UNSW Course Outline

ZEIT3102 Cryptography - 2024

Published on the 17 Oct 2024

General Course Information

Course Code : ZEIT3102
Year : 2024
Term : Semester 2
Teaching Period : Z2
Is a multi-term course? : No
Faculty : UNSW Canberra
Academic Unit : School of Systems and Computing
Delivery Mode : In Person
Delivery Format : Standard
Delivery Location : UNSW Canberra at ADFA
Campus : UNSW Canberra
Study Level : Undergraduate
Units of Credit : 6

Useful Links

Handbook Class Timetable

Course Details & Outcomes

Course Description

This course provides details of the history, theoretical foundations, and the current state of cryptographic algorithms. Topics may include classical cipher design and analysis; modern private key block cipher design, details, modes of use and analysis; stream ciphers; an introduction to number theory; public key encryption algorithms; digital signatures and hash functions; key management, X.509 certificates and certificate authorities; quantum computing and quantum cryptography.

Course Aims

This course aims to provide students with a broad understanding of the history and development of cryptographic algorithms.

Relationship to Other Courses

N/A

Course Learning Outcomes

Course Learning Outcomes	Australian Computing Society (ACS)
CLO1 : Discuss the history and development of cryptographic algorithms from classical substitution, transposition, and product ciphers to modern private-key block ciphers, public-key encryption, digital signature, and hash algorithms.	• ACS : Cyber Security
CLO2 : Examine classical substitution and transposition ciphers independently and in a group setting.	• ACS : Cyber Security
CLO3 : Use number theories to solve simple number theory problems and apply public-key algorithms for solving real-world applications ranging from simple to moderate difficulty.	• ACS : Cyber Security
CLO4 : Appraise the uses, advantages, and limitations of various categories of cryptographic algorithms and apply the acquired knowledge to solve real-world problems by working independently and in teams through individual and team-based activities.	• ACS : Cyber Security

Course Learning Outcomes	Assessment Item
CLO1 : Discuss the history and development of cryptographic algorithms from classical substitution, transposition, and product ciphers to modern private-key block ciphers, public-key encryption, digital signature, and hash algorithms.	• Classical Cryptology • Assignment 3 • Final Exam
CLO2 : Examine classical substitution and transposition ciphers independently and in a group setting.	• Classical Cryptology • Final Exam
CLO3 : Use number theories to solve simple number theory problems and apply public-key algorithms for solving real-world applications ranging from simple to moderate difficulty.	• Number Theory & Public Key • Assignment 3 • Final Exam
CLO4 : Appraise the uses, advantages, and limitations of various categories of cryptographic algorithms and apply the acquired knowledge to solve real-world problems by working independently and in teams through individual and team-based activities.	• Number Theory & Public Key • Assignment 3 • Final Exam

Learning and Teaching Technologies

Moodle - Learning Management System | Echo 360

Learning and Teaching in this course

Teaching Strategies

Whilst this course is designed to be flexible, it requires you to be highly responsible and self-directed to do well. We have provided a recommended schedule which I lecture to, and which I strongly advise you to follow to maintain a regular pace of work, regardless of whether you are studying on or off-campus. Note that some assignments require interaction with other students, hence the need to keep to the schedule.

I will support your studies by providing a theoretical base for the content via an extensive range of lectures, with their associated notes, and other materials. You will need to demonstrate that you can: apply this knowledge by completing the assessable assignments and exam.

The course will be presented in 13 weekly lessons. The content of this course is presented in 13 weekly lessons, usually requiring some preliminary reading from the text, and then attending or listening to a lecture on the theory content whilst following the supplied lecture overheads. You would then work through some example problems on that content to assess your comprehension, and then complete the assessable activities scheduled for that week.

Students are expected to attend all classes in the course in which they are enrolled. All requests for exemption from attendance or absence should be addressed to the Course Authority and where applicable, be accompanied by a medical certificate.

See University Rules at: https://student.unsw.edu.au/attendance

All teaching materials are in Moodle, unless stated otherwise.

In order to avoid shortcut style learning by guessing exam questions by looking at the solutions of recent exams/final tests, recent exams/final tests are not released. However, the final exam structure and sample questions will be provided to help prepare for the final exam.

Other Professional Outcomes

N/A

Additional Course Information

Use of Generative AI in Assessments

For all assessment tasks, you may use standard editing and referencing software (e.g., Microsoft Office suite, Grammarly, etc.), but not Generative AI. If the use of generative AI such as ChatGPT is detected, it will be regarded as serious academic misconduct and subject to the standard penalties, which may include 00FL, suspension and exclusion. In principle, online tools can only be used for learning purpose or simple calculations such as binary-decimal conversion etc. in the intermediate process. They cannot be used to search for the answers. No online tools could be used in the final exam.

Other Information

Expectations

My expectations of students in this course are that you:

- are mature, independent, self-motivated learners
- will follow up on the set resources and seek additional resources for areas that interest you
- will raise issues or problems as soon as they arise so that action can be taken to address them rather than allowing the situation to deteriorate further
- will sensitively treat the personal and professional information revealed by classmates and will be tolerant of alternative views expressed
- will fully participate in group activities
- will display a questioning attitude and apply critical thinking to the areas under study
- will value the cultural and professional diversity of the class.

You can expect that I will:

- be available for individual inquiries at times to be advised during business hours
- return assessment work within a reasonable period of the close of submissions (normally within two weeks) (noting that all submissions must be received before marking can commence and that marking takes time in order to provide individual feedback to each student)
- provide a variety of key resources, and refer to additional resources of value

be open to alternative viewpoints and appreciate robust discussion

- value the experience and knowledge that each person adds to the group
- listen sensitively to your concerns
- deal fairly and firmly with situations that compromise the integrity of the course or the learning outcomes for people in it.

Assessments

Assessment Structure

Assessment Item	Weight	Relevant Dates	Australian Computing Society (ACS)
Classical Cryptology Assessment Format: Group Short Extension: Yes (3 days)	15%	Start Date: 15/07/2024 11:59 PM Due Date: 13/09/2024 11:59 PM	• ACS : Teamwork concepts and issues • ACS : Cyber Security
Number Theory & Public Key Assessment Format: Individual Short Extension: Yes (3 days)	20%	Start Date: 16/09/2024 12:00 AM Due Date: 04/10/2024 04:16 PM	• ACS : Cyber Security • ACS : Modelling, abstraction, design
Assignment 3 Assessment Format: Group Short Extension: Yes (3 days)	15%	Start Date: 05/10/2024 04:20 PM Due Date: 25/10/2024 04:21 PM	• ACS : Teamwork concepts and issues • ACS : Modelling, abstraction, design • ACS : Cyber Security
Final Exam Assessment Format: Individual	50%	Start Date: To be determined by the student admin Due Date: to be determined by the student admin	• ACS : Cyber Security

Assessment Details

Classical Cryptology

Assessment Overview

Part A (4%)

Choose a cipher of appropriate difficulty and post some encrypted text to the forum for your peers and submit it to the assignment 1 Part A folder.

Part B (11%)

Break some other students' ciphers.

Course Learning Outcomes

- CLO1 : Discuss the history and development of cryptographic algorithms from classical substitution, transposition, and product ciphers to modern private-key block ciphers, public-key encryption, digital signature, and hash algorithms.
- CLO2 : Examine classical substitution and transposition ciphers independently and in a group setting.

Detailed Assessment Description

Part A due date: 11:59pm, Friday the 2nd August, 2024.

Part B due date: 11:59pm, Friday the 13th September, 2024.

Assessment Length

N/A

Assignment submission Turnitin type

This assignment is submitted through Turnitin and students do not see Turnitin similarity reports.

Generative AI Permission Level

Simple Editing Assistance

In completing this assessment, you are permitted to use standard editing and referencing functions in the software you use to complete your assessment. These functions are described below. You must not use any functions that generate or paraphrase passages of text or other media, whether based on your own work or not.
If your Convenor has concerns that your submission contains passages of AI-generated text or media, you may be asked to account for your work. If you are unable to satisfactorily demonstrate your understanding of your submission you may be referred to UNSW Conduct & Integrity Office for investigation for academic misconduct and possible penalties.
For more information on Generative AI and permitted use please see here.

Number Theory & Public Key

Assessment Overview

A series of exercises with classic number theory problems; and to compute “trivial” public key encryption or signature examples.

Course Learning Outcomes

- CLO3 : Use number theories to solve simple number theory problems and apply public-key algorithms for solving real-world applications ranging from simple to moderate difficulty.
- CLO4 : Appraise the uses, advantages, and limitations of various categories of cryptographic algorithms and apply the acquired knowledge to solve real-world problems by working independently and in teams through individual and team-based activities.

Assignment submission Turnitin type

This assignment is submitted through Turnitin and students do not see Turnitin similarity reports.

Generative AI Permission Level

Simple Editing Assistance

In completing this assessment, you are permitted to use standard editing and referencing functions in the software you use to complete your assessment. These functions are described below. You must not use any functions that generate or paraphrase passages of text or other media, whether based on your own work or not.
If your Convenor has concerns that your submission contains passages of AI-generated text or media, you may be asked to account for your work. If you are unable to satisfactorily demonstrate your understanding of your submission you may be referred to UNSW Conduct & Integrity Office for investigation for academic misconduct and possible penalties.
For more information on Generative AI and permitted use please see here.

Assignment 3

Assessment Overview

Certificates and secure email. An exercise in the practical use of crypto for creating a personal public key certificate and sending a secure email.

Course Learning Outcomes

- CLO1 : Discuss the history and development of cryptographic algorithms from classical substitution, transposition, and product ciphers to modern private-key block ciphers, public-key encryption, digital signature, and hash algorithms.
- CLO3 : Use number theories to solve simple number theory problems and apply public-key algorithms for solving real-world applications ranging from simple to moderate difficulty.
- CLO4 : Appraise the uses, advantages, and limitations of various categories of cryptographic algorithms and apply the acquired knowledge to solve real-world problems by working independently and in teams through individual and team-based activities.

Assignment submission Turnitin type

This assignment is submitted through Turnitin and students do not see Turnitin similarity reports.

Generative AI Permission Level

Simple Editing Assistance

In completing this assessment, you are permitted to use standard editing and referencing functions in the software you use to complete your assessment. These functions are described below. You must not use any functions that generate or paraphrase passages of text or other media, whether based on your own work or not.

If your Convenor has concerns that your submission contains passages of AI-generated text or media, you may be asked to account for your work. If you are unable to satisfactorily demonstrate your understanding of your submission you may be referred to UNSW Conduct & Integrity Office for investigation for academic misconduct and possible penalties.

For more information on Generative AI and permitted use please see here.

Final Exam

Assessment Overview

3 hour closed book exam

Course Learning Outcomes

- CLO1 : Discuss the history and development of cryptographic algorithms from classical substitution, transposition, and product ciphers to modern private-key block ciphers, public-key encryption, digital signature, and hash algorithms.
- CLO2 : Examine classical substitution and transposition ciphers independently and in a group setting.
- CLO3 : Use number theories to solve simple number theory problems and apply public-key algorithms for solving real-world applications ranging from simple to moderate difficulty.
- CLO4 : Appraise the uses, advantages, and limitations of various categories of cryptographic algorithms and apply the acquired knowledge to solve real-world problems by working independently and in teams through individual and team-based activities.

Assignment submission Turnitin type

This is not a Turnitin assignment

Generative AI Permission Level

Not Applicable

Generative AI is not considered to be of assistance to you in completing this assessment. If you do use generative AI in completing this assessment, you should attribute its use.

For more information on Generative AI and permitted use please see here.

General Assessment Information

Referencing

Adapt the following ‘Referencing’ statements according to the practice within your School. In line with UNSW Canberra policy, undergraduate students must be instructed to use either the APA 7 or Chicago NB (notes and bibliography) referencing conventions.

In this course, students are required to reference following the APA 7 / Chicago NB referencing style. Information about referencing styles is available at: https://guides.lib.unsw.adfa.edu.au/c.php?g=472948&p=3246720

Academic Integrity and Plagiarism
UNSW has an ongoing commitment to fostering a culture of learning informed by academic integrity. All UNSW staff and students have a responsibility to adhere to this principle of academic integrity. All students are expected to adhere to UNSW's Student Code of Conduct https://www.gs.unsw.edu.au/policy/documents/studentcodepolicy.pdf
Plagiarism undermines academic integrity and is not tolerated at UNSW. It is defined as using the words or ideas of others and passing them off as your own, and can take many forms, from deliberate cheating to accidental copying from a source without acknowledgement. For more information, please refer to the following: https://student.unsw.edu.au/plagiarism

Use of Generative AI in Assessments
For all assessment tasks, you may use standard editing and referencing software (e.g., Microsoft Office suite, Grammarly, etc.), but not Generative AI. If the use of generative AI such as ChatGPT is detected, it will be regarded as serious academic misconduct and subject to the standard penalties, which may include 00FL, suspension and exclusion. In principle, online tools can only be used for learning purpose or simple calculations such as binary-decimal conversion etc. in the intermediate process. They cannot be used to search for the answers. No online tools could be used in the final exam.

Grading Basis

Standard

Requirements to pass course

To pass the course you must get a final mark of 50% or greater in total for the whole course marks. There is no minimum performance for each assessment component.

Course Schedule

Teaching Week/Module	Activity Type	Content
Week 1 : 15 July - 19 July	Lecture	Introduction and History
	Tutorial	
Week 2 : 22 July - 26 July	Lecture	Classical Substitution ciphers
	Tutorial	
Week 3 : 29 July - 2 August	Lecture	Classical transposition & product ciphers
	Tutorial	
Week 4 : 5 August - 9 August	Lecture	Modern block ciphers
	Tutorial	
Week 5 : 12 August - 16 August	Lecture	Number theory. Lecture missing due to Compensation day Friday Timetable. A condensed compensation lecture will be given in the tute session.
	Tutorial	A condensed compensation lecture will be given in this session.
Week 6 : 19 August - 23 August	Lecture	Block cipher design & usage
	Tutorial	
Week 7 : 9 September - 13 September	Lecture	Modern stream ciphers
	Tutorial	
Week 8 : 16 September - 20 September	Lecture	Public key encryption algorithms. Tute missing due to military training on Wed.
Week 9 : 23 September - 27 September	Lecture	Digital signature and hash algorithms
	Tutorial	
Week 10 : 30 September - 4 October	Lecture	Key certificates & management
	Tutorial	
Week 11 : 7 October - 11 October	Lecture	Electronic Mail Security
	Tutorial	
Week 12 : 14 October - 18 October	Lecture	Quantum Cryptography and other applied cryptography technologies Bitcoin, and Blockchain
	Tutorial	
Week 13 : 21 October - 25 October	Lecture	Course review for the exam Exam structure and sample exam questions
	Tutorial	

Attendance Requirements

Students are strongly encouraged to attend all classes and review lecture recordings.

General Schedule Information

See course schedule below.

Course Resources

Prescribed Resources

1. W Stallings, <<Cryptography and Network Security>>, 7/e, Prentice-Hall, 2017, ISBN 10:1-292-15858-1, ISBN 13:978-1-292-15858-7.

2. W Stallings, <<Cryptography and Network Security: Principles and Practice>>, the 8th Edition,

Pearson. ISBN-13978-0136731313, 23 June 2020.

Course Evaluation and Development

One of the key priorities in the 2025 Strategy for UNSW is a drive for academic excellence in education. One of the ways of determining how well UNSW is progressing towards this goal is by listening to our own students. Students will be asked to complete the myExperience survey towards the end of this course.

Students can also provide feedback during the semester via: direct contact with the lecturer, the "On-going Student Feedback" link in Moodle, Student-Staff Liaison Committee meetings in schools, informal feedback conducted by staff, and focus groups. Student opinions really do make a difference. Refer to the Moodle site for this course to see how the feedback from previous students has contributed to the course development.

Important note: Students are reminded that any feedback provided should be constructive and professional and that they are bound by the Student Code of Conduct Policy https://www.gs.unsw.edu.au/policy/documents/studentcodepolicy.pdf

Staff Details

Position	Name	Email	Location	Phone	Availability	Equitable Learning Services Contact	Primary Contact
Convenor	Jiankun H u		Building 15 (IT), Room 106	61251145 159	Prof. Hu is usually available during working hours for a face-to-face consultation. Please email me to make an appointment.	No	Yes

Other Useful Information

Academic Information

Academic Information

Course Evaluation and Development

One of the key priorities in the 2025 Strategy for UNSW is a drive for academic excellence in education. One of the ways of determining how well UNSW is progressing towards this goal is by listening to our own students. Students will be asked to complete the myExperience survey towards the end of each course.

Students can also provide feedback during the semester via: direct contact with the lecturer, the

"On-going Student Feedback" link in Moodle, Student-Staff Liaison Committee meetings in schools, informal feedback conducted by staff, and focus groups (where applicable). Student opinions really do make a difference. Refer to the Moodle site for your course to see how the feedback from previous students has contributed to the course development.

Important note: Students are reminded that any feedback provided should be constructive and professional and that they are bound by the Student Code of Conduct.

https://www.gs.unsw.edu.au/policy/documents/studentcodepolicy.pdf

Equitable Learning Services (ELS)

Students living with neurodivergent, physical and/or mental health conditions or caring for someone with these conditions may be eligible for support through the Equitible Learning Services team. Equitable Learning Services is a free and confidential service that provides practical support to ensure your mental or physical health conditions do not adversely affect your studies.

Our team of dedicated **Equitable Learning Facilitators** (ELFs) are here to assist you through this process. We offer a number of services to make your education at UNSW easier and more equitable.

Further information about ELS for currently enrolled students can be found at: https://www.student.unsw.edu.au/equitable-learning

Academic Honesty and Plagarism

UNSW has an ongoing commitment to fostering a culture of learning informed by academic integrity. All UNSW staff and students have a responsibility to adhere to this principle of academic integrity. All students are expected to adhere to UNSW's Student Code of Conduct. Find relevant information at: Student Code of Conduct (unsw.edu.au)

Plagiarism undermines academic integrity and is not tolerated at UNSW. Itis defined as using the words or ideas of others and passing them off as your own, and can take many forms, from deliberate cheating to accidental copying from a source without acknowledgement.

For more information, please refer to the following:

https://student.unsw.edu.au/plagiarism

Submission of Assessment Tasks

Special Consideration

Special Consideration is the process for assessing and addressing the impact on students of short-term events, that are beyond the control of the student, and that affect performance in a specific assessment task or tasks.

Applications for Special Consideration will be accepted in the following circumstances only:

- Where academic work has been hampered to a substantial degree by illness or other cause;
- The circumstances are unexpected and beyond the student's control;
- The circumstances could not have reasonably been anticipated, avoided or guarded against by the student; and either:

(i) they occurred during a critical study period and was 3 consecutive days or more duration, or a total of 5 days within the critical study period; or

(ii) they prevented the ability to complete, attend or submit an assessment task for a specific date (e.g. final exam, in class test/quiz, in class presentation)

Applications for Special Consideration must be made as soon as practicable after the problem occurs and at the latest within three working days of the assessment or the period covered by the supporting documentation.

By sitting or submitting the assessment task the student is declaring that they are fit to do so and cannot later apply for Special Consideration (UNSW 'fit to sit or submit' requirement).

Sitting, accessing or submitting an assessment task on the scheduled assessment date, after applying for special consideration, renders the special consideration application void.

Find more information about special consideration at: https://www.student.unsw.edu.au/special/consideration/guide

Or apply for special consideration through your MyUNSW portal.

Late Submission of assessment tasks (other than examinations)

UNSW has a standard late submission penalty of:

- 5% per day,

- capped at five days (120 hours) from the assessment deadline, after which a student cannot submit an assessment, and
- no permitted variation.

Students are expected to manage their time to meet deadlines and to request extensions as early as possible before the deadline.

Electronic submission of assessment

Except where the nature of an assessment task precludes its electronic submission, all assessments must be submitted to an electronic repository, approved by UNSW or the Faculty, for archiving and subsequent marking and analysis.

Release of final mark

All marks obtained for assessment items during the session are provisional. The final mark as published by the university following the assessment review group meeting is the only official mark.

School-specific Information

The Leaning Management System

Moodle is the Learning Management System used at UNSW Canberra. All courses have a Moodle site which will become available to students at least one week before the start of semester. Please find all help and documentation (including Blackboard Collaborate) at the Moodle Support page.

UNSW Moodle supports the following web browsers:
• Google Chrome 50+
• Safari 10+
Internet Explorer is not recommended. Addons and Toolbars can affect any browser's performance.

Operating systems recommended are:
• Windows 10,
• Mac OSX Sierra,
• iPad IOS10

Further details:

[Moodle System Requirements]

[Moodle Log In]

If you need further assistance with Moodle:

For enrolment and login issues please contact:
IT Service Centre
Email: itservicecentre@unsw.edu.au
Phone: (02) 9385-1333
International: +61 2 9385 1333

For all other Moodle issues please contact:
External TELT Support
Email: externalteltsupport@unsw.edu.au
Phone: (02) 9385-3331
International: +61 2 938 53331
Opening hours:
Monday – Friday 7:30am – 9:30 pm
Saturday & Sunday 8:30 am – 4:30pm

Study at UNSW Canberra

Study at UNSW Canberra has lots of useful information regarding:

- Where to get help
- Administrative matters
- Getting your passwords set up
- How to log on to Moodle
- Accessing the Library and other areas.

UNSW Canberra Student Hub

For News and Notices, Student Services and Support, Campus Comminity, Quick Links, Important Dates and Upcoming Events

School Contact Information

Deputy Head of School (Education): Dr Erandi Hene Kankanamge
E: e.henekankanamge@adfa.edu.au
T: 02 5114 5157

Syscom Admin Support: syscom@unsw.edu.au

T: 02 5114 5284

Syscom Admin Office: Building 15, Level 1, Room 101 (open 10am to 4pm, Mon to Fri)