<table>
<thead>
<tr>
<th>Code:</th>
<th>IY5502</th>
<th>Course Value:</th>
<th>20</th>
<th>Status:</th>
<th>Core A / Core B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title:</td>
<td>Introduction to Cryptography and Security Mechanisms</td>
<td>Availability:</td>
<td>Autumn term</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prerequisites:</td>
<td>None</td>
<td>Recommended:</td>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Co-ordinator:</td>
<td>Keith Martin</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Course Staff</td>
<td>Keith Martin, Lydia Garms, Ben Curtis</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Aims:         | This course will:  
• introduce the main types of cryptographic mechanism  
• explain how different cryptographic mechanisms provide different security services  
• identify some key issues relating to the management of these services |
| Learning Outcomes: | Successful completion of the course will enable students to:  
• explain exactly what cryptography can be used for.  
• describe several basic cryptographic mechanisms for providing each of the core security services.  
• appreciate the differences between various types of cryptographic mechanism and in which situations they are most usefully employed.  
• identify the issues that need to be addressed when assessing what types of cryptographic mechanism are necessary to "secure" an application.  
• identify the limitations of cryptography and how to support it within a full security architecture. |
| Course Content: | This course is divided into three parts:  
1. Setting the scene:  
• core security services provided by cryptography  
• basic model of a cipher system and use of cryptography  
• historical algorithms  
• security in theory and practice  
2. Cryptographic Toolkit  
• symmetric and public key encryption  
• data integrity  
• entity authentication  
• digital signatures  
• cryptographic protocols  
3. Practical aspects  
• key management  
• cryptographic applications |
| Teaching & Learning Methods: | Eleven three-hour presentations with exercise sheets and handouts  
Weekly mathematics support tutorials; pre-examination tutorial  
Moodle course space with forums and electronic resources  
Two laboratory sessions  
Private study |
| Key Bibliography: | Essential reading:  
Highly recommended:  
N. Ferguson, B. Schneier and T. Kohno, Cryptography Engineering, Wiley (2010). |
| Formative Assessment and Feedback: | Three sets of exercises are accepted for submission with feedback provided. |
| Summative Assessment: | Exam 75% This component is assessed by a two-hour written examination. (1 compulsory question, 2 out of a further 4 questions)  
Coursework 25% The third set of formative exercises is assessed and contributes towards the final mark.  
Deadlines: The written examination will be held in the Summer term. The summative exercise is due in the first week of the Second Semester. |

The information contained in this course outline is correct at the time of publication, but may be subject to change as part of the Department’s policy of continuous improvement and development. Every effort will be made to notify you of any such changes.