This Unit Outline must be read in conjunction with:


c) Any additional information specified in section 6f.

### 1: General Information

1a **Unit title:** Computer and Network Security PG

1b **Unit number:** 6697

1c **Semester and year offered:** Semester 1/2007

1d **Credit point value:** 3

1e **Unit level:** PG

1f **Name of Unit Convener and contact details (including telephone and email):**
Prof. Michael Wagner, T 02 62015477, E michael.wagner@canberra.edu.au

**Name of Unit Moderator and contact details (including telephone and email):**
Dr Wanli Ma, T 02 62012838, E wanli.ma@canberra.edu.au

1g **Administrative contact details (including name, location, telephone and email):**
School Office, Room 11B14, T 02 62012417, E ise@canberra.edu.au
2: Academic Content

2a Unit description and learning outcomes:
Syllabus: Classical encryption, block ciphers, DES, AES, other contemporary symmetric ciphers, key distribution, public-key cryptography, RSA, other public-key cryptosystems, message authentication, hash algorithms, DSS, authentication applications, Kerberos, X.509, email security, PGP/GPG, S/MIME, IP security, system security, intruders, viruses and worms, firewalls.
Learning Outcomes: An understanding of the principles of cryptography and cryptanalysis; an understanding of the principles of security and control, especially in the context of computer systems and networks; an in-depth understanding of vulnerabilities of computer systems and networks and possible counter measures.

2b Prerequisites and/or co-requisites: Computers & Programming G and Computing Mathematics G or approval by unit convener.

3: Delivery of Unit and Timetable

3a Delivery mode: Traditional mode: on campus with weekly lectures, tutorials and practicals. The following weekly schedule is to be seen as a guideline only. The precise week-by-week progress will be determined in response to student understanding of the subject matter and to feedback from the class.

3b Schedule of topics/lectures/tutorials/practicals/field classes by week

<table>
<thead>
<tr>
<th>Week</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Overview, Introduction to PGP and GPG</td>
</tr>
<tr>
<td>2</td>
<td>Mathematical foundations: information theory, complexity theory</td>
</tr>
<tr>
<td>3</td>
<td>Mathematical foundations: fields, number theory</td>
</tr>
<tr>
<td>4</td>
<td>Classical encryption and cryptanalysis</td>
</tr>
<tr>
<td>5</td>
<td>Block ciphers, DES</td>
</tr>
<tr>
<td>6</td>
<td>AES, Blowfish, RC5, RC4, protocols</td>
</tr>
<tr>
<td>7</td>
<td>Public-key cryptography, knapsack, RSA</td>
</tr>
<tr>
<td>8</td>
<td>(Class-free period)</td>
</tr>
<tr>
<td>9</td>
<td>(Class-free period)</td>
</tr>
<tr>
<td>10</td>
<td>Diffie-Hellman, elliptic curves</td>
</tr>
<tr>
<td>11</td>
<td>Authentication, hashing, protocols, Kerberos, X.509</td>
</tr>
<tr>
<td>12</td>
<td>Email security, IP security</td>
</tr>
<tr>
<td>13</td>
<td>Network defences, firewalls</td>
</tr>
<tr>
<td>14</td>
<td>Intrusion detection, forensics</td>
</tr>
<tr>
<td>15</td>
<td>Policy, politics, PKI, review</td>
</tr>
</tbody>
</table>
4: Unit Resources

4a Lists of required texts/readings:
Textbook:

Reference books:

4b Materials and equipment: Computer laboratory, PGP or GPG software

4c Unit website: http://www.ise.canberra.edu.au/un6697/

5: Assessment

5a Assessment overview

<table>
<thead>
<tr>
<th>Assessment Item (including exams held in the exam period)</th>
<th>Due Date of Assignments</th>
<th>Weighting (total to equal 100%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assignment 1 (20 marks)</td>
<td>end of Week 6</td>
<td>20%</td>
</tr>
<tr>
<td>Assignment 2 (20 marks)</td>
<td>end of Week 12</td>
<td>20%</td>
</tr>
<tr>
<td>Final Examination (60 marks)</td>
<td></td>
<td>60%</td>
</tr>
</tbody>
</table>

5b Details of each assessment item
The 2 assignments will comprise factual questions, mathematical problem solving, problem solving by computer programming and/or independent research tasks. Assignments must be encrypted to the lecturer and digitally signed by the student.

In all submitted written work, the author-date or 'Harvard' system, as outlined in the University Library Citation Guide available online at http://www.canberra.edu.au/library/research-gateway/research_help/citation-guide, should be used for referencing. Assignments must be submitted electronically exactly as prescribed. Late assignments or assignment that are not submitted correctly will not be accepted.

5c Special assessment requirements
The final grade is determined according to the following algorithm:
\[
totalMark := Assignment1Mark + Assignment2Mark + examMark;
\]
if totalMark \(\geq\) 85 and examMark \(\geq\) 51 then grade := HD
else if totalMark \(\geq\) 75 and examMark \(\geq\) 45 then grade := DI
else if totalMark \(\geq\) 65 and examMark \(\geq\) 39 then grade := CR
else if totalMark \(\geq\) 50 and examMark \(\geq\) 30 then grade := P
else grade := FAIL
5d **Supplementary assessment**
There is no supplementary assessment.

5e **Text-matching software**
Students’ text-based assignments may be checked for matching text. If so, information about the process will be made available in conjunction with the first of any such assessment items.

6: **Student Responsibility**

6a **Workload**
The amount of time you will need to spend on study in this Unit will depend on a number of factors including your prior knowledge, learning skill level and learning style. Nevertheless, in planning your time commitments you should note that for a 3cp Unit the total notional workload over the fifteen week semester is assumed to be 150 hours or an average of 10 hours per week. These hours include time spent in classes. The total workload for Units of different credit point value should vary proportionally. For example, for a 6cp Unit the total notional workload over a fifteen week semester is assumed to be 300 hours or an average of 20 hours per week.

6b **Special needs**
Students who need assistance in undertaking the unit because of disability or other circumstances should inform their Unit Convener or the Disabilities Office as soon as possible so the necessary arrangements can be made.

6c **Attendance requirements:**
Attendance at lectures, tutorials and practicals is highly recommended.

6d **Required IT skills:** Computer programming skills are a prerequisite to this unit.

6e **Costs:** No costs other than the ordinary costs of textbooks, materials etc.

6f **Additional information:** None

7: **Authority of this Unit Outline**
Any change to the information contained in Section 2 (Academic content), Section 3 (Delivery of Unit and timetable) and Section 5 (Assessment) of this document, will only be made by the Unit Convener if the written agreement of staff and a majority of students has been obtained; and if written advice of the change is then forwarded to each student enrolled in the Unit at their registered term address. Any individual student who believes him/herself to be disadvantaged by a change is encouraged to discuss the matter with the Unit Convener.