.edu.au/informatics/scsse/current/SubjectInformation/UOW049401.html>

## Attendance Requirements:

It is the responsibility of students to attend all lectures/tutorials/labs/seminars/practical work for subjects for which you are enrolled. It should be noted that the amount of time spent on each 6 credit point subject should be at least 12 hours per week, which includes lectures/tutorials/labs etc.

Satisfactory attendance is deemed by the University, to be attendance at approximately 80% of the allocated contact hours.

Students **MUST** attend their **allocated** tutorial unless they have the written permission of the subject coordinator.

## Method of Presentation:

In order to maximize learning outcomes, it is strongly recommended that students attend all lectures.

## Lecture Schedule:

A proposed Lecture schedule for the subject is as follows:

Week	Topic	Reading
1	Introduction, cryptology.	
2	Encryption, block ciphers: AES.	A1 released.
3	Linear cryptanalysis, differential cryptanalysis.	
4	Finite fields for cryptography.	
5	Hashing, Integrity	
6	Security notions	
7	Public Key cryptography. ElGamal, Cramer-Shoup.	A1 due. A2 released.
8	Signature schemes, Elliptic curve cryptography.	
9	Elliptic curve cryptography, Bilinear pairing.	
10	Bilinear pairing, Identity based cryptography.	
11	Presentation	
12	Presentation	
13	Revision.	A2 due.

Changes to the above schedule will be posted via e-Learning space <http://www.uow.edu.au/student/>. Any information posted to the web site is deemed to have been notified to all students.

### Subject Materials:

Any readings/references are recommended only and are not intended to be an exhaustive list. Students are encouraged to use the library catalogue and databases to locate additional readings

Any readings/references are recommended only and are not intended to be an exhaustive list. Students are encouraged to use the library catalogue and databases to locate additional readings

Lecture material for the course will be posted on the eLearning site for the course.

### Textbook(s):

Wenbo Mao, *Modern Cryptography*, Prentice-Hall.

### Other Resources:

References:

J. Pieprzyk, T. Hardjono and J. Seberry, *Cryptography: an introduction to computer security*, Springer Verlag, 2003.

D.Gollmann, *Computer Security*, John Wiley, 1999.

C.H. Meyer, S.M. Matyas, *Cryptography: a new dimension in computer data security*, John Wesley & Sons, New York, 1982.

B.Schneier, *Applied Cryptography*, John Wiley, Second edition, 1996.

W Stallings, *Cryptography and Network Security*, Fourth Edition, Prentice Hall, 2006.

C. Kaufman, R. Perlman, and M. Speciner *Network Security: PRIVATE communication in a PUBLIC world*, Second edition, Prentice Hall, 2002.

These may be available from UniCentre Bookshop

### Assessment:

This subject has the following assessment components.

ASSESSMENT ITEMS & FORMAT	% OF FINAL MARK	GROUP/INDIVIDUAL	DUE DATE
A1: Cryptography, block ciphers, cryptanalysis, finite fields, hashing, hardness. Some programming may be required.	15%	Individual	Week Seven
A2: Public key cryptography, security notions, security proofs, implementations. Some programming may be required.	15%	Individual	Week Thirteen
Presentation and report, possibly to be done in pairs. Topics will be made available by about Week 5 or 6.	20%	Possibly in pairs, depending on the numbers of students enrolled.	Week Eleven or Twelve.
Final Examination	50%		Examination Period

### Notes on Assessment:

All assignments are expected to be completed independently. Plagiarism may result in a FAIL grade being recorded for that assignment.

### Electronic Submission of Assessment Items:

Unless otherwise notified by the subject coordinator, all written assignments must be submitted electronically.

Submission of assessment items via email will not be accepted.

Submission of assignments will primarily be in the form of handwritten/printed copies. If there are programming exercises the code will be submitted using *submit* on Banshee.

### **Other Procedures for the submission of assessment items:**

In addition to electronic submission students are required to submit assignments in hard copy to their tutor.

All assignments will be returned within 2 weeks of their submission.

**To be eligible for a Pass in this subject a student must achieve a mark of at least 40% in the exam. Students who fail to achieve this minimum mark & would have otherwise passed will be given a TF (Technical Fail) for this subject.**

### **Procedures for the return of assessment items:**

Generally assignment marks will be given to students, by email, within two weeks of the final submission date.

### **Penalties for late submission of assessment items:**

Penalties apply to all late work, except if student academic consideration has been granted. Late submissions will attract a penalty of 20% deduction of the assessment mark.

This amount is per day including weekends.

Work more than five (5) days late will be awarded a mark of zero.

### **Tutorial/Lab Closure Policy**

If for any reason, the number of students in a tutorial or lab falls below a sustainable enrolment level, as determined by the Head of School, tutorials/labs offered for that subject may be collapsed or deleted.

You will have to attend the new tutorials/lab if this closure affects the one you are attending.

We will endeavour to make this decision no later than Week 4 of session.

### **Supplementary Exams**

Supplementary Exams will be dealt with in accordance with student academic consideration policy (<http://www.uow.edu.au/about/policy/studentacademicconsiderationpolicy.pdf>) 9.2 Timing of Supplementary Exams.

While the School normally grants supplementary exams when the student does not sit the standard exam for an acceptable reason, each case will be assessed on its own merit and there is no guarantee a supplementary exam will be granted. If a supplementary exam is granted, you will normally be notified via SOLS Mail the time and date of this supplementary exam. You must follow the instructions given in the email message.

**Please note that if this is your last session and you are granted a supplementary exam, be aware that your results will not be processed in time to meet the graduation deadline.**

### **Student Academic Consideration Policy**

The School recognises that it has a responsibility to ensure equity and consistency across its subjects for all students. Sometimes, in exceptional circumstances, students need to apply for student academic consideration in order to complete all assessable work.

The University applies strict criteria to the granting of student academic consideration. Before applying for student academic consideration, students should carefully read the University's policy which can be found at: <http://www.uow.edu.au/about/policy/studentacademicconsiderationpolicy.pdf>.

## **Plagiarism**

### **When you submit an assessment task, you are declaring the following**

1. It is your own work and you did not collaborate with or copy from others.
2. You have read and understand your responsibilities under the University of Wollongong's policy on plagiarism.
3. You have not plagiarised from published work (including the internet). Where you have used the work from others, you have referenced it in the text and provided a reference list at the end of the assignment.

Students must remember that:

Plagiarism will not be tolerated.

Students are responsible for submitting original work for assessment, without plagiarising or cheating, abiding by the University's policies on Plagiarism as set out in the University Handbook under University Policy Directory and in Faculty handbooks and subject guides. Plagiarism has led to the expulsion from the University.

## **Student Academic Grievance Policy**

The School aims to provide a fair, equitable and productive learning environment for all its students. The Student Academic Grievance Policy seeks to support the achievement of this goal by providing a transparent and consistent process for resolving student academic grievances.

Any student who has a grievance over a result should obtain a Faculty of Informatics Appeal Against Decision or Action Affecting Academic Experience form from the Informatics Student Enquiry Centre. (<http://www.uow.edu.au/content/groups/public/@web/@inf/@faculty/documents/doc/uow017433.pdf>) The student should firstly take the form to the marker/lecturer to discuss the matter and, if the student is still not satisfied, s/he should take the next step as outlined on the form.

Once the grievance has been considered by the Faculty, if the student still feels the situation has not been fully resolved s/he may consult the Dean of Students. However, the Dean of Students can have no input into the academic judgment of the lecturer and can only review the grievance to ensure proper procedure has been followed.

### **Relevant University Policies, procedures and students services:**

For more information students must refer to the Faculty handbook, online references or consult the UOW policy in full at <http://www.uow.edu.au/handbook/courserules/studacgrievpol.html> which contains a range of policies on educational issues and student matters.

This subject outline can be found at: <http://www.uow.edu.au/informatics/scsse/current>

This outline should be read in conjunction with the following documents:

Code of Practice - Teaching and Assessment <a href="http://www.uow.edu.au/handbook/codesofprac/teaching_code.pdf">http://www.uow.edu.au/handbook/codesofprac/teaching_code.pdf</a>	Code of Practice - Students <a href="http://www.uow.edu.au/handbook/codesofprac/cop_students.html">http://www.uow.edu.au/handbook/codesofprac/cop_students.html</a>
Code of Practice-Honours <a href="http://www.uow.edu.au/handbook/CodeofPractice-Honours.pdf">http://www.uow.edu.au/handbook/CodeofPractice-Honours.pdf</a>	Acknowledgement Practice <b>Plagiarism will not be tolerated:</b> <a href="http://www.uow.edu.au/handbook/courserules/plagiarism.html">http://www.uow.edu.au/handbook/courserules/plagiarism.html</a>
Key Dates <a href="http://www.uow.edu.au/student/dates.html">http://www.uow.edu.au/student/dates.html</a>	Student Academic Consideration Policy: <a href="http://www.uow.edu.au/about/policy/studentacademicconsiderationpolicy.pdf">http://www.uow.edu.au/about/policy/studentacademicconsiderationpolicy.pdf</a>
Course Progress Requirements: <a href="http://www.uow.edu.au/student/mrp/index.html">http://www.uow.edu.au/student/mrp/index.html</a>	Graduate Qualities Policy: <a href="http://www.uow.edu.au/about/teaching/qualities/index.html#_The new UOW">http://www.uow.edu.au/about/teaching/qualities/index.html#_The new UOW</a>
Academic Grievance Policy (Coursework and honours students) <a href="http://www.uow.edu.au/handbook/courserules/studacgrievpol.html">http://www.uow.edu.au/handbook/courserules/studacgrievpol.html</a>	Non-Discriminatory Language Practice and Presentation <a href="http://staff.uow.edu.au/eed/nondiscrimlanguage.html">http://staff.uow.edu.au/eed/nondiscrimlanguage.html</a>
Occupational Health and Safety <a href="http://staff.uow.edu.au/ohs/commitment/ohspolicy/index.html">http://staff.uow.edu.au/ohs/commitment/ohspolicy/index.html</a>	Ownership of Work & Intellectual Property Policy: <a href="http://www.uow.edu.au/handbook/generalcourserules/UOW028651.html">http://www.uow.edu.au/handbook/generalcourserules/UOW028651.html</a>
Human Research Ethics Committee: <a href="http://www.uow.edu.au/research/rso/ethics/human/">http://www.uow.edu.au/research/rso/ethics/human/</a>	Rules for student conduct: <a href="http://www.uow.edu.au/handbook/generalrules/StudentConductRules.pdf">http://www.uow.edu.au/handbook/generalrules/StudentConductRules.pdf</a>
Independent Learners' Introductory Program <a href="http://www.uow.edu.au/student/attributes/ilip/">http://www.uow.edu.au/student/attributes/ilip/</a>	Informatics Faculty Librarian, Ms Annette Meldrum, phone: 4221 4637, email: <a href="mailto:ameldrum@uow.edu.au">ameldrum@uow.edu.au</a>
Student Support Services: <a href="http://www.uow.edu.au/student/services/">http://www.uow.edu.au/student/services/</a> Informatics Faculty SEDLO ( <b>Student Equity and Diversity Liaison Officers</b> ) Virginie Schmelitschek, phone 4221 3833, <a href="mailto:virginie@uow.edu.au">virginie@uow.edu.au</a>	SCSSE Internet Access & Student Resource Centre <a href="http://www.uow.edu.au/informatics/common/uow024466.html">http://www.uow.edu.au/informatics/common/uow024466.html</a>
SCSSE Computer Usage Rules <a href="http://www.uow.edu.au/informatics/common/uow024457.html">http://www.uow.edu.au/informatics/common/uow024457.html</a>	SCSSE Subject Outlines <a href="http://www.uow.edu.au/informatics/scsse/current">http://www.uow.edu.au/informatics/scsse/current</a>