UNIVERSITY OF CANBERRA

Advanced Cyber Security

Unit code and version	11907.1
Unit offering option	215756
Study level	Level 3 - Undergraduate Advanced Unit
Credit points	3
Faculty	Faculty of Science and Technology
Discipline	Academic Program Area - Technology
Unit offering details	Semester 2, 2023 , ON-CAMPUS , UC - Canberra, Bruce

Unit convener name and contact details

Unit Convener/Lecturer:

Dr. Mohammad Abualsheikh

Phone: +61 2 62012156

Email: mohammad.abualsheikh@canberra.edu.au

Office: 6C42

Webpage:https://mabualsh.github.io

Administrative contact details

Student Central

Building 1, Level B

Email: Student.Centre@canberra.edu.au

Phone: 1300 301 727

Academic content

Unit description

Recent times have seen a proliferation of digital devices and the subsequent concern for the security of information. This unit introduces students to the basic principles and practices of computer and information security. Focus will be on the software, operating system and network security techniques with detailed analysis of real-world examples. Topics include cryptography, authentication, software and operating system security, network security, mobile security, and legal and ethical issues. In addition, the unit promotes and strengthens important generic skills, such as communication, analysis and inquiry, problem solving, independent and group working, and professionalism and social responsibility.

Learning outcomes

On successful completion of the unit, students will be able to:

1. Describe basic cryptographic functionality, including symmetric ciphers, public key encryption, and digital signatures;

2. Evaluate the security of systems that use cryptography and secure communication techniques;

3. Identify the vulnerability of information systems and justify specific security technologies, settings, and parameters that can improve system security design;

4. Describe existing secure network architectures by applying security technologies such as firewalls, intrusion detection systems, and malicious software scanners; and

5. Discuss how privacy and social engineering issues can impact system design.

Graduate attributes

1. UC graduates are professional

◦ communicate effectively

◦ display initiative and drive, and use their organisation skills to plan and manage their workload

◦ employ up-to-date and relevant knowledge and skills

◦ take pride in their professional and personal integrity

◦ use creativity, critical thinking, analysis and research skills to solve theoretical and real-world problems

◦ work collaboratively as part of a team, negotiate, and resolve conflict

2. UC graduates are global citizens

◦ adopt an informed and balanced approach across professional and international boundaries

◦ behave ethically and sustainably in their professional and personal lives

◦ communicate effectively in diverse cultural and social settings

◦ make creative use of technology in their learning and professional lives

◦ think globally about issues in their profession

◦ understand issues in their profession from the perspective of other cultures

3. UC graduates are lifelong learners

◦ adapt to complexity, ambiguity and change by being flexible and keen to engage with new ideas

◦ be self-aware

◦ evaluate and adopt new technology

◦ reflect on their own practice, updating and adapting their knowledge and skills for continual professional and academic development

Skills development

As students of the University of Canberra, you will develop your critical thinking skills, your ability to solve complex problems, your ability to work with others, your confidence to learn independently, your written communication skills, your spoken communication skills and a number of work-related knowledge and skills.

Prerequisites

11906 Introduction to Cyber Security AND 4483 Software Technology 1

Corequisites

None.

Accreditation

This unit is part of courses accredited by the Australian Computer Society (ACS)

Skills Framework for the Information Age (SFIA) v8

This unit aligns with the following SFIA professional skills:

- Security administration SCAD
- Information security SCTY
- Technical specialism TECH
- Network Support NTAS
- Research RSCH
- Network Planning NTPL
- Network Design NTDS

SFIA skills are defined by levels of responsibility, based on autonomy, influence, complexity, business skills, and knowledge. Although this unit may cover knowledge and skills at higher levels, it is expected that graduates of undergraduate degrees will be capable of operating at Level 3 overall.

Seoul Accord

The UC generic attributes address graduate attributes 1, 6, 7, 9, and 10 of the Seoul Accord. The remaining graduate attributes that are covered in this unit are:

2. Knowledge for Solving Computing Problems

3. Problem Analysis

4. Design/Development of Solution

This unit addresses complex computing problems that have the following characteristics:

- involves wide-ranging or conflicting technical, computing, and other issues;

- has no obvious solution, and requires conceptual thinking and innovative analysis to formulate suitable abstract models;

- a solution requires the use of in-depth computing or domain knowledge and an analytical approach that is based on well-founded principles;

- is a high-level problem possibly including many component parts or sub-problems;

These complex computing problems are assessed in the following assessment item:

- Project

- Assignment

- Quizzes

EA Accreditation

This unit is part of courses accredited by Engineers Australia (EA)

This unit assesses and exposes students to the following Professional Engineer Stage 1 Competencies:

1.1 Comprehensive, theory based understanding – Indicators Assessed: a

1.2 Conceptual understanding – Indicators Assessed: a

1.3 In-depth understanding – Indicators Assessed: a

1.4 Discernment – Indicators Assessed: a, b

1.5 Knowledge – Indicators Assessed: a, Exposed d, f

1.6 Understanding – Indicators Assessed: Exposed a, d, e

2.1 Application of established engineering methods – Indicators Assessed: a, b, c, d, Exposed e, g

2.2 Fluent application of engineering techniques, tools and resources – Indicators Assessed: a, b, Exposed d

2.3 Application of systematic engineering systems and Design Processes– Exposed b

2.4 Application of Systematic Approaches – Indicators Assessed a, Exposed b, c

3.1 Ethical conduct and professional accountability – Indicators Assessed: a, Exposed b

3.2 Effective oral and written communication in professional and lay domains – Indicators Assessed: a, b

3.3 Creative, innovative and pro-active demeanour – Indicators Assessed: a, Exposed c

3.4 Aprofessional Use and Management of Information– Indicators Assessed: a, b, Exposed c

3.5 Orderly Management of Self, and Professional Conduct– Indicators Assessed: a, Exposed b, c, d, e

3.6 Effective Team Membership and Team Leadership – Indicators Assessed b

Timetable of activities

Weeks	Lecture Topic	Due Dates (see Assessment Details For More Information)			
1	Introduction & Overview	-			
2	Cryptography	-			

3	Block Ciphers	Quiz 1
4	Advanced Encryption Standard (AES)	-
5	Public-Key Cryptography	-
6	Data Integrity and Digital Signature	-
7	Key Management	Quiz 2
8	Class free period	-
9	Transport-Level Security	Assignment
10	Secure Network Architectures: Firewall and Malicious Software	-
11	Cloud and the Internet of Things (IoT) Security	Quiz 3
12	Legal and Ethical Aspects	-
13	Unit Review	Project

Unit resources

Required texts

Cryptography and Network Security: Principles and Practice, 8th Edition, Global Edition, by William Stallings

Materials and equipment

Latest version of Microsoft Office: It is available on campus PCs. You can also use Google Docs (https://www.google.com/docs).

Unit website

Each unit you are enrolled in has an online teaching site in the learning management system UCLearn. You access UCLearn through MyUC.

Assessment

Assessment item details

Quiz 1

Due date

Week 3, Friday 11:59pm

Weighting

10%

Assessment details

Three quizzes throughout the semester. The quizzes must be completed individually. Each quiz will open for one week. Each quiz includes various question types, including but not limited to multiple choice, multiple selection, text filling, and matching. More information will be provided on the Canvas teaching website.

Addresses learning outcomes

On successful completion of the unit, students will be able to:

- 1. Describe basic cryptographic functionality, including symmetric ciphers, public key encryption, and digital signatures;

Related graduate attributes

1. UC graduates are professional
   - communicate effectively
   - display initiative and drive, and use their organisation skills to plan and manage their workload
   - use creativity, critical thinking, analysis and research skills to solve theoretical and real-world problems
2. UC graduates are global citizens
   - think globally about issues in their profession
3. UC graduates are lifelong learners
   - evaluate and adopt new technology

Quiz 2

Due date

Week 7, Friday 11:59pm

Weighting

15%

Assessment details

Three quizzes throughout the semester. The quizzes must be completed individually. Each quiz will open for one week. Each quiz includes various question types, including but not limited to multiple choice, multiple selection, text filling, and matching. More information will be provided on the Canvas teaching website.

Addresses learning outcomes

On successful completion of the unit, students will be able to:

- 1. Describe basic cryptographic functionality, including symmetric ciphers, public key encryption, and digital signatures;
- 2. Evaluate the security of systems that use cryptography and secure communication techniques;
- 3. Identify the vulnerability of information systems and justify specific security technologies, settings, and parameters that can improve system security design;

Related graduate attributes

1. UC graduates are professional
    ◦ communicate effectively
    ◦ employ up-to-date and relevant knowledge and skills
    ◦ use creativity, critical thinking, analysis and research skills to solve theoretical and real-world problems
2. UC graduates are global citizens
    ◦ make creative use of technology in their learning and professional lives
3. UC graduates are lifelong learners
    ◦ reflect on their own practice, updating and adapting their knowledge and skills for continual professional and academic development
    ◦ adapt to complexity, ambiguity and change by being flexible and keen to engage with new ideas

Quiz 3

Due date

Week 11, Friday 11:59pm

Weighting

15%

Assessment details

Three quizzes throughout the semester. The quizzes must be completed individually. Each quiz will open for one week. Each quiz includes various question types, including but not limited to multiple choice, multiple selection, text filling, and matching. More information will be provided on the Canvas teaching website.

Addresses learning outcomes

- 3. Identify the vulnerability of information systems and justify specific security technologies, settings, and parameters that can improve system security design;
- 4. Describe existing secure network architectures by applying security technologies such as firewalls, intrusion detection systems, and malicious software scanners; and
- 5. Discuss how privacy and social engineering issues can impact system design.

Related graduate attributes

1. UC graduates are professional
    ◦ communicate effectively
    ◦ display initiative and drive, and use their organisation skills to plan and manage their workload
2. UC graduates are global citizens

- adopt an informed and balanced approach across professional and international boundaries
- behave ethically and sustainably in their professional and personal lives

3. UC graduates are lifelong learners
- reflect on their own practice, updating and adapting their knowledge and skills for continual professional and academic development
- evaluate and adopt new technology
- adapt to complexity, ambiguity and change by being flexible and keen to engage with new ideas

Assignment

Due date

Week 9, Friday 11:59pm

Weighting

25%

Assessment details

The assignment will address advanced topics in cyber security. The assignment must be submitted online via the unit's website. This assignment will be completed in groups of up to three students. All group members must participate significantly in the assignment work. Students must clearly state their individual contributions to the assignment. The group members' marks will be adjusted per their efforts and contributions to the assignment. More information will be provided on the Canvas teaching website.

Addresses learning outcomes

On successful completion of the unit, students will be able to:

- 1. Describe basic cryptographic functionality, including symmetric ciphers, public key encryption, and digital signatures;
- 2. Evaluate the security of systems that use cryptography and secure communication techniques;
- 3. Identify the vulnerability of information systems and justify specific security technologies, settings, and parameters that can improve system security design;

Related graduate attributes

1. UC graduates are professional
- communicate effectively
- employ up-to-date and relevant knowledge and skills
- use creativity, critical thinking, analysis and research skills to solve theoretical and real-world problems
- work collaboratively as part of a team, negotiate, and resolve conflict

2. UC graduates are global citizens
- adopt an informed and balanced approach across professional and international boundaries
- behave ethically and sustainably in their professional and personal lives
- communicate effectively in diverse cultural and social settings
- understand issues in their profession from the perspective of other cultures

3. UC graduates are lifelong learners
- adapt to complexity, ambiguity and change by being flexible and keen to engage with new ideas
- be self-aware

Project

Due date

Week 13, Friday 11:59pm

Weighting

35%

Assessment details

The project will address practical topics in advanced cyber security. The project's outcomes and solution must be submitted online via the unit's website. This project will be completed in groups of up to three students. All group members must participate significantly in the project. Students must clearly state their individual contributions to the project. The group members' marks will be adjusted per their efforts and contributions to the assignment. More information will be provided on the Canvas teaching website.

Addresses learning outcomes

On successful completion of the unit, students will be able to:

- 1. Describe basic cryptographic functionality, including symmetric ciphers, public key encryption, and digital signatures;
- 2. Evaluate the security of systems that use cryptography and secure communication techniques;
- 3. Identify the vulnerability of information systems and justify specific security technologies, settings, and parameters that can improve system security design;
- 4. Describe existing secure network architectures by applying security technologies such as firewalls, intrusion detection systems, and malicious software scanners; and
- 5. Discuss how privacy and social engineering issues can impact system design.

Related graduate attributes

1. UC graduates are professional
   - communicate effectively
   - display initiative and drive, and use their organisation skills to plan and manage their workload
   - employ up-to-date and relevant knowledge and skills
   - take pride in their professional and personal integrity
   - use creativity, critical thinking, analysis and research skills to solve theoretical and real-world problems
   - work collaboratively as part of a team, negotiate, and resolve conflict
2. UC graduates are global citizens
   - adopt an informed and balanced approach across professional and international boundaries
   - behave ethically and sustainably in their professional and personal lives
   - communicate effectively in diverse cultural and social settings
   - make creative use of technology in their learning and professional lives

Submission of assessment items

Group Work

Students must clearly state their individual contributions to group assignments. The marks will be given as per their efforts and contributions to the assignment.

Extensions

Students can apply for an extension to the submission due date for an assessment item due to extenuating, evidenced circumstances (specific details are found in the Assessment Procedures). An extension must be applied for before the due date. Documentary evidence (e.g. medical certificate) will be expected for an extension to be granted, however this will not guarantee that the application will be successful. The Unit Convener or relevant Program Director/Course Convener will decide whether to grant an extension and the length of the extension.

An Assignment Extension form is available from the Student Forms page.

Late submissions

The following late submission period and penalty is applicable to any teaching period commencing after 1 April 2024.

To support the provision of timely feedback to students within the unit, late penalties will apply for summative assessments where late submission is permitted. Late submissions without an approved extension or reasonable adjustment will result in a penalty of a mark reduction of 10% of the maximum available marks for the assessment item per day (or part thereof) up to and including three calendar days. If a student submits more than three calendar days late without an approved extension or reasonable adjustment, the student will be allocated a mark of zero for that assessment, with no feedback provided.

Approval of extensions based on extenuating circumstances will be dependent upon the production of supporting documentation and at the discretion of the unit convener.

For teaching periods commencing prior to 1 April 2024, a late penalty of 5 % of the maximum available marks for the assessment item per day (or part thereof) was applied up to and including seven calendar days. An assignment submitted over 7 days late will not be accepted.

Special assessment requirements

- An aggregate mark of 50% is required to pass the unit.
- The unit convenor reserves the right to question students on any of their submitted work for moderation and academic integrity purposes, which may result in an adjustment to the marks awarded for a specific task.

Supplementary assessment

Refer to the Assessment Policy and Assessment Procedures

Academic integrity

Students have a responsibility to uphold University standards on ethical scholarship. Good scholarship involves building on the work of others and use of others' work must be acknowledged with proper attribution made. Cheating, plagiarism, and falsification of data are dishonest practices that contravene academic values. Refer to the University's Student Charter for more information.

To enhance understanding of academic integrity, all students are expected to complete the Academic Integrity Module (AIM) at least once during their course of study. You can access this module within UCLearn (Canvas) through the 'Academic Integrity and Avoiding Plagiarism' link in the Study Help site.

Use of Text-Matching Software

The University of Canberra uses text-matching software to help students and staff reduce plagiarism and improve understanding of academic integrity. The software matches submitted text in student assignments against material from various sources: the internet, published books and journals, and previously submitted student texts.

Student responsibility

Learner engagement

Activities	Estimated hours
12 lectures x 2 hours each	24
11 tutorials x 2 hours each	22
Weekly study commitment: 12 weeks x 3 hours	36
Assignment and project	48
Quizzes	20
Total	150

Inclusion and engagement

It is strongly recommended that students who need assistance in undertaking the unit because of disability or an ongoing health condition register with the Inclusion and Engagement Office as soon as possible so that reasonable adjustment arrangements can be made.

Participation requirements

Your participation in both class and online activities will enhance your understanding of the unit content and the quality of your assessment work. Lack of participation may result in your inability to satisfactorily pass assessment items.

Withdrawal

If you are planning to withdraw please discuss with your Unit Convener. UC College students must also seek advice from the College.

Required IT skills

Appropriate understanding of mathematics, computer programming, and networking.

Work integrated learning

N/A

Student feedback

All students enrolled in this unit will have opportunities to provide anonymous feedback on the unit through the InterFace Student Experience Questionnaire (ISEQ). The request for your feedback will be posted on your InterFace page at least twice during a teaching period. InterFace can be accessed through MyUC.

Changes to unit based on student feedback

This unit is offered for the first time. Student feedback will be collected during the semester.

Authority of this unit outline

This unit outline must be read in conjunction with the University of Canberra's Policies and Procedures, including the Assessment Policy and associated Procedure. The Assessment Policy and Assessment Procedure include information on matters such as plagiarism, grade descriptors, moderation, feedback, and deferred exams.

Any change to the information contained in the Academic content and Assessment sections of this document, will only be made by the Unit Convener if the written agreement of the Program Director and a majority of students has been obtained; and if written advice of the change is then provided on the teaching site in UCLearn. If this is not possible, written advice of the change must be then forwarded to each student enrolled in the unit at their registered term address. Any individual student who believes themselves to be disadvantaged by a change is encouraged to discuss the matter with the Unit Convener.

Authority Text

Main

Exception – Potential changes to a unit's learning activities and assessment items (Approved Academic Board 2020)

In the event of Australian Government and/or ACT Government directive, such as those requiring physical distancing and restrictions on

movement because of a pandemic, learning activities and/or assessment items in some units may change. These changes will not be updated in the published Unit Outline but will be communicated to students via the unit's UCLearn (Canvas) teaching site. The new learning activities and/or assessment items will continue to meet the unit's learning outcomes, as described in the Unit Outline.

New learning activities and/or assessment items will be available on the unit's UCLearn (Canvas) teaching site. Please contact the Unit Convener with any questions.