Note:

Course content may be changed, term to term, without notice. The information below is provided as a guide for course selection and is not binding in any form, and should not be used to purchase course materials.
COURSE SYLLABUS

CSCI 502
APPLIED CRYPTOGRAPHY

COURSE DESCRIPTION
This course covers topics in modern cryptography with an emphasis on learning how to implement cryptographic protocols using mainstream cryptographic libraries such as OpenSSI.

RATIONALE
This course offers an introduction to the mathematical foundation and primary building blocks of the field of cryptography. In today’s interconnected world, it is more important than ever to keep our data safe. The student will learn what techniques are used to keep information secure and confidential, as well as its limitations. Mathematical rigor is emphasized; however the primary thrust of the course is to enable the student to develop cryptographically secure code.

I. PREREQUISITES
For information regarding prerequisites for this course, please refer to the Academic Course Catalog.

II. REQUIRED RESOURCE PURCHASES
Click on the following link to view the required resource(s) for the term in which you are registered: http://bookstore.mbsdirect.net/liberty.htm

III. ADDITIONAL MATERIALS FOR LEARNING
A. Computer with basic audio/video output equipment
B. Internet access (broadband recommended)
C. Microsoft Office

IV. MEASURABLE LEARNING OUTCOMES
Upon successful completion of this course, the student will be able to:
A. Identify the difference between public key and symmetric key cryptography.
B. Implement basic cryptographic protocols safely and securely.
C. Evaluate a cryptographic protocol.
D. Integrate biblical principles within the field of applied cryptography.

V. COURSE REQUIREMENTS AND ASSIGNMENTS
A. Textbook readings and lecture presentations
B. Course Requirements Checklist
After reading the Course Syllabus and Student Expectations, the student will complete the related checklist found in Module/Week 1.

C. Discussion Board Forums (3)

Discussion boards are collaborative learning experiences. Therefore, the student is required to provide a thread in response to the provided prompt for each forum. Each thread must be at least 300 words and demonstrate course-related knowledge. In addition to the thread, the student is required to reply to 2 other classmates’ threads. Each reply must be at least 150 words. All assertions in the thread and replies must be supported by Reading & Study materials, good examples, thoughtful analysis, and at least 2 scholarly resources.

D. Labs (5)

The student will complete labs associated with the course material. Each lab will have specific instructions for tasks, along with deliverables, to be completed in the virtual lab environment.

E. Quizzes (6)

Each quiz will cover the Reading & Study material for the module/week in which it is assigned. Each quiz will be open-book/open-notes, contain 6 multiple-choice, 6 true/false, and 1 short answer questions, and have a 1-hour time limit.

F. Midterm Exam

The Midterm Exam will cover the Reading & Study material for Modules/Weeks 1–4. The Midterm Exam will be open-book/open-notes, contain 15 true/false and multiple choice questions and 5 short answer questions, and have a 2-hour time limit.

G. Final Exam

The Final Exam will cover all the Reading & Study material for the course. The Final Exam will be open-book/open-notes, contain 20 true/false and multiple choice questions and 7 short answer questions, and have a 2-hour and 45-minute time limit.

VI. Course Grading and Policies

A. Points

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Course Requirements Checklist</td>
<td>10</td>
</tr>
<tr>
<td>Discussion Board Forums (3 at 50 pts ea)</td>
<td>150</td>
</tr>
<tr>
<td>Labs (5 at 100 pts)</td>
<td>500</td>
</tr>
<tr>
<td>Quizzes (6 at 15 pts ea)</td>
<td>90</td>
</tr>
<tr>
<td>Midterm Exam (Modules 1–4)</td>
<td>110</td>
</tr>
<tr>
<td>Final Exam (Modules 1–8)</td>
<td>150</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>1010</td>
</tr>
</tbody>
</table>

B. Scale

CSCI 502 Course Syllabus

C+ = 820–839  C = 780–819  C- = 760–779  F = 0–759

C. Late Assignment Policy

If the student is unable to complete an assignment on time, then he or she must contact the instructor immediately by email.

Assignments that are submitted after the due date without prior approval from the instructor will receive the following deductions:

1. Late assignments submitted within one week of the due date will receive a 10% deduction.

2. Assignments submitted more than one week late will receive a 20% deduction.

3. Assignments submitted two weeks late or after the final date of the class will not be accepted.

4. Late Discussion Board threads or replies will not be accepted.

Special circumstances (e.g. death in the family, personal health issues) will be reviewed by the instructor on a case-by-case basis.

D. Disability Assistance

Students with a documented disability may contact Liberty University Online’s Office of Disability Academic Support (ODAS) at LUODAS@liberty.edu to make arrangements for academic accommodations. Further information can be found at www.liberty.edu/disabilitysupport.
# COURSE SCHEDULE

## CSCI 502


<table>
<thead>
<tr>
<th>MODULE/WEEK</th>
<th>READING &amp; STUDY</th>
<th>ASSIGNMENTS</th>
<th>POINTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ferguson et al.: chs. 1–2 1 presentation</td>
<td>Course Requirements Checklist  Class Introductions  DB Forum 1  Quiz 1</td>
<td>10 0 50 15</td>
</tr>
<tr>
<td>2</td>
<td>Ferguson et al.: chs. 3–4 1 presentation Lab 1 Worksheet</td>
<td>Lab 1: Cryptanalysis  Quiz 2</td>
<td>100 15</td>
</tr>
<tr>
<td>3</td>
<td>Ferguson et al.: chs. 5–7 1 presentation</td>
<td>DB Forum 2  Quiz 3</td>
<td>50 15</td>
</tr>
<tr>
<td>4</td>
<td>Ferguson et al.: chs. 8–9 1 presentation Lab 2 Worksheet</td>
<td>Lab 2: File Encryption Design and Implementation  Midterm Exam</td>
<td>100 110</td>
</tr>
<tr>
<td>5</td>
<td>Ferguson et al.: chs. 10–12 1 presentation Lab 3 Worksheet</td>
<td>Lab 3: Steganography  Quiz 4</td>
<td>100 15</td>
</tr>
<tr>
<td>6</td>
<td>Ferguson et al.: chs. 13–16 1 presentation</td>
<td>DB Forum 3  Quiz 5</td>
<td>50 15</td>
</tr>
<tr>
<td>7</td>
<td>Ferguson et al.: chs. 17–21 1 presentation Lab 4 Worksheet</td>
<td>Lab 4: Cryptographic Protocol Analysis  Quiz 6</td>
<td>100 15</td>
</tr>
<tr>
<td>8</td>
<td>1 presentation Lab 5 Worksheet</td>
<td>Lab 5: Cryptographic Protocol Attack  Final Exam</td>
<td>100 150</td>
</tr>
</tbody>
</table>

DB = Discussion Board

NOTE: Each course module/week begins on Monday morning at 12:00 a.m. (ET) and ends on Sunday night at 11:59 p.m. (ET). The final module/week ends at 11:59 p.m. (ET) on **Friday**.