In this course you will learn the basic concepts related to network security and cryptography. This course can be very fun! If you like playing games, you will enjoy doing the homeworks and hopefully even the exams! So just think of it as a game and let your imagination and creative thinking drive you through.

The main topics covered in this course are as follows:

- Introduction to cryptography and network security
- Symmetric cryptography
  - Classical techniques
  - Modern techniques
  - Confidentiality using symmetric encryption
- Public-key cryptography and hash functions
  - Public-key cryptography and RSA
  - Key management and other public-key cryptosystems
  - Message authentication and Hash functions

This course is mostly self-contained, however, a basic knowledge of number theory, modular arithmetics, and probability theory is required. The number theoretic concepts needed for this class will be reviewed in class when necessary.
This is a tentative schedule and is subject to change. I will fine tune it according to the needs of the class as we go along.

<table>
<thead>
<tr>
<th>Lecture</th>
<th>Topic</th>
<th>Recommended Reading</th>
</tr>
</thead>
</table>
| 1       | Introduction to security concepts: *attacks, services, mechanisms, and models*  
Overview of the course  
Review of Modular Arithmetics | S(1), M(1)  
M(2.4) |
| 2       | Symmetric encryption: *rules of the game, classifications*  
Classical encryption techniques | S(2), P(1) |
| 3       | Block ciphers and DES | S(3) |
| 4       | More on symmetric ciphers | S(6) |
| 5       | Block cipher modes of operation  
Stream ciphers and RC4, **MIDTERM EXAM** | M(7.2.2)  
P(2), S(6.3) |
| 6       | Confidentiality using symmetric encryption | S(7) |
| 7       | Public-key cryptography and RSA | S(9) |
| 8       | Key management and other public key cryptosystems | S(10) |
| 9       | Message Authentication and Hash functions | S(11) |
| 10      | Digital Signatures and Authentication Protocols | S(13) |

S(i) = Chapter i of Stallings  
M(i) = Chapter i of Menezes et. al.  
P(i) = Chapter i of Paar’s notes

**BIBLIOGRAPHY**

**Basic Bibliography**

**Note:** This book has a Student Resources website which contains useful links related to the material covered in the course. Make sure to check it out at http://williamstallings.com/Crypto/Crypto4e.html

**Complementary Bibliography**
Other Recommended Reading

The following lecture notes by Prof. Christof Paar, from Ruhr-Universitat Bochum, can be very useful, especially when you don't have access to the Stallings book.

http://www.box.net/shared/static/76vk1rd49n.pdf

The concepts are very clearly explained and it is easy to read. HIGHLY RECOMMENDED!

EVALUATION METHOD

The students in this course will be evaluated based on their performance in the following activities:

A. Continuous Evaluation

1) homework (15%)
   - distributed weekly
   - in group
   - corrected in class

2) Quizzes (15%)
   - taken weekly
   - in group

3) Project (7.5%)
   - 1 throughout the trimester
   - done individually

4) Course Wiki (7.5%)
   - every lecture has to be summarized in a wiki by one or more groups (to be determined)
   - in group

5) In-class positive and negative bonus points
   - worth 0.1 points each, added (subtracted) directly to (from) the total final grade
   - given (taken) based on in-class behavior and performance
   - does not help passing the course if your final exam is below minimum required

B. Partial and Final Evaluation

1) Exams
   - 1 midterm exam (15%)
   - final exam (40%) - minimum 4.0 required for passing the course
   - September exam – see below for explanation
   - all exams are carried out individually

At the beginning of the trimester, the students are asked to organize themselves into groups of two or three students. These groups will remain together for the duration of the trimester.

Homework:

For every homework assignment, each group is required to turn in one completed assignment which is solved by participation of all members of the group. The homework should be delivered at the beginning of each seminar session. All individuals in the group will get the same grade for every homework.

Occasionally, you may be asked to help with the grading process of the homeworks in seminar classes.
**Quiz:**
For each quiz, **one individual per group** is randomly chosen who will serve as the representative of the group. The chosen individuals will participate in the quiz, and the grade that they get will be assigned to the rest of the members of their group. This way the students are encouraged to work together in the homework and make sure that all individuals in their group equally participate in solving the homework. They will also help each other learn the concepts when solving homework.

**Bonus points:**
The in-class positive bonus points are given to individuals for participation and exceptionally good performance in the class activities. The negative points are given to individuals who show exceptionally disruptive behavior in class, or refuse to participate in certain class activities.

**Exams:**
The **midterm exam** will be taken around the middle of the trimester. It will include some multiple choice and some analytical questions.

The **final exam** will also include both multiple choice and analytical questions. The students will be individually evaluated in the exam. A minimum grade of 4.0 (out of 10) on the final exam is required for passing the course.

The evaluation method is summarized in the following table:

<table>
<thead>
<tr>
<th>Component</th>
<th>Grading impact</th>
<th>Grading agent</th>
<th>Grouping</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Mandatory</td>
<td>Optional</td>
<td>Faculty</td>
<td>Self</td>
</tr>
<tr>
<td>Homework (H)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Quizzes (Q)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Project (P)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Wiki (W)</td>
<td>X</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Midterm Exam (M)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Final Exam (F)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>

\[
Total\ grade = 0.15 \left( H + Q + M + \frac{P+W}{2} \right) + 0.4F + Bonus
\]

Students will pass the course if they meet the minimum of 4.0 required for their final exam grade and their Total grade (as calculated above) is at least 5.0. In other words if:

\[
(F \geq 4.0) \land (Total\ grade \geq 5.0)
\]

Students who have a Total grade greater than 5.0, but don't pass the course because they don't meet the minimum requirement for the final exam grade will receive a final grade of 4.9. Otherwise, the final grade will be equal to the Total grade.

**September exam:** Students who do not pass the course in the end of the trimester have the opportunity to pass the course in September. The final grade in this case is calculated as follows:

\[
Final\ grade = \max \left( 0.15 \left( H + Q + M + \frac{P+W}{2} \right) + 0.4S + Bonus, S \right)
\]

For passing the course in September it is required that your grade in September exam is at least 4 (\( S \geq 4 \)). If Final grade \( \geq 5 \) but \( S < 4 \), the Final grade will be reduced to 4.9.