3205 Applied Cryptography and Network Security
(Abbreviated and Preliminary Description)

Zvi M. Kedem

Updated April 9, 2015

Contents

1 Administrative Details .................................................. 1
  1.1 General Information .............................................. 1
  1.1.1 Instructor ...................................................... 1
      1.1.1.1 Email .................................................... 1

2 Course Description ................................................... 2
  2.1 Short Description ................................................ 2
  2.2 Goals and Material Covered ..................................... 3
  2.3 Prerequisites ..................................................... 3
  2.4 Assignments, Exams, and Grading ............................... 3
      2.4.1 Homework .................................................... 3
      2.4.2 Midterm ...................................................... 4
      2.4.3 Project ....................................................... 4
          2.4.3.1 Option 1: Implementing a restricted version of RSA and some protocols based on it 4
          2.4.3.2 Option 2: Writing a survey or a research paper ................................. 4
  2.4.4 Grading ......................................................... 4

1 Administrative Details

1.1 General Information

1.1.1 Instructor


1.1.1.1 Email

To make email communications as efficient as possible, please follow the following procedures for all course-related emails:
1. If your email is not confidential, please use http://bit.ly/kedemzm (no security guarantees are made for this email). Choose the class as “What is this about” and do not add a website or a bio.

2. You can and may always use NYU email, if you prefer: mailto:zk1@nyu.edu.

   Please put in the Subject line the course number followed by an informative phrase summarizing the contents of your email. It is even better if your email can be fully stated in a reasonable-length subject without a body, so it can be quickly seen and responded to. And the best subject line is phrased as a request for me to do something specific, if applicable.

   Please

   (a) If you write on a new topic, do not do that by replying to an irrelevant old email.

   (b) Do not include irrelevant material from old email messages.

   Email with a subject not including the course number may be automatically classified as low priority and may even be filtered out and not seen.

If your email requires a response from me, I will respond quickly and generally no later than the next business day during the semester if your email follows the format described above.

2 Course Description

2.1 Short Description

When you reach a web page that claims to be your Amazon’s account page by reaching a URL such as https://www.amazon.com/gp/css/homepage.html/ref=gno_yam_ya and give it your credit card number, how do you know that

1. you are indeed talking to amazon.com and not some other web site, or somebody else like your ISP, which told your browser that it is amazon.com, and

2. that nobody else between you and www.amazon.com can “overhear” your credit card number?

Amazon presumably can authenticate you (knows that you are the person you claim to be) because you have an account at Amazon and you have input your password. But Amazon does not have an account with you and she has not supplied any passwords.

There is a perhaps strange asymmetry here: Amazon needs your password to trust you, but you trust Amazon without her having established a password to trust her.

There is possibly a small padlock on the web page or a “similar reassurance” that you have to trust, or else you cannot buy books from Amazon. But what is actually happening “under the hood”?

At the end of this course you will know that and will also have a useful understanding of most fundamental cryptographically-based mechanisms used in currently deployed systems, with focus on those used on the Web. You will also understand, and know how to use, some of the freely available, open-source packages for securing information on your personal computer and email exchanges with others. You may find them useful for your own future use if you are concerned by privacy and security.
2.2 Goals and Material Covered

The main goal of the course will be to understand and deploy

1. cryptographic algorithms that are the key components for security and privacy mechanisms, and
2. representative protocols and applications based on them.

If you are interested in really understanding the underpinnings of current privacy/security cryptography-based mechanisms, this course may be of interest to you. If you are interested in cryptography per se (more mathematics and theory focus), or privacy/security mechanisms protocols with the cryptography-based components being magic black boxes that work (more systems focus), this will be of lesser interest to you.

The material covered is likely to include the following:

1. Fundamentals, such as basic complexity-related concepts (one way functions), basic concepts of probability and information theory, basic properties of integers, and related algorithms.
2. Cryptographic tools, such as public/private encryption (RSA and Diffie/Hellman), symmetric encryption (DES and AES), secure hash functions, digital signatures, authentication, zero-knowledge proofs, and secret sharing.
3. Example protocols and applications, some selected from Kerberos, Digital Certificates, PGP/GnuPG, S/MIME, secure shell, password maintenance, IP security, SSL and TSL, WiFi security, digital cash, and VeraCrypt.

We will use the following resources:

1. A detailed set of course notes that I will prepare and post.

2.3 Prerequisites

1. A course in algorithms (undergraduate or graduate) or permission of the instructor.
2. The ability to write short to medium length programs in a programming language of your choosing.

2.4 Assignments, Exams, and Grading

Come to the classes. Although attendance will not be taken, this is important for understanding the material. Although I provide very extensive written material it is not a substitute for coming to the classes. Please do not register for the class if you are not sure to attend the class regularly.

Formally, class attendance will not count towards the grade.

2.4.1 Homework

Do the homework. It may include reading assignments, written assignments, and relatively short programs.
2.4.2 Midterm

Take the midterm exam. It will take place in class on March 30. Material will be announced later, once we know what is covered before the midterm.

The exam will be closed books, but you may bring one letter-size (8.5” × 11”) or A4 (210 mm × 297 mm) sheet of paper on both sides of which you may write (not print or copy) any notes you like. You will write your name on top of the sheet on both sides. You will hand in the sheet with your answers.

2.4.3 Project

Tentatively, the project will be due one week before the last class day.

You will have a choice of two projects. The default option is described in Section 2.4.3.1. If you decide on the option described in Section 2.4.3.2, you need to tell me that as early as possible, but not later than by the first class day after the spring break. While this option may still be accommodated if you choose it later, this is not guaranteed.

2.4.3.1 Option 1: Implementing a restricted version of RSA and some protocols based on it

It will be a programming project with an interview about it later. Its goal is for you to put together many of the ideas and algorithms studied in the course. In effect, you will implement a simplified, partial version of the algorithmic (not system) infrastructure used for SSL/TLS. You may write it in any programming language you like. You will be individually interviewed for approximately 30 minutes about your submission.

If you are considering taking the course and would like to see the preliminary description of the project, please email me in a way specified in Section 1.1.1.1.

2.4.3.2 Option 2: Writing a survey or a research paper

You will have to propose a topic for an original paper and get my approval for the topic, the scope, and the format.

2.4.4 Grading

The percentage of the course grade for each of the three components: Homework, Midterm, and Project will be decided after the class starts and before the “drop date.”