Instructor: Quang Bach (qtbach@ucsd.edu)

Teaching Assistants:
- Jun Lau (jblau@ucsd.edu)
- Jason O’Neill (jmoneill@ucsd.edu)
- Tian Qiu (tiq011@ucsd.edu)
- Vincent Yu (vey001@ucsd.edu)

Lecture Times: MWF 10:00am – 10:50am in YORK 2622

Discussions: Discussion sections are held weekly on Tuesday
- A01: APM 7421 - 6:00pm–6:50pm (Lau)
- A02: APM 7421 - 7:00pm–7:50pm (O’Neill)
- A03: APM 6402 - 6:00pm–6:50pm (Qiu)
- A04: APM 6402 - 7:00pm–7:50pm (Qiu)
- A05: APM 2402 - 8:00pm–8:50pm (Yu)

Textbook: There is no required textbook for this class.
Optional reference text: *An Introduction to Mathematical Cryptography* by Hoffstein, Pipher and Silverman. The electronic version of this book is available at UCSD library website.

Prerequisites: Upper-division standing with programming experience.

Course Description: This is an introduction to the basic concepts and techniques of modern cryptography. Topics include but not limited to the following:
- Classical cryptography: Caesar, Vigenère, Rectangular Transposition, Mono-alphabetic Substitution, Playfair, ADFGVX, Vernam, Affine, Hill, etc.
- Elementary probability and statistics: random variables, probability, conditional probability, Chi-square test, etc.
- Intro to information theory: entropy, the Huffman code, and perfect secrecy crypto-systems.
- Elementary number theory: Euclidean algorithm, Chinese remainder theorem, Euler phi-function, quadratic residues, and primality testing.
Homework (35% of your course grade): Late homework will not be accepted.

- Homework assignments are posted on the class website under “Assignments” and due at 10:00pm on the indicated date through Gradescope. Before the deadline, you may submit as many copies of your homework paper as you would like; however, only the most recent submission will be considered. There will be eight assignments in total (7 mandatory + 1 optional). If you do not have a submission on Gradescope before the deadline, then you will automatically get a zero for that assignment. Please do not contact the instruction staff to ask for an exception.

The scores and solutions to these problems will be available on Gradescope and TritonED.

Exams (65% of your course grade): There will be two in-class midterms and one in-class final. No textbook, notes, calculator, nor any other electronic devices will be allowed. There will be no make up exam! It is your responsibility to ensure that you do not have a schedule conflict involving the exams.

- The first midterm will be held on Friday, April 20 in lecture, covers topics on classical cryptography.
- The second midterm will be held on Friday, May 11 in lecture, covers topics on probability, number theory, and information theory.
- The final will be held on Monday, June 11, 8:00am – 10:59am. Location TBA. The final exam is cumulative and will cover all materials from the course.

Grade Policy: Your grade will be based on the scores of the homework assignments, two midterms, and the final exam. It will be the maximum of the following two scores:

Score 1 = 35% HW + 15% First Mid + 15% Second Mid + 35% Final
Score 2 = 35% HW + 15% Best Mid + 50% Final

You must pass the final examination (scoring at least 60%) in order to pass the course. Since there is no makeup exam, if you miss one midterm exam for any reason then your course grade will automatically be computed using the second method. The letter grade you receive at the end of the course will be based on the following scale:

<table>
<thead>
<tr>
<th>Grade</th>
<th>97</th>
<th>93</th>
<th>90</th>
<th>87</th>
<th>83</th>
<th>80</th>
<th>75</th>
<th>70</th>
<th>65</th>
</tr>
</thead>
<tbody>
<tr>
<td>A+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Regrade Policy: The scores to all graded materials will be posted on Gradescope and TritonED. If you find a grading error on any graded material, you must immediately request a regrade through Gradescope. All regrade requests must be posted within one week after the score is published. Late requests will not be considered.

Grade Recording Errors: Only the grades posted on Gradescope and TritonED will be computed toward your final score percentage. You must keep all of your graded materials and check these websites frequently to make sure there is no error with your grade. If there is any mistake, you must provide the original graded materials in order for us to make a change.
• It is your responsibility to check your scores and contact your TA before the end of the 10th week of the quarter to resolve recording errors. Questions regarding missing or incorrectly recorded scores will not be considered after the last day of instruction.

Academic Honesty and Attendance Policy: As a student of UC San Diego, you have agreed to abide by the university’s academic honesty policy. Violation of such policy may result in failing the class, suspension, and even expulsion from the university. Students are expected to attend classes regularly. Cell-phone and all electronic devices must be turned off during lecture time, unless being used for taking note. A student who is absent for an excessive amount of times may be dropped from the class.

Important Dates:

- Drop Deadline without an “W” .......................... April 27
- Drop Deadline without an “F” .......................... June 1
- Midterm 1 ..................................................... April 20
- Midterm 2 ..................................................... May 11
- Final Exam .................................................... June 11