

# Syllabus for “Course 1-02-328: Communication and E-Commerce Security”

Kinneret College on the Sea of Galilee  
School of Engineering

Instructor: Michael J. May

Semester 2 of 5770

## 1 Course Details

The course meets **9:00am – 11:00am** on Tuesdays. The Targil for the course is **11:00am – 12:00pm** on Tuesdays.

The course has **2** hours of lecture and **1** hour of Targil. The room for the course is Room 13. The room for the Targil is Computer Room 207 in the Sciences Building.

## 2 Prerequisites

The prerequisites for this course are “Course 1-02-218: Algorithms” and “Course 1-02-284: Logic”, proficiency in programming in C#, and a working knowledge of probability. “Course 1-02-327: Introduction to Computer Networks” is a co-requisite.

## 3 Overview

The main books for the course, as listed below, are *The Foundations of Cryptography* by Oded Goldreich [6] and *Secure Electronic Commerce* by Ford and Baum [4]. Additional, freely available online books will be used throughout the semester to augment the material: *Handbook of Applied Cryptography* by Menzes, van Oorschot, and Vanstone [7], and *Security Engineering* by Ross Anderson [2].

We will be covering some or all of the following topics during the course of the semester (as time allows):

Threats and Security Requirements	Foundations of Modern Cryptography
Encryption and Randomness	Hash Functions
Authentication	Public/Private Key Pairs
Shared Secrets	Decentralized Cryptography
Key Management	Certificates
Network Security	Internet Security
Trust Management	Electronic Banking
Secure Payments	Credit Card Transactions
Telephone and Cellular Payments	Micropayments
Money Transfers	Privacy Protection
Digital Cash	Content Protection
Trusted Third Party Services: Digital Safes, Notaries, Agents	

The course will be built with a focus on the use of cryptographic primitives for the development of secure online services. To this end we will begin with a study of foundational cryptographic techniques, develop an understanding of how they work, and build higher level services and protocols on top of them. To that end, students must be familiar with modular arithmetic, probability, and complexity theory. We will not spend a lot of time on number theory, only to the extent that it is necessary to gain a strong understanding of how cryptographic primitives are properly used.

The course will spend some time discussing business and legal aspects of electronic commerce systems. The material is structured from a Western Common Law point of view as most of the resources we will be using have been developed by scholars in the United States and the United Kingdom (UK). Israeli law differs in some ways and the instructor will make an effort to point out such places as possible.

## 4 Lecture Schedule

The course lectures are structured in the following way. The relevant chapters the Ford and Baum (SEC), Menzes, van Oorschot, and Vanstone (HAC), and Ross Anderson (SE), books are listed in the indicated column. Material not covered well in the books may be supplemented from papers or other sources as shown in the O column which will be updated in the course of the semester.

#	Date	Subject	SEC	HAC	SE	O
1	2 March	E-Commerce, Internet Security, Requirements	1-3		1,19	
2	9 March	Cryptographic Foundations, History	4.2,4.3	1-2	1,5	[1]
3	16 March	Stream vs Block Ciphers, DES	4.3	7.2	5	
4	23 March	Triple-DES, AES, CBC, Hashes		7.2.1-3, 9.1		
5	13 April	Hashes, Diffie-Hellman	4.4	9.1-4, 12.6.1	2	
6	27 April	Public/Private Key Pairs, RSA	4.4,6.2	8	2,3	
7	4 May	Authentication	4.5	10	2,3	
8	11 May	Authentication Defenses	4.5	10	2,3	
9	25 May	Digital Signatures, Key Exchange	4.3	11		
10	1 June	Certificates, PKI	6,8,2, 7	1.11, 13, 19		
11	8 June	Kerberos, One Time Passwords		10	4	
12	15 June	Passwords	5		18	[5, 3]
13	22 June	SSL, SSH				

Since this is an advanced course, students **are expected to come to class having read the material listed above in the lecture schedule**. Students who do not come prepared will find themselves at a significant disadvantage.

## 5 Quizzes

There will be (a maximum of) four in class short quizzes at the beginning of lectures during the course of the semester. The quizzes will take place from 9:00-9:10am. There will be (a maximum of) one quiz during weeks 1-4, one between weeks 5-7, one between weeks 8-10, and one between weeks 11-13. The quiz material will come from the readings assigned for the lecture on which the quiz is given. Students will be told of the upcoming quiz **in class the week before the quiz**.

Students may skip or drop the grade of one of the quizzes without penalty.

Students who arrive in class after 9:10am will not be given the opportunity to take the quiz.

Quizzes are tentatively scheduled to take place on the following dates and on the following material:

#	Date	Topic	Source
1	23 March	Stream/Block Ciphers and Hashes	HAC 1.5-1.9
2	27 April	Diffie-Hellman, Key Establishment	HAC 12
3	11 May	Modular Arithmetic, RSA	HAC 2.4.3, 8.2
4	8 June	Certificates	HAC 13.4.2, 13.6
5	22 June	Passwords and Kerberos	

## 6 Assignments

There will be four assignments during the course of the semester. Some will involve a fairly significant amount of programming.

Each assignment can be done in groups of two (2) or three (3) students.

More details of the assignments will be distributed during the course of the semester.

## 7 Recitation and Laboratory Work

Exercise sessions are a combination of recitation and hands on experimentation sessions. Students may ask questions during the session and the instructor will answer all questions and issues posed.

Some exercise sessions will include a laboratory assignment due at the end of the session. Some will include a laboratory assignment due at the beginning of the following lecture period. Any laboratory work will be based on material covered in previous lecture or readings, not new material. They will not be taken into account in the final grade for the course.

## 8 Attendance

Students are responsible for all material presented in class, recitation, and laboratory sessions, all assigned readings, and all material provided for additional reading out of class.

Attendance of lectures and targil sessions is expected and required for this course. As per College policy, a student who misses 20% or more of the lectures or targil sessions may not be permitted to take the final exam. Attendance will be taken from time to time, but will not be taken directly into consideration in the calculation of the course grade. Students who miss lectures do so at their own risk and expense and will be expected to make up missed material on their own.

Students who know they will be missing two or more lectures due to circumstances beyond their control should inform the instructor as soon as possible before or after the fact to prevent misunderstandings or problems at the end of the semester.

Students who miss a lecture or targil are recommended to contact their classmates to get notes or find out what material was covered. The course syllabus and web page will also indicate the material covered and have the slide sets presented at all lectures.

### 8.1 Decorum

Students who attend lecture are expected to give their full attention to the material. Talking on cellular phones, text messaging, or other disturbing behavior will not be tolerated. Students who need to speak on the phone during lecture time or are expecting urgent messages *must* leave the classroom quietly, conduct their business, and return when they can participate fully in the class.

Students must arrive to lectures **on time, within the first 5 minutes of class**. As per college policy, the instructor reserves the right to expel from the classroom any student who enters more than 5 minutes late for lecture or who is disturbing others.

## 9 Submissions

### 9.1 How to Submit Work

To ensure timely submission of projects and work, students may only submit work via one of the following mechanisms:

- the Telem system
- in person
- via email to the course address: `ise328@gmail`

Materials sent via email to any other address risk being ignored or ungraded without consideration of their merits. Technical issues with the Telem software should be directed to the information technology support staff in Kinneret College who will address them in a timely manner.

### 9.2 Late Submission Policy

Students are expected to be on time with their project submissions and assignments. Each assignment must be turned in by the date it is due.

Each student may turn in **one** assignment up to 7 days late without penalty. Subsequent assignments will be assessed a 20% penalty for up to 4 days late and a 30% penalty for up to 7 days late. After 7 days, any assignment will be accepted with a 60% penalty until January 24, the last day of classes in the semester, until the solutions are posted on line, or any date announced by the instructor.

Students who are called up to Miluim duty will have their assignment deadlines extended in accordance with college policy.

## 10 Cheating

Cheating of any sort will not be tolerated. Student collaboration is encouraged, but within limits as set forth in the college's rules on academic integrity. Any students caught cheating will be immediately referred to the office of the Deacon and may receive a failing grade for the course.

Cheating includes:

- Copying information, content, or verbatim text to answer questions, solutions, or aid in programming projects from other students, internet sites, books (other than the ones listed in the bibliography), other other unaffiliated individuals.
- Copying source code **without attribution** from other students, **web sites**, online repositories, text books, open source programs, or other unaffiliated individuals.
- Other forms of academic misconduct as described on the site: [www.vpul.upenn.edu/osl/acadint.html](http://www.vpul.upenn.edu/osl/acadint.html) or as reasonably assessed by the instructor, program head, or deacon.

## 11 Exams

There will be a single exam at the end of the course. The final exam will be worth **80%** of the course grade and will be scheduled in accordance with the Mador Bechinot of Kinneret College. In accordance the School of Engineering rules, the final will be three (3) hours long, will cover all of the material in the course, and is a required element of the course grade.

## 12 Grading

Final grades will be calculated by combining grades from quizzes, projects, and exams. The grades are weighted as follows:

4%	Quizzes
16%	Assignments
80%	Final Exam

The instructor will not address questions about specific individual grades during the lecture or review sessions. Students may contact the instructor *in person* during office hours or after the lecture/review sessions at the instructor's convenience.

Students may request a regrade for exams or assignment using the regrade request form found on the course web site. The instructor will regrade the entire item submitted, without prejudice to the grade previously assigned to it.

## 13 Books

The following books are used for the class: Anderson [2], Ford and Baum [4], Goldreich [6], and Menzes, van Oorschot, and Vanstone [7].

The library has copies of the books listed, but students are encouraged, to purchase the books as needed. Some of the above books are available freely online as indicated in the bibliography.

A bibliography of the books and articles used in the course of the semester is shown below. Two of the books and all of the articles are freely available on line at URLs shown in the bibliography below.

## 14 Contact Information

Instructor: Michael J. May  
Email: [mjmay@kinneret.ac.il](mailto:mjmay@kinneret.ac.il)  
Office Hour: Wednesdays 11:00am – 12:00pm or by appointment

## References

- [1] Ross Anderson. Why cryptosystems fail. In *CCS '93: Proceedings of the 1st ACM conference on Computer and Communications Security*, pages 215–227, New York, NY, USA, 1993. ACM.
- [2] Ross Anderson. *Security Engineering: A Guide for Building Dependable Systems*. Wiley, 2nd edition, 2008. [www.cl.cam.ac.uk/~rja14/book.html](http://www.cl.cam.ac.uk/~rja14/book.html).
- [3] Rachna Dhamija, J. D. Tygar, and Marti Hearst. Why phishing works. In *CHI '06: Proceedings of the SIGCHI conference on Human Factors in Computing Systems*, pages 581–590, New York, NY, USA, 2006. ACM.
- [4] Warwick Ford and Michael S. Baum. *Secure Electronic Commerce*. Prentice-Hall, 2nd edition, 2001.
- [5] Kevin Fu, Emil Sit, Kendra Smith, and Nick Feamster. Do's and donts of client authentication on the web. Technical Report 818, MIT, 2001. [pdos.csail.mit.edu/papers/webauth:sec10.pdf](http://pdos.csail.mit.edu/papers/webauth:sec10.pdf).
- [6] Oded Goldreich. *The Foundations of Cryptography*, volume 1 (Basic Tools). Cambridge University Press, 1st edition, 2001.
- [7] Alfred J. Menzes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996. [www.cacr.math.uwaterloo.ca/hac/](http://www.cacr.math.uwaterloo.ca/hac/).