Teaching Portfolio

Steve Matsumoto

Contents

Teaching Statement

During my undergraduate career I was very fortunate to experience many classes with truly amazing professors who exhibited many highly effective teaching strategies. Learning under these strategies greatly shaped my own teaching, and taught me an important lesson: at its core, effective teaching is about relationships, both with the students and with the material. In particular, it is the teachers who are caring, adaptive, enthusiastic, and broad who can best foster deep, meaningful relationships with their students and with their subjects, and therefore I strive to make these qualities a central part of my teaching.

First and foremost, successful teachers are caring. Students who know that their instructor cares about their learning and well-being are often motivated to seek help and push themselves based on that fact alone. One way I show that I care about my students is to learn all of their names in the first week of classes. Because some students look very different from the photos the university has on file, I bring a camera to the first class meeting and take their pictures. I then make flashcards and study them every day until I learn their names. When I address students by name in the second week of classes, many students are impressed and express their appreciation when I collect feedback. Though it is a small gesture, I have found it to be highly motivating to students.

I also have the opportunity to demonstrate a caring spirit when I help students with their questions on the material. For example, this past semester, one of my students emailed me in tears because he was having great difficulty with the material. Though I was busy and dealing with an important personal issue at the time, I sympathized with him and scheduled a meeting with him outside of class to answer his questions. He was very appreciative, and ended up doing extremely well in the course. I believe that moments like these have a huge impact on students' motivation.

Second, successful teachers are adaptive. I have incorporated adaptiveness into my own teaching by carefully preparing each day's activities for each section of students. This past semester, I led recitations for a section of about five very strong students, a section of twenty very inquisitive students, and a section of about fifteen very quiet students. I approached each of these sections very differently, exploring alternative problem-solving methods in the first section while taking many more questions in the second. As I got to know each student better, I also began to approach each student's questions differently, allowing me to more effectively handle mixes of the above types of students in a single section. I believe that such adaptability, while certainly more difficult on the instructor, providers students with an effective educational environment tailored to their specific learning styles.

I also adapt my teaching and courses over the long term, carefully collecting students' feedback both during and at the end of the course. My students' feedback played a key part in my decision to eliminate recitation quizzes and replace them with additional practice problems in my recitation sections this past semester. This feedback affects my courses at a more fundamental level, fixing inefficiencies that cannot be solved by a quick, improvised change in teaching. I believe that this long-term adaptiveness is just as important as short-term adaptiveness, affecting the design of my courses rather than just the implementation.

Third, successful teachers are enthusiastic. An instructor's enthusiasm can often be contagious, motivating students to share in the same passion for the subject material. The excitement with which I approach problems and concepts motivates me to incorporate jokes and other "fun" elements into my teaching, making my classes more enjoyable for students. For example, in one of my recitations I decided to take my students outside, where we solved math problems with chalk on the sidewalk. The students were able to enjoy the sun and see how their classmates were approaching the same problems, and many of them wrote how much they appreciated this in their mid-semester teaching evaluations.

Additionally, I try to convey my enthusiasm by leading students to discover the biggest key ideas in my courses rather than simply teaching them. For example, I once spent most of a recitation meeting asking students to solve a problem that they had not been taught to solve. Though they struggled to solve the problem on their own, this approach allowed them to better understand why the solution worked. Furthermore, the students that did manage to solve the problem were able to work on the additional challenge of developing a general method for solving similar problems. This approach not only allows students to be creative in solving problems, but also primes them to learn concepts which may be taught in the near future.

Finally, successful teachers are broad. Though depth in the subject material is equally important for teachers, I believe that breadth is a key factor in making the material accessible to students. When I design courses, I try to demonstrate this harmony of breadth and depth by examining subject material through a variety of activities and perspectives. In my own field of computer security, this approach is particularly effective because security vulnerabilities can occur in both the design and the implementation of systems, allowing students to see how systems are exploited through both theoretical and hands-on approaches. For example, my introductory security course has a password-cracking lab in which students analyze the theoretical weaknesses of various hash functions and apply these analyses to design fast, efficient password-cracking algorithms.

In addition, I seek to engage my students with my field in the context of other academic disciplines. With the increasing ubiquity of computing devices in our everyday lives, computer security has become more intertwined with other fields, particularly economics, politics, and psychology. Criminals are compromising financial systems with greater frequency because of the economic motivations, and governments are facing great challenges in regulating the use of the Internet. By analyzing these connections, students can take the lessons they learn in my courses with them, even if they do not pursue further studies in security.

Good teaching, of course, has many other attributes, but caring, adaptability, enthusiasm, and breadth have made the biggest difference in my own teaching and learning. In my future teaching endeavors, I hope to further refine my teaching through continual reflection on both my own and others' teaching strategies. In doing so, I hope to keep providing an effective learning environment for my students, helping them discover the great insights and wondrous applications of my field.

Summary of Teaching Activities

TA Responsibilities

Recitation TA for 18-202: Mathematical Foundations for Electrical Engineering. Instructors: Tom Sullivan, Yi Luo. Department of Electrical and Computer Engineering, Carnegie Mellon University, Pittsburgh, PA. Fall 2013.

- Leading three weekly recitation students (93 students total)
- Writing solution sets for assigned homework problems
- Preparing practice problems for students to work on during recitations
- Guiding students one-on-one during weekly office hours
- Helping to design and grade exams

Recitation TA for 18-202: Mathematical Foundations for Electrical Engineering. Instructor: Xin Li. Department of Electrical and Computer Engineering, Carnegie Mellon University, Pittsburgh, PA. Spring 2013.

- Leading three weekly recitation students (80 students total)
- Preparing practice problems for students to work on during recitations
- Guiding students one-on-one during weekly office hours
- Helping to design and grade exams

Educational Outreach

CSCI 182: Robotics Outreach Seminar. Instructor: Zach Dodds. Department of Computer Science, Harvey Mudd College, Spring 2012.

- Designing a series of hands-on robotics lessons for middle-school students
- Teaching the above lessons to students at the Fremont Academy of Engineering and Design in Pomona, CA

Science Bus. Harvey Mudd College, Fall 2009.

- Teaching weekly science lessons to students at Montvue Elementary School in Pomona, CA

Teaching Development

Future Faculty Program. Eberly Center for Teaching Excellence, Carnegie Mellon University, Pittsburgh, PA. Fall 2012-present.

- See Future Faculty Program Completion Letter on p. 31 for details.

Evaluation Data: Mathematical Foundations of Electrical Engineering, Fall 2013

Here I present selected TA evaluation data collected at the conclusion of Fall 2013 for 18-202: Mathematical Foundations for Electrical Engineering. This teaching assistantship was carried out for the Electrical and Computer Engineering Department at Carnegie Mellon University. These do not represent the entirety of the data I collected, but rather highlight a sample of opinions my students had after a semester-long course with me.

Numerical Ratings

Students were given evaluation forms at the end of the semester and asked to respond to each of the statements below using the following 5-point scale: 1 (strongly disagree), 2 (disagree), 3 (neutral), 4 (agree), and 5 (strongly agree).

Responses were collected in three sections: A (6 students), B (21 students), and C (17 students), for a total of 44 student responses. (There were 93 students enrolled in the class.) The distribution of ratings was similar across all sections, so only the averages across all sections are reported here.

Statement	**Average Rating**
Explained complex numbers well	4.86
Explained circuit problems well	4.49
Explained differential and difference equations well	4.71
Explained matrices, eigenvalues, and eigenvectors well	4.76
Explained multivariable calculus well	4.31
Displayed an interest in my learning	4.81
Answered questions well	4.91
Was approachable	4.91
Showed respect for all students	4.95
Exhibited excellent teaching overall	4.86

Written Comments

Below are some selected responses to the question, "What is effective about Steve's teaching?" collected from students at the end of the semester.

- Learning everyone's name was the best start to the recitation and showed you cared.
- I also liked that he explained how answers to problems were derived but also gave us the quick way to solve problems.
- I really felt like Steve put a lot of time into the class, which made me want to work harder.
- He paced recitation well, and I never felt "stupid" asking a question, because he was kind and receptive always.
- He was very good about explaining why things worked, not just how they worked.

Sample Solution Set: Mathematical Foundations of Electrical Engineering, Fall 2013

In my experience I have found that many students view solution sets to assigned homework as the first step in getting help for problems they may have struggled to solve. Therefore, I strive to make each of my solution sets clear and detailed. My hope is to answer students' most common questions through these solutions so that I can focus on more in-depth questions during office hours.

For the following problem set, which many students described as one of the most difficult of the semester, I explore many of the finer details of solving second-order differential equations using step-by-step explanations. By explaining my thought process in solving each problem, I focus on the approach to these problems much more than on the final solutions themselves.

18-202: Mathematical Foundations of Electrical Engineering, Fall 2013
Homework 4, due Monday, October 7

1 Section 2.7 Problem 11 [12 Points]

Note: for problems 1-4, do the following:

(a) **[4 Points]** Solve the equation for the particular solution, $y_p(x)$, using the differential equation and right-hand side driving function.

(b) **[4 Points]** Solve the equation for the homogeneous solution, $y_h(x)$, using the differential equation and initial conditions (remember, the initial conditions to use for the homogeneous solution are derived by subtracting the initial condition contribution from the particular solution found in part (a) from the given initial conditions). Sum $y_p(x)$ and $y_h(x)$ to get the total solution, $y(x)$.

(c) **[4 Points]** Check your result, by differentiating your result for $y(x)$ and substituting it back into the differential equation and showing that it solves the equation. Check the initial conditions too.

Solve the initial value problem. Show each step of your calculation in detail.

$$y'' + 3y = 18x^2,\ y(0) = -3,\ y'(0) = 0$$

Solution.

(a) We let $y_p(x) = ax^2 + bx + c$. Then,

$$\begin{aligned} y_p'(x) &= 2ax + b \\ y_p''(x) &= 2a \end{aligned}$$

Substituting into the equation, we have

$$2a + 3(ax^2 + bx + c) = 3ax^2 + 3bx + 2a + 3c = 18x^2$$

which gives us the system of equations

$$\begin{aligned} 3a &= 18 \\ 3b &= 0 \\ 2a + 3c &= 0 \end{aligned}$$

This has the solution $a = 6$, $b = 0$, and $c = -4$, so $y_p(x) = 6x^2 - 4$.

We can also see that $y_p(0) = -4$ and $y_p'(0) = 0$.

(b) We solve the characteristic equation:

$$\begin{aligned} \lambda^2 + 3 &= 0 \\ \lambda &= \frac{\pm\sqrt{-12}}{2} = \pm j\sqrt{3}. \end{aligned}$$

Therefore, the homogeneous solution is of the form $y_h(x) = k_1 \cos(x\sqrt{3}) + k_2 \sin(x\sqrt{3})$.

We know from our initial conditions and from the contribution of the particular solution at $x = 0$ that $y_h(0) = 1$ and $y_h'(0) = 0$. Since $y_h(0) = k_1$ and $y_h'(0) = k_2\sqrt{3}$, we know that $k_1 = 1$ and $k_2 = 0$. Therefore, our solution is

$$y(x) = \cos(x\sqrt{3}) + 6x^2 - 4.$$

(c) We take the first and second derivatives of y:

$$\begin{aligned} y'(x) &= -\sqrt{3}\sin(x\sqrt{3}) + 12x \\ y''(x) &= -3\cos(x\sqrt{3}) + 12 \end{aligned}$$

Substituting this into the equation, we get

$$\begin{aligned} -3\cos(x\sqrt{3}) + 12 + 3(\cos(x\sqrt{3}) + 6x^2 - 4) &= -3\cos(x\sqrt{3}) + 12 + 3\cos(x\sqrt{3}) + 18x^2 - 12 \\ &= 18x^2. \end{aligned}$$

2 Section 2.7 Problem 12 [12 Points]

Solve the initial value problem. Show each step of your calculation in detail.

$$y'' + 4y = -12\sin 2x,\ \ y(0) = 1.8,\ \ y'(0) = 5.0$$

Solution.

(a) We can see that out characteristic equation will be $\lambda^2 + 4 = 0$, resulting in roots of $\pm 2j$. Therefore, we must use the modification rule to find the particular solution. Then

$$\begin{aligned}
y_p(x) &= Kx\cos(2x) + Mx\sin(2x)\\
y_p'(x) &= K\cos(2x) - 2Kx\sin(2x) + M\sin(2x) + 2Mx\cos(2x)\\
y_p''(x) &= -2K\sin(2x) - 2K\sin(2x) - 4Kx\cos(2x) + 2M\cos(2x) + 2M\cos(2x) - 4Mx\sin(2x)\\
&= (-4Kx + 4M)\cos(2x) + (-4K - 4Mx)\sin(2x)
\end{aligned}$$

and so we have the following system of equations:

$$\begin{aligned}
4M &= 0\\
-4K &= -12
\end{aligned}$$

This has the solution $K = 3$, $M = 0$. Therefore, $y_p(x) = 3x\cos(2x)$. The initial condition contribution of the particular solution is

$$\begin{aligned}
y_p(0) &= 0\\
y_p'(0) &= 3.
\end{aligned}$$

(b) As we saw above, the roots of our characteristic equation are $\pm 2j$. Therefore, our homogeneous solution has the form $y_h(x) = k_1\cos(2x) + k_2\sin(2x)$. Based on the initial condition contribution of the particular solution,

$$\begin{aligned}
y_h(0) &= 1.8\\
y_h'(0) &= 2.
\end{aligned}$$

Thus we have the system of equations

$$\begin{aligned}
k_1 &= 1.8\\
2k_2 &= 2
\end{aligned}$$

and therefore $k_1 = 1.8$ and $k_2 = 1$. Thus our solution is

$$y(x) = 1.8\cos(2x) + \sin(2x) + 3x\cos(2x).$$

(c) Taking derivatives, we have

$$\begin{aligned}
y'(x) &= -3.6\sin(2x) + 2\cos(2x) + 3\cos(2x) - 6x\sin(2x)\\
&= -3.6\sin(2x) + 5\cos(2x) - 6x\sin(2x)\\
y''(x) &= -7.2\cos(2x) - 10\sin(2x) - 6\sin(2x) - 12x\cos(2x)\\
&= -7.2\cos(2x) - 16\sin(2x) - 12x\cos(2x)
\end{aligned}$$

Substituting into our equation, we get

$$\begin{aligned}
-7.2\cos(2x) - 16\sin(2x) - 12x\cos(2x) + 4(1.8\cos(2x) + \sin(2x) + 3x\cos(2x) \\
&= -7.2\cos(2x) - 16\sin(2x) - 12x\cos(2x) + 7.2\cos(2x) + 4\sin(2x) + 12x\cos(2x) \\
&= -12\sin(2x).
\end{aligned}$$

3 Chapter 2 Review Problem 19 [12 Points]

Solve the problem, showing the details of your work. Sketch or graph the solution.

$$y'' + 16y = 17e^x, \; y(0) = 6, \; y'(0) = -2$$

Solution.

(a) Let $y_p(x) = ke^x$. Then, $y_p'(x) = y_p''(x) = ke^x$. Substituting into our equation, we have

$$17ke^x = 17e^x$$

and thus $k = 1$. Therefore, $y_p(x) = e^x$. Our initial condition contribution is therefore

$$y_p(0) = 1$$
$$y_p'(0) = 1$$

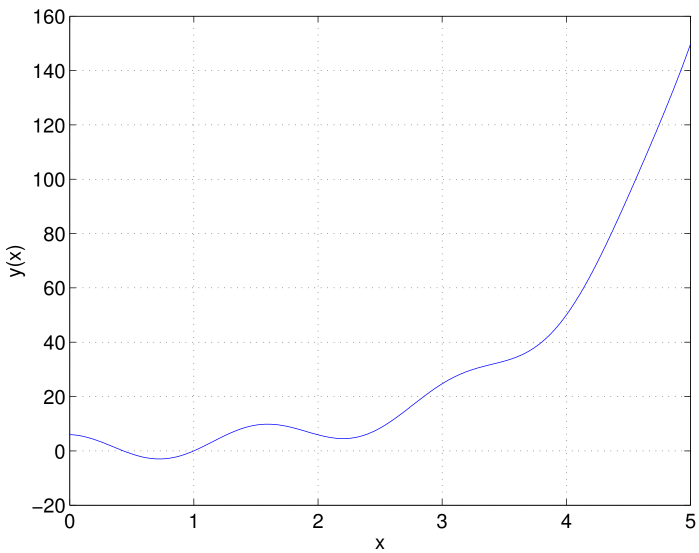


Figure 1: Graph of solution to Problem 3.

(b) Since our characteristic equation is $\lambda^2 + 16 = 0$, our roots are $\lambda = \pm 4j$. Therefore our homogeneous solution takes the form $y_h(x) = k_1 \cos(4x) + k_2 \sin(4x)$. Our initial condition contribution from $y_h(x)$ is

$$y_h(0) = 5$$
$$y_h'(0) = -3.$$

Therefore, we have the system of equations

$$k_1 = 5$$
$$4k_2 = -3$$

which has the solutions $k_1 = 5$, $k_2 = -0.75$. Therefore, our solution is

$$y(x) = 5\cos(4x) - 0.75\sin(4x) + e^x.$$

(c) Taking derivatives, we have

$$\begin{aligned} y'(x) &= -20\sin(4x) - 3\cos(4x) + e^x \\ y''(x) &= -80\cos(4x) + 12\sin(4x) + e^x. \end{aligned}$$

Substituting into the equation, we get

$$\begin{aligned} &-80\cos(4x) + 12\sin(4x) + e^x + 16(5\cos(4x) - 0.75\sin(4x) + e^x) \\ &\qquad = -80\cos(4x) + 12\sin(4x) + e^x + 80\cos(4x) - 12\sin(4x) + 16e^x \\ &\qquad = 17e^x. \end{aligned}$$

4 Chapter 2 Review Problem 19 [12 Points]

Solve the problem, showing the details of your work. Sketch or graph the solution.

$$y'' - 3y' + 2y = 10\sin x,\ y(0) = 1,\ y'(0) = -6$$

Solution.

(a) We can solve for the particular solution using the system of equations

$$(c - a\omega^2)K + b\omega M = d$$
$$-b\omega K + (c - a\omega^2)M = e$$

where $a = 1$, $b = -3$, $c = 2$, $d = 0$, $e = 10$, and $\omega = 1$. This gives us the system

$$K - 3M = 0$$
$$3K + M = 10$$

which has the solution $K = 3$, $M = 1$. Therefore $y_p(x) = 3\cos x + \sin x$. The initial condition contribution is

$$y_p(0) = 3$$
$$y_p'(0) = 1$$

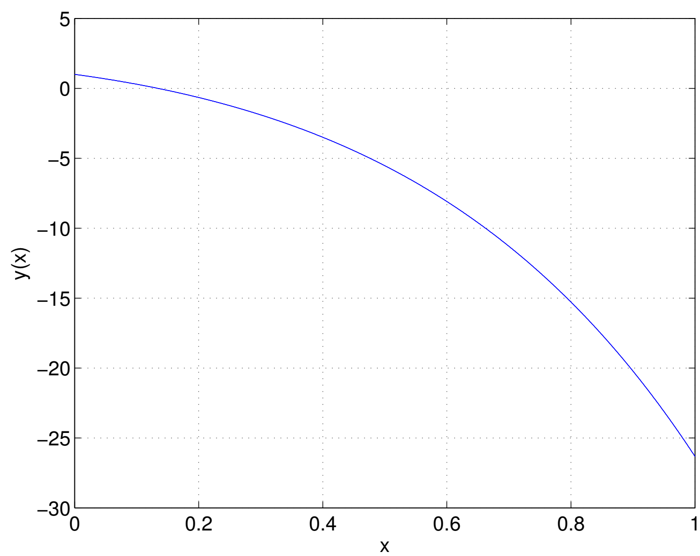


Figure 2: Graph of solution to Problem 4.

(b) Our characteristic equation is $\lambda^2 - 3\lambda + 2 = 0$, which we can factor to get $(\lambda - 1)(\lambda - 2) = 0$. Therefore, our roots are 1 and 2, and thus our homogeneous solution is of the form

$$y_h(x) = k_1 e^x + k_2 e^{2x}.$$

We know that our initial condition contribution is

$$\begin{aligned} y_h(0) &= -2 \\ y_h'(0) &= -7 \end{aligned}$$

This gives us the system of equations

$$\begin{aligned} k_1 + k_2 &= -2 \\ k_1 + 2k_2 &= -7 \end{aligned}$$

which has the solutions $k_1 = 3$, $k_2 = -5$. Thus our final solution is

$$y(x) = 3e^x - 5e^{2x} + 3\cos x + \sin x.$$

(c) Taking derivatives, we have

$$\begin{aligned} y'(x) &= 3e^x - 10e^{2x} - 3\sin x + \cos x \\ y''(x) &= 3e^x - 20e^{2x} - 3\cos x - \sin x \end{aligned}$$

Substituting into our equation, we have

$$\begin{aligned} &3e^x - 20e^{2x} - 3\cos x - \sin x - 3(3e^x - 10e^{2x} - 3\sin x + \cos x) + 2(3e^x - 5e^{2x} + 3\cos x + \sin x) \\ &\quad = (3 - 9 + 6)e^x + (-20 + 30 - 10)e^{2x} + (-3 - 3 + 6)\cos x + (-1 + 9 + 2)\sin x \\ &\quad = 10\sin x \end{aligned}$$

5 Homogeneous RLC Circuit [22 Points]

Solution.

(a) Based on KVL, we know that $V_C = V_R + V_L$. Since this means that the polarity of the resistor and inductor is opposite that of the capacitor, KCL gives us $I_C = -I_R = -I_L$. We can take the derivative of the first equation to get $V_C' = V_R' + V_L'$. We know that $I_C = CV_C'$, $V_R = RI_R$, and $V_L = LI_L'$. Substituting into the equation we get

$$I_C/C = RI_R + (LI_L')' = -I_L/C + RI_L + LI_L''.$$

We rewrite this as our governing equation

$$I_L'' + \frac{R}{L}I_L' + \frac{1}{LC}I_L = 0.$$

(b) **Initial condition.** We know that $V_L = LI_L'$. Therefore, $I_L'(0) = V_L(0)/L$. By our KVL equation, $V_L = V_C - V_R = V_C - RI_R = V_C - RI_L$. Therefore,

$$I_L'(0) = V_L(0)/L = (V_C(0) - RI_L(0))/L = (V_0 - 0)/L = V_0/L.$$

Our characteristic equation is

$$\lambda^2 + \frac{R}{L}\lambda + \frac{1}{LC} = 0$$

which we can solve using the quadratic formula:

$$\lambda = \frac{-\frac{R}{L} \pm \sqrt{\left(\frac{R}{L}\right)^2 - \frac{4}{LC}}}{2}.$$

For simplicity, let

$$\alpha = -\frac{R}{L}$$
$$\beta = \left(\frac{R}{L}\right)^2 - \frac{4}{LC}.$$

Then, $\lambda = (\alpha \pm \sqrt{\beta})/2$.

Overdamped case. If $\beta > 0$, our system is overdamped. Then, our solution is of the form

$$I_L(t) = k_1 e^{\left(\frac{\alpha - \sqrt{\beta}}{2}\right)t} + k_2 e^{\left(\frac{\alpha + \sqrt{\beta}}{2}\right)t}$$

We then use the initial conditions to obtain the system of equations

$$I_L(0) = k_1 + k_2 = 0$$
$$I_L'(0) = \left(\frac{\alpha - \sqrt{\beta}}{2}\right)k_1 + \left(\frac{\alpha + \sqrt{\beta}}{2}\right)k_2 = \frac{V_0}{L}$$

Thus $k_1 = -k_2$, which gives us

$$-\left(\frac{\alpha - \sqrt{\beta}}{2}\right) k_2 + \left(\frac{\alpha + \sqrt{\beta}}{2}\right) k_2 = \sqrt{\beta} k_2 = \frac{V_0}{L}$$

Therefore, $k_1 = -\frac{V_0}{L\sqrt{\beta}}$ and $k_2 = \frac{V_0}{L\sqrt{\beta}}$. In the denominator,

$$L\sqrt{\beta} = \sqrt{L^2\beta} = \sqrt{R^2 - 4\frac{L}{C}}.$$

Thus

$$\begin{aligned} I_L(t) &= -\frac{V_0}{L\sqrt{\beta}} e^{\left(\frac{\alpha - \sqrt{\beta}}{2}\right)t} + \frac{V_0}{L\sqrt{\beta}} e^{\left(\frac{\alpha + \sqrt{\beta}}{2}\right)t} \\ &= -\frac{V_0}{\sqrt{R^2 - 4\frac{L}{C}}} e^{\left(\frac{-\frac{R}{L} - \sqrt{\left(\frac{R}{L}\right)^2 - \frac{4}{LC}}}{2}\right)t} + \frac{V_0}{\sqrt{R^2 - 4\frac{L}{C}}} e^{\left(\frac{-\frac{R}{L} + \sqrt{\left(\frac{R}{L}\right)^2 - \frac{4}{LC}}}{2}\right)t} \end{aligned}$$

Critically damped case. If $\beta = 0$, then the system is critically damped. Our solution will be of the form

$$I_L(t) = k_1 e^{\alpha t/2} + k_2 t e^{\alpha t/2}.$$

We can use the initial conditions to obtain the system of equations

$$\begin{aligned} I_L(0) &= k_1 = 0 \\ I_L'(0) &= \alpha k_1/2 + k_2 = \frac{V_0}{L}. \end{aligned}$$

Then, $k_1 = 0$ and $k_2 = V_0/L$. Therefore,

$$I_L(t) = \frac{V_0}{L} t e^{\alpha t/2} = \frac{V_0}{L} t e^{-\frac{R}{2L}t}.$$

Underdamped case. If $\beta < 0$, then the system is underdamped. Then

$$\lambda = \frac{\alpha \pm j\sqrt{-\beta}}{2}$$

Therefore, our solution is of the form

$$I_L(t) = e^{\alpha t/2}\left(k_1 \cos\left(\sqrt{-\beta} t/2\right) + k_2 \sin\left(\sqrt{-\beta} t/2\right)\right).$$

Using the initial conditions we can obtain the system of equations

$$\begin{aligned} I_L(0) &= k_1 = 0 \\ I_L'(0) &= \alpha k_1/2 + k_1\sqrt{-\beta}/2 = \frac{V_0}{L} \end{aligned}$$

Thus $k_1 = 0$ and $k_2 = \frac{2V_0}{L\sqrt{-\beta}}$. Therefore,

$$\begin{aligned}
I_L(t) &= \frac{2V_0}{L\sqrt{-\beta}} e^{\alpha t/2} \sin\left(\frac{\sqrt{-\beta}}{2} t\right) \\
&= \frac{2V_0}{\sqrt{4\frac{L}{C} - R^2}} e^{-\frac{R}{2L}t} \sin\left(t \frac{\sqrt{\frac{4}{LC} - \left(\frac{R}{L}\right)^2}}{2}\right) \\
&= \frac{2V_0}{\sqrt{4\frac{L}{C} - R^2}} e^{-\frac{R}{2L}t} \sin\left(t \frac{\sqrt{4\frac{L}{C} - R^2}}{2L}\right).
\end{aligned}$$

(c) Substituting in the appropriate values, we see that

$$\beta = \frac{R^2}{10^{-8}} - \frac{4}{10^{-14}} = 10^8 R^2 - 4 \times 10^{14}.$$

When the system is critically damped, $\beta = 0$, which means that

$$R = \sqrt{4 \times 10^6} = 2000.$$

Therefore, the values of 10, 2000, and 10000 ohms represent underdamped, critically damped, and overdamped systems respectively.

We plot the solutions below using MATLAB.

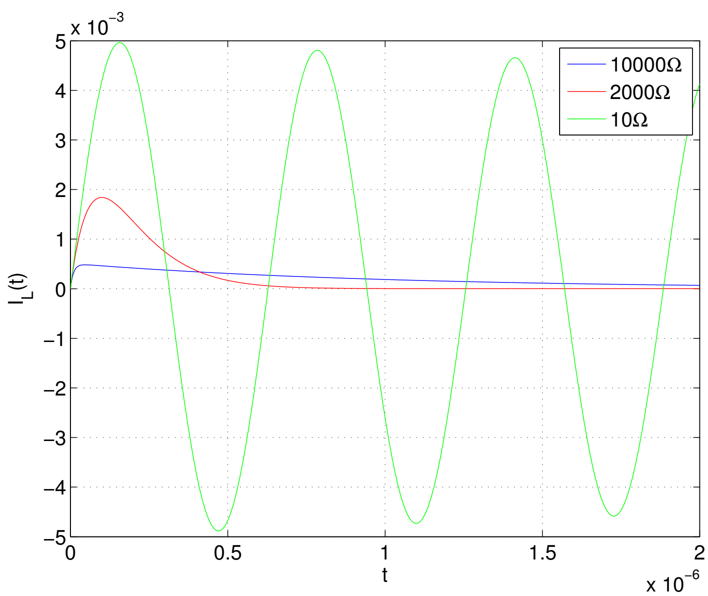


Figure 3: Graph for Problem 5c.

6 Nonhomogeneous RLC Circuit [20 Points]

Solution.

(a) We use KVL and KCL to see that $V_S = V_L + V_R + V_C$ and $I_L = I_R = I_C$. Since $I_L = I_C = CV_C'$, we know that $V_C'(0) = 0$. We also know that

$$V_S(0) = V_L(0) + V_R(0) + V_C(0) = LI_L'(0) + RI_L(0) + 0 = LI_L'(0).$$

Thus $I_L'(0) = V_S/L$, since $V_S(t)$ is constant.

We know that $V_L = LI_L' = LI_C' = L(CV_C')' = LCV_C''$, and that $V_R = RI_R = RI_C = RCV_C'$. Therefore, our ODE for V_C is

$$LCV_C'' + RCV_C' + V_C = V_S$$

which we can write as

$$V_C'' + \frac{R}{L}V_C' + \frac{1}{LC}V_C = \frac{V_S}{LC}.$$

The initial conditions are $V_C(0) = V_C'(0) = 0$.

We also know that $V_S' = V_L' + V_R' + V_C'$. Since $V_L' = (LI_L')' = LI_L''$, $V_R' = RI_R' = RI_L'$,, and $V_C' = I_C/C = I_L/C$, our ODE for I_L is

$$LI_L'' + RI_L' + I_L/C = V_S'$$

which we can write as

$$I_L'' + \frac{R}{L}I_L' + \frac{1}{LC}I_L = \frac{V_S'}{L}.$$

The initial conditions are $I_L(0) = 0$ and $I_L'(0) = V_S/L$.

(b) The characteristic equation is

$$\lambda^2 + \frac{R}{L}\lambda + \frac{1}{LC} = 0.$$

Thus using the quadratic formula,

$$\lambda = \frac{-\frac{R}{L} \pm \sqrt{\left(\frac{R}{L}\right)^2 - \frac{4}{LC}}}{2}.$$

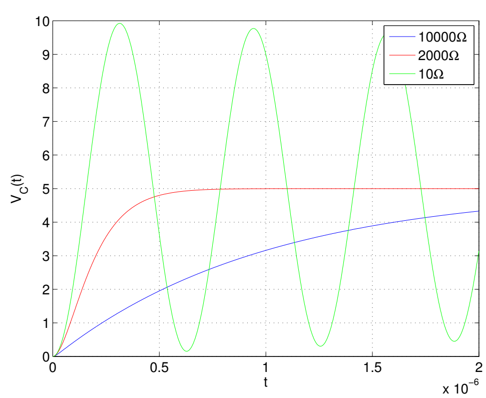
(c) The system will be overdamped if

$$\left(\frac{R}{L}\right)^2 - \frac{4}{LC} > 0.$$

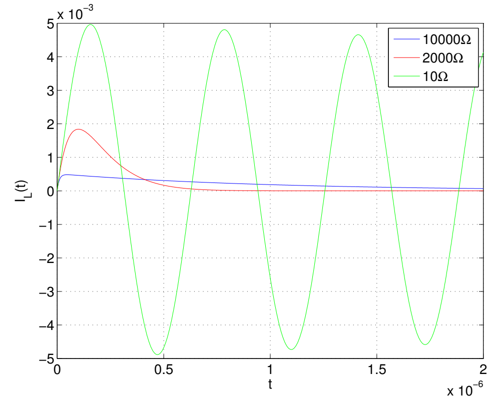
Solving this, we get

$$R > 2\sqrt{\frac{L}{C}} = 2\sqrt{10^6} = 2000.$$

Then, we know that if $R < 2000$ the system will be underdamped, and if $R = 2000$ then the system will be critically damped.



(a) Graph for $V_C(t)$ in Problem 6d.



(b) Graph for $I_L(t)$ in Problem 6d.

(d) In MATLAB we can use the `ode45` function to plot V_C and I_L directly from the ODE. Using this, we can create the plots shown in Figures 4a and 4b.

Notice that since V_S is constant, $V_S' = 0$. Additionally, $I_L'(0) = V_S/L$, where V_S is the same as V_0 from the previous problem. Therefore, our plot for $I_L(t)$ is identical to the one in Problem 5c.

7 Chapter 2 Review Problem 26 [10 Points]

This is a 2nd-order R-L-C circuit with a sinusoidal driving function. Follow a methodology similar to what you did in problem 6, but use the component values for this problem from Kreysig instead of the ones you used in problem 6. Assume that the initial conditions on $V_C(t)$ and $I_L(t)$ are: $V_C(0) = 0\,\mathrm{V}$; $I_L(0) = 0\,\mathrm{A}$ for $t < 0\,\mathrm{s}$ and that $E(t)$ is turned on right at $t = 0\,\mathrm{s}$. Solve for $I_L(t)$ as the problem asks.

Find the current in the RLC-circuit in the figure below when $R = 40\,\Omega$, $L = 0.4\,\mathrm{H}$, $C = 10^{-4}\,\mathrm{F}$, $E = 220 \sin 314t\,\mathrm{V}$ (50 cycles/sec).

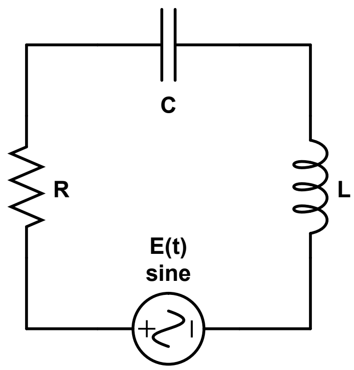


Figure 4: Figure for Problem 7.

Solution. Our circuit laws tell us that $E(t) = V_R + V_C + V_L$ and $I_R = I_C = I_L$. We know that $V_L = LI'_L$, $V_R = RI_R = RI_L$, and $I_C = CV'_C$. If we take the derivative of the equation we get from applying KVL, then we have

$$\begin{aligned} E'(t) &= V'_R + V'_C + V'_L \\ &= (RI_L)' + I_C/C + (LI'_L)' \\ &= RI'_L + I_L/C + LI''_L. \end{aligned}$$

Therefore, our ODE is

$$I''_L + \frac{R}{L} I'_L + \frac{1}{LC} I_L = \frac{1}{L} E'(t).$$

We find the derivative of $E(t)$:

$$E'(t) = 220(314)\cos(314t) = 69080 \cos(314t).$$

Substituting the given values into the equation, we have

$$I''_L + 100 I'_L + 25000 I_L = 172700 \cos(314t).$$

We know that $E(0) = V_R(0) + V_C(0) + V_L(0) = LI'_L(0)$. Since $E(0) = 0$, $I'_L(0) = 0$. Thus our initial conditions are $I_L(0) = I'_L(0) = 0$.

Our characteristic equation is $\lambda^2 + 100\lambda + 25000 = 0$. Then,

$$\lambda = \frac{-100 \pm \sqrt{10000 - 100000}}{2} = -50 \pm 150j.$$

Then, our homogeneous solution is of the form

$$I_{L_h}(t) = e^{-50t}(k_1 \cos(150t) + k_2 \sin(150t)).$$

To find the particular solution, we let $I_{L_p}(t) = K \cos(314t) + M \sin(314t)$ and use the following system of equations:

$$\begin{aligned} (25000 - 314^2)K + 31400M &= 172700 \\ -31400K + (25000 - 314^2)M &= 0 \end{aligned}$$

The solutions are approximately $K = -1.985$ and $M = 0.847$.

We can now solve for our initial conditions:

$$I_L(0) = k_1 - 1.985 = 0 I_L'(0) = -50k_1 + 150k_2 + 314(0.847) = 0$$

This has the solution $k_1 = 1.985$, $k_2 = -2.435$. Therefore,

$$I_L(t) = e^{-50t}(1.985 \cos(150t) - 2.435 \sin(150t)) - 1.985 \cos(314t) + 0.847 \sin(314t).$$

Sample Syllabus: Introduction to Computer Security

My syllabus for the course “Introduction to Computer Security” was created for a course and syllabus design project at the CMU Eberly Center for Teaching Excellence. In it, I explore several new teaching strategies that I feel would be extremely effective for an introductory undergraduate course in computer security.

In particular, the increasingly interdisciplinary nature of computer security has necessitated engagement with the field’s key concepts through a range of activities and variety of perspectives. Because of this, only a third of the class meetings are lectures; the rest of the class meetings are used for lab sessions and discussions of security literature in both small and large groups.

Additionally, the course places a strong emphasis on written communication. I believe that this emphasis will cause students to carefully think about the relevant topics beyond the point of basic understanding, since they must further distill their thoughts into written form. The course provides ample opportunities for practicing this skill, as problem sets and lab writeups are due weekly, providing students with a steady stream of feedback to help them improve their writing in the field of computer security.

Finally, the course examines security in the context of ethics, economics, public policy, and other philosophical and social scientific contexts. The many opportunities that students have to connect topics in computer security to other disciplines offers unique insights into many nuances of the field, and provides even non-majors with applications that may come up in their future work.

CS 182: Introduction to Computer Security, Spring 2014
Course Syllabus

Course Description

Instructor:	Steve Matsumoto
Email:	`smatsumoto@cmu.edu`
Meeting times:	MWF 10-11 AM
Location:	TBD
Units:	9 (CMU units)
TAs:	TBD

Course Overview

This course is an introduction to topics in computer security for undergraduate students in their third or fourth year. Through an in-depth look at three main areas of security (cryptography, system/software security, and network security), this course seeks to develop students' security mindsets. By taking part in a variety of analytical and hands-on activities, we will also discover the interaction of security with other disciplines and in turn reflect on how we should communicate with others about security topics.

Course Objectives

There are three primary objectives which run as common threads throughout the course:

1. **Development of a security mindset.**

   > Uncle Milton Industries has been selling ant farms to children since 1956. Some years ago, I remember opening one up with a friend. There were no actual ants included in the box. Instead, there was a card that you filled in with your address, and the company would mail you some ants. My friend expressed surprise that you could get ants sent to you in the mail.
   >
   > I replied: "What's really interesting is that these people will send a tube of live ants to anyone you tell them to." (Bruce Schneier)

   The craft of computer security is built upon the *security mindset*, a way of observing and questioning systems in the world around us. This mindset is an acquired skill honed through practice and vigilance. When security experts see a new system, they think about how it can be made to fail and what mistakes or faulty assumptions lead to these vulnerabilities.

   This course is designed to help you sharpen your security mindset. You will learn how to reason about the security of computer systems in a variety of applications. You will also practice the skill of questioning and testing the security of systems through lab assignments and reflect on the assumptions that you and your classmates make about the way these systems work.

   Students with a good security mindset should be able to:

   - Identify the assumptions underlying a system.

- Determine the extent to which these assumptions reflect reality.
- Determine any mistakes that have been made in implementing the system.
- Propose an attack based on any mistakes or faulty assumptions that were made.

2. **Understanding the ethics of security.** Ethics plays a critical role in security. Knowing when and how to disclose vulnerabilities and exploits is of the utmost importance, particularly when attacks can leak sensitive personal information or cause millions of dollars in damage. Therefore, in this course we will frequently discuss the ethical aspects of security topics. Assignment writeups will require you to consider what information to disclose, and readings may examine the ethics of security practices that are common in the field.

   Students who understand the role of ethics in security should be able to:

   - Provide examples of white-hat, gray-hat, and black-hat activities.
   - Write a vulnerability report with an appropriate scope and audience.
   - Follow ethical practices when testing the security of a system.

3. **Engaging with security in its societal context.** Areas of security such as cryptography have rich theoretical underpinnings, but it is important to remember that security takes place in the real world. The best cryptography in the world cannot protect data from a user who can be easily fooled or coerced into giving up his or her password. Therefore, we will discuss interactions of security with the social sciences, such as digital currency, Internet governance, and usability in security.

   Students who can engage with security in its social context should be able to:

   - Identify the real-world aspects that may cause even a secure system to fail.
   - Classify adversarial motivations in the context of the social sciences.
   - Analyze the tradeoffs between usability, convenience, and security in a system.
   - Discuss how security and public policy affect each other.

Course Format

The course meets three times per week. Each week consists of one lecture, one lab session, and one group activity. My goal with this format is to maintain a steady, predictable workload (about 6 hours outside of class) during the semester, allowing you to budget a set amount of time each week for this course rather than working in bursts. I ask that you budget some time each week (and ideally each day) to spend on this course and stick to it – if you do so, the work for this course should be quite manageable.

Please see the schedule at the end of this syllabus for a list of topics.

Course Text

I try to keep my course self-sufficient; therefore, there are no required textbooks. I may assign papers as required reading, but I will provide electronic copies of these papers.

I draw some of my material from the following texts, which you may find useful references:

- Charles P. Pfleeger and Shari Lawrence Pfleeger. "Analyzing Computer Security: A Threat / Vulnerability / Countermeasure Approach." ISBN 978-0132789462.
- Bruce Schneier. "Applied Cryptography." Second Edition. ISBN 978-0471117094.

Prerequisites

Students are expected to have a basic knowledge of competency in discrete math and programming. In particular, you should be familiar with basic number theory, programming in C/C++, and be comfortable working in a UNIX command-line environment. Knowledge of computer systems and networking, such as x86 assembly language, compilation, and TCP/IP is helpful, but not required.

Grading

Over the semester you will have the opportunity to demonstrate your learning through five types of assessments: quizzes, problem sets, group discussions, labs, and a final project. Each component counts for 20% of your final course grade. There will be approximately 40 quizzes, 12 problem sets, 6 discussions, 6 syntheses, and 12 labs, as well as a final project.

I expect this course to take approximately 6 hours per week outside of class meetings. If you find that you are putting in significantly more or less time for this class, please contact me, and I will try to provide additional help or adjust the workload.

Quizzes

This course will have a short, five-minute quiz at the beginning of each class meeting. The purpose of these quizzes are threefold: to reinforce long-term retention of the material, to ensure that students are keeping up with the pace of the course, and to indicate to me which concepts need to be clarified or reiterated. Each quiz may cover material from any previous class meeting, though generally concepts taught in a class will be tested in the next class's quiz and retested less frequently as the course progresses. Questions will be brief and straightforward (e.g., definitions, simple calculations, etc). Quizzes will be graded, scanned, and returned to you by email within 24 hours of class.

These quizzes are designed to assess your learning over the course of the semester, rather than assessing your learning through your performance in a single sitting as an exam would. Therefore, you should consider each quiz a daily opportunity to demonstrate your learning. My hope is that over the semester, the quiz material becomes common knowledge that we can use as the foundation of our class discussions.

There are no makeup quizzes, but the lowest two quiz scores will be dropped in calculating your final grade.

Problem Sets

The problem sets in this course facilitate deeper exploration of the material we discuss in class. Problems will be assigned each week and will cover both theoretical and practical elements of the course. Problems may ask you to do things such as:

- analyze a proposed solution to a security vulnerability

- prove the security of a cryptographic protocol
- calculate the complexity of an attack or defense
- discuss the ethical implications of a defense

Problem sets are due on Mondays at the beginning of class, and should take 2-3 hours to complete. They will not be assigned in the last weeks of the course. You are, however, expected to use this time to instead work on your final project.

Group Discussions

Over the semester we will frequently interact as a class or in small groups. The purpose of these interactions is to practice the art of communication in security-related topics and to examine the role of security in its societal contexts. To accomplish these goals, we will participate in several activities:

- **Engaging with security literature.** We will be reading a series of articles and papers in the field, which will serve as the basis for our group interactions. You are expected to analyze the readings, considering their main points and claims with a healthy dose of scientific skepticism. It is important that you consider the evidence at hand when analyzing the literature, since you will need to bring up such evidence (or lack thereof) when defending discussion points with your classmates. These readings will form the basis for the syntheses and discussions (described below). While you are not directly graded for completing the readings, doing so is essential for successfully completing the syntheses and discussions.
- **Literature syntheses.** At times you will be assigned to groups of 3 or 4 and given a series of readings. The group is responsible for dividing these readings amongst the members when they are assigned. Each member will then read his or her assigned reading and prepare a short, 1-page handout that summarizes the main points of the reading and provides a brief analysis of its arguments. On synthesis days, you should bring one copy of the handout for each member in your group, plus an additional copy for me.

  On the specified day, these groups will meet with one another and be given a brief, specific prompt. Each member will share their findings with the other members, using the handout as a reference. The group will then use the class time to synthesize their findings into a brief essay of about 500 words. Your handouts and group essays count for half of your grade in this component, or 10% of the total course grade.
- **Class discussions.** We will also discuss some topics as a whole class. You are expected to take part in these discussions, offering thoughtful perspectives and insightful questions. Your grade for these discussions will be based on the quality, not the quantity, of your contributions. Quality talking points should align with the course objectives and demonstrate that you have deeply thought about the discussion topics. Your participation in these discussions is also worth 10% of the total course grade.

Labs

To facilitate hands-on learning and to impart a deeper understanding of the concepts we discuss in class, you will complete a series of lab assignments throughout this course. Examples of lab activities include:

- Implementing a password cracker
- Gaining administrative access to a website using SQL injection
- Reading encrypted web traffic by forging an SSL certificate

These lab assignments can be completed individually or in pairs. I have allocated the class time on Wednesdays as a chance for you to get started on the lab with the help of the course staff. Each lab will have a pre-lab exercise to be completed before the in-class session. While these exercises are not graded, if you understand the concepts in the exercise, then the lab activity should not take more than two hours to complete. You will then complete a short writeup detailing your findings which should take no more than an hour.

Final Project

This course is designed to expose you to a breadth of topics in computer and information security. The final project is an opportunity for you to take a topic that particularly interests you and explore it in greater depth. I expect the project to strike a reasonable balance between theory and hands-on work, and scoped appropriately to the allotted time period.

Projects can be completed in teams of two to four students, and you are responsible for choosing your own teams. When the project period begins, you should come up with several ideas for your project. I will then meet with each team individually to help you refine and scope these ideas. You will then have several weeks to carry out your project and design some sort of exhibition for your results (e.g. a presentation, poster, or website). You will be graded on the quality of your analysis, your communication skills, and *the degree to which you demonstrate your security mindset and understanding of security in its ethical and societal contexts*.

Policies

Special Accommodations

If you have a physical or learning disability and would like to request a special accommodation in this course, please contact me as soon as possible. I will do my best to provide you with an effective learning environment. You can also coordinate this through the Office of Disability Resources, but in any case please come speak to me so that I am aware of any special needs you may have.

Classroom Behavior

Regarding aspects of classroom behavior and etiquette, I have one fundamental policy: I will do my best to provide a beneficial, enjoyable learning environment, and I ask that you in turn do your best to promote and enhance that environment for yourself and your classmates. That is, be mindful of the class, our time, and our attention, and please keep distractions to an absolute minimum.

In particular, I ask that you adhere to the following policies:

- **Attendance:** Please be on time for class. If you must arrive late or leave early, please let me know in advance and sit in a location that minimizes distraction, such as near the door.

- **Electronic devices:** I hand out course notes at the beginning of each lecture. Therefore, please do not use phones, tablets, or laptops during class. If this presents a serious problem to your learning during lectures, please come speak to me and we can make appropriate arrangements.
- **Cell phones:** Noises such as those made by cell phones can draw the attention of others and affect your classmates' learning. Therefore, please remember to silence your phones and other devices which may make noise.

  However, life goes on outside of the classroom. It is completely acceptable to step outside of the class to handle emergency situations that may arise during class time. If you know in advance that such a situation may happen during class (e.g., a loved one is in critical condition, getting an important job-related call, etc.), please inform me by email and sit near the door to keep distractions to a minimum.

Academic Integrity and Collaboration Policy

We highly encourage collaboration with your classmates in the form of discussion. You are free to discuss approaches to problems with your classmates, the graders, and instructor. However, copying solutions, whether code or prose, is strictly prohibited unless explicitly stated otherwise. In the event that a collaborative discussion involves writing of any kind, each person must complete their own write-up and all writing that took place during the discussion must be thrown away or erased prior to each person beginning their write-up.

If you are unsure of whether a specific type of collaboration is allowed, ask a grader or the instructor first. Please also look at the official university policy on academic integrity for further details. Penalties for academic dishonesty in this course may range from failure of the assignment to failure of the course, and any cases of academic dishonesty will be reported to the Dean of Student Affairs.

Security Techniques

In this course you will gain a deeper understanding of some security attacks by carrying them out firsthand against our test machines. This experience is intended to highlight the nuances of a security vulnerabilities so that you can avoid them in your future coding practices. While some of these techniques are sometimes in a legal gray area, they can be annoying or damaging if you apply them without being authorized to do so. Do not "test the security" of systems without obtaining prior permission from the owner, or you may be subject to criminal sanctions.

Late Homework

In general, late homework is not accepted. However, recognizing that life goes on outside the classroom and that urgent matters can come up unexpectedly, I will accept one problem set or lab, no questions asked, up to 24 hours late without any penalty. Labs completed in pairs may require both students to use their late days, but this will be handled on a case-by-case basis. Think of this provision as an emergency aid; you should have a very good reason for using it. Because of this, I cannot guarantee that I will accept any additional late assignments beyond the one you are given. However, if your request is reasonable then I will give it serious consideration.

Changes to this Syllabus

This syllabus is subject to change based on circumstances that may arise during the course. In the event that I make changes to the syllabus, I will inform you by email and post an updated version of the syllabus.

Tentative Schedule

	Date	Activity	Topic
			Foundations
W	1/22	Lecture	Syllabus, Security Mindset, Ethics
F	1/24	Lecture	Adversary Models, Definitions
			Cryptography
M	1/27	Lecture	Mathematical Foundations
W	1/29	Lab	Fast Modular Arithmetic
F	1/31	Discussion	“Hard” Problems in Number Theory
M	2/3	Lecture	Symmetric Key Cryptography
W	2/5	Lab	Decrypting Secret Messages
F	2/7	Synthesis	Encryption Models
M	2/10	Lecture	Public Key Cryptography
W	2/12	Lab	Forging Messages
F	2/14	Discussion	Real-World Implementations
M	2/17	Lecture	Hashes and MACs
W	2/19	Lab	Password Cracking
F	2/21	Synthesis	Hashing Vulnerabilities
			System and Software Security
M	2/24	Lecture	Assembly Language, Program Compilation
W	2/26	Lab	Reverse Engineering Tools
F	2/28	Discussion	Ethics of Reverse Engineering
M	3/3	Lecture	Program Analysis
W	3/5	Lab	Bug Hunting
F	3/7	Synthesis	Limitations of Analysis
M	3/10	Lecture	Buffer Overflow
W	3/12	Lab	Stack Smashing
F	3/14	Discussion	Stack Defenses
M	3/17	Lecture	Input Filtering
W	3/19	Lab	SQL Injection
F	3/21	Synthesis	Input Rectification
			Network Security
M	3/24	Lecture	Web Security
W	3/26	Lab	Cookie Attacks
F	3/28	Discussion	Vulnerability Disclosure
M	3/31	Lecture	SSL/TLS
W	4/2	Lab	Man-in-the-Middle Attacks
F	4/4	Synthesis	Public Key Infrastructures
M	4/7	Lecture	Routing Security
W	4/9	Lab	Traffic Hijacking
F	4/11	Discussion	Internet Governance
M	4/14	Lecture	TCP/IP Security
W	4/16	Lab	Denial of Service (DoS)
F	4/18	Synthesis	Computational Puzzles

The remainder of the semester will consist of special topics lectures and project exhibitions.

Future Faculty Program Completion Letter

To be added upon completion of the Future Faculty Program.