SCIT

School of Computing and Information Technology
Faculty of Engineering & Information Sciences

SIM Session 3, 2024
Subject Outline
CSCI361 – Cryptography and Secure Applications

Subject Organisation

Subject Coordinator/Lecturer:	Distinguished Professor Willy Susilo
Email:	wsusilo@uow.edu.au
Credit Points:	6 credit points
Duration:	1 session
Lecture Times & Location:	Refer to SIMConnect

The University uses the eLearning system Moodle to support all coursework subjects.

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

In extraordinary circumstances the provisions stipulated in this Subject Outline may require amendment after the Subject Outline has been distributed. All students enrolled in the subject must be notified and have the opportunity to provide feedback in relation to the proposed amendment, prior to the amendment being finalised.

Data on student performance and engagement (such as Moodle and University Library usage, task marks, use of SOLS) will be available to the Subject Coordinator to assist in analysing student engagement, and to identify and recommend support to students who may be at risk of failure. If you have questions about the kinds of data the University uses, how we collect it, and how we protect your privacy in the use of this data, please refer to http://www.uow.edu.au/dvca/bala/analytics/index.html

Subject Description

This subject develops the skills and knowledge necessary to identify and address security problems in a variety of simple communication models. Topics covered include: Classical cryptology, Modern secret key cryptography including block (DES, AES) and stream ciphers (RC4), security properties (authentication, integrity, confidentiality, availability), public key cryptography (knapsacks, RSA, Rabin, Elgamal), digital signatures (RSA, DSS, Elgamal), hashing (birthday paradox, Merkle-Damgard construction), MACS's, Key management (PKI, certificates, key establishment/exchange/transport, Diffie-Hellman) and other applications.

Subject Learning Outcomes

On successful completion of this subject, students will be able to:

1. Explain and apply fundamental cryptographic principles and terminology;
2. Classify and distinguish cryptographic algorithms in terms of their cryptographic characteristics and services provided;
3. Select and apply appropriate fundamental cryptographic building blocks, such as encryption, hashing and authentication, based on a critical analysis of an application scenario;
4. Implement cryptographic algorithms in Java or C/C++.
5. Describe and demonstrate the use of some of the mathematics underlying modern public key cryptography.
6. Assess and contrast the security of given scenarios, and justify the need for additional security as appropriate, taking into account the required cryptographic properties and such factors as efficiency.
7. Analyse implementations of cryptographic algorithms.
8. Explain the role of, and illustrate and usage of, cryptography in a range of applications.
9. Discuss the significance of cryptography in modern society.
10. Read and interpret aspects of cryptographic technical documents such as RFC's and standard's documents, if relevant.
11. Present and rewrite material demonstrating competence in the above outcomes.
12. Apply statistical cryptanalysis.

Recent Improvements

The School is committed to continual improvement in teaching and learning and takes into consideration student feedback from many sources. These sources include direct student feedback to tutors and lecturers, feedback through Student Services and the Faculty Central, and responses to the Subject Evaluation Surveys. This information is also used to inform comprehensive reviews of subjects and courses.

Attendance Requirements

It is the responsibility of students to attend all lectures/tutorials/labs/seminars/practical work for subjects for which you are enrolled.

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

Method of Presentation

The subject will be presented as a series of lectures and tutorials.

Students must be aware that they are responsible for their own learning. Students must prepare adequately for lectures and tutorials in order to properly digest the material presented in those forms. Students are expected to undertake private study in order to fully understand and integrate all the material covered in this unit.

Subject Material

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.

Reference Books

- *Cryptography Engineering: Design Principles and Practical Applications*, Niels Ferguson, Bruce Scheneier and Tadayoshi Kohno, Addison-Wesley, 2010.
- *Understanding* Cryptography, Christof Paar and Jan Pelzl, Springer, 1998.
- Cryptography *and Network Security*, W. Stallings, Fourth Edition, Prentice Hall, 2005
- *Introduction to Computer Security*, J. Seberry, J. Pieprzyk and T. Hardjono, Springer-Verlag, 2003
- *Modern Cryptography: Theory and Practice*, W. Mao, First Edition, Prentice Hall, 2003
- *Security in Computing*, C. P. Pfleeger and S. L. Pfleeger, Third Edition, Prentice Hall, 2003
- *Cryptography: Theory and Practice*, D. Stinson, Third Edition, CRC Press, 2005

Assessment

This subject has the following assessment components.

ASSESSMENT ITEMS & FORMAT	% OF FINAL MARK	GROUP/ INDIVIDUAL	DUE DATE	SUBJECT LEARNING OUTCOMES	CRITERIA TO ASSESS ITEM
2 Assignments: Analysis and Programming	15%	Individual	TBA	3, 4, 5, 6, 7, 12	Consistency with specification
Written test	15%	Individual	TBA	1, 2, 8, 9, 10, 11	Correctness of the answers
Final Examination	55%	Individual	During Exam	1, 2, 8, 9, 10, 11	Correctness of the answers

			Period		

Notes on Assessment

- There is NO supplementary test available for the written test. All students MUST attend the tutorial and do the test in order to get the available 15% marks.
- Assignments are to be submitted on the due date. Details will be provided in the tutorial.
- Assignments may be scanned with a plagiarism detector.
- Late assignments without granted extension will be marked but the mark awarded will be **reduced by 25% for each day late**. Assignments more than three days late **will not be accepted**.

Method of Submission of Assessment Items

Assignments are to be submitted via Moodle.

Arrangement for acknowledging submission of written work

Acknowledgement of submission will occur electronically through Moodle.

Procedure for the return of assessment items

Assessment of assignments will be done electronically on Moodle.

Procedure for the retention of assessed work

The University may retain copies of student work in order to facilitate quality assurance of assessment processes, in support of the continuous improvement of assessment design, assessment marking and for the review of the subject. The University retains records of students' academic work in accordance with the University Records Management Policy and the State Records Act 1988 and uses these records in accordance with the University Privacy Policy and the Privacy and Personal Information Protection Act 1998.

Assessment General

Submission of assessment items via email will not be accepted.

Student contributions to tutorial and/or seminars

Not applicable.

Assessment task is set up to be checked by Turnitin

This subject does not use Turnitin.

Assessment Quality Cycle

The University of Wollongong is committed to the quality assurance and quality enhancement of assessment. The University will meet its legislative and regulatory obligations, to ensure consistent and appropriate assessment through course management and coordination, including assessment quality assurance procedures. An Assessment Quality Cycle is used to describe quality assurance at the points

of assessment design, assessment delivery, the declaration of marks and grades, and review and improvement activities.

Referencing System

The type of referencing system to be used for written work is as follows:

- the Author-Date (Harvard) referencing system is the University's default referencing system to be used in the absence of a documented faculty/school preferred referencing style. Refer to the Library Referencing and Citing link: https://www.uow.edu.au/student/learningcoop/referencingciting/index.html

Internet Resources

Not applicable.

Technical Fail

Students that receive **less than 40% (22/55) of the marks available for the final examination** may receive **a technical fail (TF) grade if their overall subject mark is 50 or higher.**

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 25% of the assessment mark.**

This amount is per day including weekends.

Assignments more than three days late **will not be accepted**.

UOW Grade Descriptors

GRADE	DESCRIPTOR
High Distinction(HD) 85-100%	For performance that provides evidence of an outstanding level of attainment of the relevant subject learning outcomes, demonstrating the attributes of a distinction grade plus (as applicable) one or more of the following: • consistent evidence of deep and critical understanding • substantial originality and insight in identifying, generating and communicating competing arguments, perspectives or problem-solving approaches • critical evaluation of problems, their solutions and their implications • use of quantitative analysis of data as the basis for deep and thoughtful judgments, drawing insightful, carefully qualified conclusions from this work • creativity in application as appropriate to the discipline • eloquent and sophisticated communication of information and ideas in terms

	of the conventions of the discipline • consistent application of appropriate skills, techniques and methods with outstanding levels of precision and accuracy • all or almost all answers correct, very few or none incorrect
Distinction (D) 75-84%	For performance that provides evidence of a superior level of attainment of the relevant subject learning outcomes, demonstrating the attributes of a credit grade plus (as applicable) one or more of the following: • evidence of integration and evaluation of critical ideas, principles, concepts and/or theories • distinctive insight and ability in applying relevant skills, techniques, methods and/or concepts • demonstration of frequent originality in defining and analysing issues or problems and providing solutions • fluent and thorough communication of information and ideas in terms of the conventions of the discipline • frequent application of appropriate skills, techniques and methods with superior levels of precision and accuracy • most answers correct, few incorrect
Credit (C) 65-74%	For performance that provides evidence of a high level of attainment of the relevant subject learning outcomes, demonstrating the attributes of a pass grade plus (as applicable) one or more of the following: • evidence of learning that goes beyond replication of content knowledge or skills • demonstration of solid understanding of fundamental concepts in the field of study • demonstration of the ability to apply these concepts in a variety of contexts • use of convincing arguments with appropriate coherent and logical reasoning • clear communication of information and ideas in terms of the conventions of the discipline • regular application of appropriate skills, techniques and methods with high levels of precision and accuracy • many answers correct, some incorrect
Pass (P) 50-64%	For performance that provides evidence of a satisfactory level attainment of the relevant subject learning outcomes, demonstrating (as applicable) one or more of the following: • knowledge, understanding and application of fundamental concepts of the field of study • use of routine arguments with acceptable reasoning • adequate communication of information and ideas in terms of the conventions

	of the discipline • ability to apply appropriate skills, techniques and methods with satisfactory levels of precision and accuracy • a combination of correct and incorrect answers
Fail (F) <50%	For performance that does not provide sufficient evidence of attainment of the relevant subject learning outcomes.
Technical Fail (TF)	When minimum performance level requirements for at least one assessment item in the subject as a whole has not been met despite the student achieving at least a satisfactory level of attainment of the subject learning outcomes.

https://www.uow.edu.au/curriculum-transformation/aqc/uowgradedescriptors/index.html

Plagiarism - University's Academic Integrity Policy

The University's policy on acknowledgement practice and plagiarism provides detailed information about how to acknowledge the work of others: http://www.uow.edu.au/about/policy/UOW058648.html

The University's Academic Integrity Policy, Faculty Handbooks and subject guides clearly set out the University's expectation that students submit only their own original work for assessment and avoid plagiarising the work of others or cheating. Re-using any of your own work (either in part or in full) which you have submitted previously for assessment is not permitted without appropriate acknowledgement or without the explicit permission of the Subject Coordinator. Plagiarism can be detected and has led to students being expelled from the University.

The use by students of any website that provides access to essays or other assessment items (sometimes marketed as 'resources'), is extremely unwise. Students who provide an assessment item (or provide access to an assessment item) to others, either directly or indirectly (for example by uploading an assessment item to a website) are considered by the University to be intentionally or recklessly helping other students to cheat. Uploading an assessment task, subject outline or other course materials without express permission of the university is considered academic misconduct and students place themselves at risk of being expelled from the University.

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 Academic Integrity 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 to 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 Academic Integrity Policy as set out in the University

Handbook, the University's online Policy Directory and in Faculty handbooks and subject guides.

Student Academic Complaints Policy (Coursework or Higher Degree Research)

In accordance with the Coursework Student Academic Complaints Policy, a student may request an explanation of a mark for an assessment task or a final grade for a subject consistent with the student's right to appropriate and useful feedback on their performance in an assessment task. Refer to the Coursework Student Academic Complaints Policy for further information
http://www.uow.edu.au/about/policy/UOW058653.html

General Advice

This outline should be considered in conjunction with policy documents available through the University of Wollongong website. Those policies are subject to revision.

Please see the additional documentation provided with this subject outline.