# Applied Cryptanalysis Syllabus

## Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Basic Information</td>
<td>2</td>
</tr>
<tr>
<td>2 Overview</td>
<td>2</td>
</tr>
<tr>
<td>3 Instructor and Student Roles</td>
<td>3</td>
</tr>
<tr>
<td>4 Syllabus Policy</td>
<td>3</td>
</tr>
<tr>
<td>5 Email Policy</td>
<td>3</td>
</tr>
<tr>
<td>6 Computer and Internet Access Policy</td>
<td>3</td>
</tr>
<tr>
<td>7 Textbook</td>
<td>4</td>
</tr>
<tr>
<td>8 Calculator Requirement</td>
<td>4</td>
</tr>
<tr>
<td>9 Course Components</td>
<td>4</td>
</tr>
<tr>
<td>9.1 Class Meetings</td>
<td>4</td>
</tr>
<tr>
<td>9.2 Lessons</td>
<td>5</td>
</tr>
<tr>
<td>9.2.1 Lesson Instructions</td>
<td>5</td>
</tr>
<tr>
<td>9.3 Non-quiz Class Meetings</td>
<td>6</td>
</tr>
<tr>
<td>9.4 Quizzes</td>
<td>6</td>
</tr>
<tr>
<td>9.4.1 Quiz Schedule</td>
<td>6</td>
</tr>
<tr>
<td>9.4.2 Quiz Policies</td>
<td>7</td>
</tr>
<tr>
<td>9.4.3 Make-Up Quizzes</td>
<td>7</td>
</tr>
<tr>
<td>9.4.4 Quiz Grading</td>
<td>8</td>
</tr>
<tr>
<td>9.4.5 Understanding Quiz Results</td>
<td>8</td>
</tr>
<tr>
<td>10 Getting Help</td>
<td>9</td>
</tr>
<tr>
<td>10.1 Office Hours</td>
<td>9</td>
</tr>
<tr>
<td>10.2 Online Help</td>
<td>9</td>
</tr>
<tr>
<td>10.3 Email Help</td>
<td>10</td>
</tr>
<tr>
<td>11 Course Grade</td>
<td>10</td>
</tr>
<tr>
<td>12 Course Content and Objectives</td>
<td>10</td>
</tr>
<tr>
<td>12.1 Bulletin Description</td>
<td>10</td>
</tr>
<tr>
<td>12.2 Course Objectives</td>
<td>11</td>
</tr>
<tr>
<td>12.3 Course Outline</td>
<td>11</td>
</tr>
<tr>
<td>12.4 Bibliography</td>
<td>12</td>
</tr>
<tr>
<td>13 University Policies</td>
<td>12</td>
</tr>
<tr>
<td>13.1 Undergraduate Bulletin</td>
<td>12</td>
</tr>
<tr>
<td>13.2 Attendance Policy</td>
<td>12</td>
</tr>
</tbody>
</table>
1 Basic Information

Course: Applied Cryptanalysis, 2030:461-101 16128
Course Type: Web-based (31%–99% online)
Course Web Site: https://srandby.org/2020-1/461-101/home.html
Class Location: Polsky 424
Time and Dates: 2:45–3:35 p.m., Tu, 1/14/2020–4/28/2020
Instructor: Dr. Scott Randby
Department: Applied General and Technical Studies
Email: srandby@uakron.edu
Office: Polsky 131F
Office Hours
  Monday: 1:45–3:45 p.m.
  Wednesday: 1:45–3:45 p.m.
  or by appointment
Online Office Hours
  Monday: 1:45–3:45 p.m.
  Wednesday: 1:45–3:45 p.m.
  or by appointment
  Online meetings require prior notification.
Quiz Schedule
  Quiz 1: 1/21
  Quiz 2: 2/4
  Quiz 3: Online
  Quiz 4: 3/3
  Quiz 5: 3/17
  Quiz 6: 4/7
  Quiz 7: 4/21
  Quiz 8: 5/5, 4:45–6:45 p.m.

2 Overview

1. The class will meet once per week on campus. Each class meeting will be 50 minutes in length. A 50-minute quiz will be given in class during weeks 2, 4, 8, 10, 12, 14, and during finals week. The quiz during week 6 will be a 60-minute online quiz.
2. New lessons will be posted in the Current Lessons section of the Lessons page of the course website during week 1 and after each bi-weekly quiz.
3. The lessons should be done in the order they appear in the *Current Lessons* section of the *Lessons* page.

4. Follow the instructions for each lesson. Plan to spend at least 200 minutes each week working through lessons and at least 400 minutes each week working on homework problems.

5. Each bi-weekly quiz will be worth 50 points and will cover the lessons posted in the *Current Lessons* section of the *Lessons* page.

6. The notes and audio recordings made in each non-quiz class will be posted on the *Sessions* page of the course website.

7. Help is available from Dr. Randby in person and online. See the *Help* page of the course website or the *Getting Help* section of this document for instructions on obtaining help.

### 3 Instructor and Student Roles

The relationship between the instructor and a student will be a professor-student relationship. This type of relationship is not employer-employee, commander-subordinate, parent-child, or friend-friend. The role of the professor in this class is to guide students through the course and help students learn the course material. The role of the student is to learn the course material and demonstrate that learning on quizzes.

### 4 Syllabus Policy

Students are required to download the syllabus from the homepage of the course website. It is the responsibility of every student to read and understand the syllabus.

### 5 Email Policy

All students are required to check their `zips.uakron.edu` email account at least once a day.

Email is not sent out every day, but students are required to check their `zips.uakron.edu` account anyway.

Students are required to use their `zips.uakron.edu` email account when they send email to the instructor.

Email from the instructor to a student is sent only to the student’s `zips.uakron.edu` account.

### 6 Computer and Internet Access Policy

All students are required to have continuous access for the entire duration of the course to the Internet using a fully functional computer that works properly.
7  Textbook

No textbook is used in this class. All course materials (lessons, session notes, session audio recordings, etc.) are posted on the course website.

8  Calculator Requirement

All students are required to have a either a scientific or graphing calculator with minimum functionality equivalent to that of the Texas Instruments TI–30X IIS calculator.

Every student is required to have possession of their calculator by the end of the first week of classes.

Students are required to bring a suitable calculator to each class.

Phone or laptop calculators are not permitted to be used when taking quizzes.

9  Course Components

All lessons and other course materials are posted online at the following website.

https://srandby.org/2020-1/461-101/home.html

Course materials may also be accessed via the learning management system operated by the university.

The course website contains lessons, notes and audio from non-quiz class meetings, instructions for obtaining help, and other information about the course.

The course website does not track via cookies or other means. It is up to students to determine when they will access the site and how they will study the course materials. The instructor provides a suggested process for going through the course—a process based on the science of learning.

9.1  Class Meetings

The class will meet once per week on campus. Each class meeting will be 50 minutes in length.

Students will take a quiz during the class meetings of each of the weeks 2, 4, 8, 10, 12, 14, and finals week. The quiz during week 6 will be a 60-minute online quiz.

Class meetings during which there is no quiz will be devoted to answering questions students have about the lessons that appear in the Current Lessons section of the Lessons page on the course website. Attendance will be taken during these class meetings.
9.2 Lessons

Links to the lessons are given on the Lessons web page available at the following address.


New lessons will be posted in the Current Lessons section of the Lessons page during week 1 and after the bi-weekly quizzes on weeks 2, 4, 6, 8, 10, 12, and 14. Lessons studied in previous weeks will appear in the Old Lessons section of the Lessons page.

The lessons should be done in the order they appear in the Current Lessons section of the Lessons page.

Lessons should be completed by the evening of the day before the bi-weekly quiz.

Make sure to follow the lesson instructions. Plan to spend at least 200 minutes each week studying lessons and at least 400 minutes each week working on homework problems.

It takes time for the human brain to absorb and comprehend mathematics, and setting aside that time is crucial for success in this course. You should begin studying the lessons posted in the Current Lessons section of the Lessons page soon after they are posted. Set aside ample time each day to work on the current lessons. By the day before a quiz, you should have worked through each lesson, completed all of the homework problems, thoroughly understood the material covered in the lessons, and reworked the homework problems several times. If you work in this manner, then you will have ample time to ask the instructor questions and understand the course material well enough to earn a good grade on a quiz.

Students are required to complete all homework assignments.

It is the responsibility of the student to seek help in a timely manner if it is needed on a homework assignment.

9.2.1 Lesson Instructions

You may study a lesson online, or you can download it for offline use. The lesson’s PDF files may be viewed using any PDF reader.

In order to learn the material covered in this course, students need to have good learning practices while working on a lesson. Scientific research into learning has shown that students who use certain “good” practices are more successful than students who don’t use those practices. The following instructions are meant to encourage students to use good learning practices while working on a lesson.

1. Read the text of the lesson carefully in a place without distractions.
   • Take thorough, complete, and good notes as you study the lesson.
     – Taking notes is an effective memory-retention technique that improves learning.
   • Make note of items you do not understand and go back over those items until you understand them. Ask for help on any items you are unable to understand yourself.
   • Do not use other electronic devices (except for a calculator) or visit other web sites when you are studying the lesson unless their use is required in the lesson.
2. Work through the homework problems referring to your notes and the lesson when necessary. Use the homework problem solutions only when you get completely stuck.

3. Do not consider the lesson to be completed until you thoroughly understand it. If there is something about the lesson you do not understand, then obtain help by either visiting Dr. Randby in his office during his office hours, making an appointment to meet with him in his office and meeting with him during the appointment’s time, making an appointment to meet with the Dr. Randby in his online office and meeting with him in the online office during the appointment’s time, or sending an email message to srandby@uakron.edu asking for help.

4. Redo the homework problems before a quiz without referring to any other materials. It is best to do this more than once.

9.3 Non-quiz Class Meetings

A class meeting during which no quiz is given is not optional. Students are required to adhere to the university’s official attendance policy. Students who miss a non-quiz class and fail to submit a valid and acceptable excuse for missing the class may be required to meet with Dr. Randby outside of class to discuss the absence and the university’s official attendance policy. Students who fail to meet with Dr. Randby to discuss unexcused absences may have up to 5 points deducted from their numerical course grade for each meeting missed.

Class notes and audio recorded during non-quiz class meetings will be posted on the Sessions page of the course website. The address of this page is the following:

https://srandby.org/2020-1/461-101/sessions.html

Students are required to obtain notes from the Sessions page whenever they miss a non-quiz class.

9.4 Quizzes

A 50 point quiz will be given in class during weeks 2, 4, 6, 8, 10, 12, 14, and during finals week.

Each quiz will be over the material covered in the lessons that were posted after the weekly class meeting preceding the quiz.

Students will have 50 minutes to complete each in-class quiz. Students will be given 60 minutes to complete an online quiz.

The instructor will grade the quizzes and post the grades on Brightspace.

9.4.1 Quiz Schedule

Quiz 1: 1/21
Quiz 2: 2/4
Quiz 3: Online
Quiz 4: 3/3
Quiz 5: 3/17
Quiz 6: 4/7
Quiz 7: 4/21
Quiz 8: 5/5, 4:45–6:45 p.m.

The quiz schedule may be altered by Dr. Randby if necessary.

9.4.2 Quiz Policies

Students are required to arrange their schedules so that they arrive to all quizzes on time. Students who are late to a quiz may not disturb other students in any way, and they will be given the quiz only after all other students are settled.

Early quizzes will not be given for any reason.

Students are not permitted to use scrap paper, red pens, or red pencils during a quiz.

Except for approved calculators, students are not permitted to use electronic devices (laptops, smartphones, cell phones, headphones, earbuds, etc.) during a quiz unless the use of such devices meets an accommodation requirement or their use has been approved by the instructor prior to the quiz. These devices are not permitted to be visible and they may not make any sounds during a quiz (unless their use is permitted of course). Students may not leave the class during a quiz to use an electronic device for any reason.

Phone or laptop calculators are not permitted to be used when taking quizzes.

Students are required to turn in all materials they have received from the instructor after completing a quiz.

Students are required to finish their quizzes by the end of the class period. Students who arrive late to a quiz will not be given a time extension.

The final quiz is given during finals week. Early final quizzes will not be given for any reason whatsoever. Students who plan to leave campus before the final quiz will be given no accommodation. Students who miss the final quiz without an excusable and valid reason (determined solely by Dr. Randby) will receive a grade of 0 on the quiz.

9.4.3 Make-Up Quizzes

Students are required to take every quiz during its scheduled date and time unless Dr. Randby agrees to schedule a make-up quiz.

It is the responsibility of a student to request a make-up quiz. Dr. Randby reserves the right to require a student to provide additional information or documentation whenever a student requests a make-up quiz.

Make-up quizzes are given at the discretion of Dr. Randby. Requesting a make-up quiz does not guarantee that a make-up quiz will be granted. Some of the factors that are taken into account when determining whether or not to grant a make-up quiz request are (1) the reason for the request, (2) the length of time between the quiz and the submission of the request, (3)
attendance, (4) homework completion, and (5) the number of previous make-ups. A make-up quiz will not be granted if the reason for the request is either not exceptional or not beyond the control of the student or both.

Make-up quiz requests for participation in a university-sponsored event or jury duty require documentation. Students are required to supply Dr. Randby with documentation in PDF form. A make-up quiz will only be given on campus in the presence of Dr. Randby.

9.4.4 Quiz Grading

Each problem or part of a problem on a quiz is graded on a 0–1 point scale in increments of 1/10th of a point. The points are totaled, the point total is divided by the maximum possible point total, the result of the division is multiplied by 50, and the result of the multiplication is rounded to the nearest 1/10th. The rounded number is the grade on the quiz.

The following questions are considered when a quiz problem is graded.

1. Does the solution demonstrate an understanding of the concepts and methods covered in class that are relevant to the problem?
2. Does the solution use the required and proper techniques and methods?
3. Is the solution presented in a logical and coherent manner?
4. Does the solution use notation properly and correctly?
5. Are the theoretical and numerical computations that appear in the solution correct?
6. Are the numerical values that appear in the solution correct?
7. Is the solution succinct and to-the-point?
8. Is the solution clear and unambiguous?

Problem Grading
-0: Perfect work
-0.1: A work with minor errors
-0.2: B work
-0.3: C work
-0.4: D work
-0.5 – -1.0: F work
-1.0: No work or required work missing

9.4.5 Understanding Quiz Results

When graded quizzes are returned to a student, only the student’s graded work is returned. The sheet containing the quiz problems is not returned. The reason for this practice is that quizzes are not learning tools, they are where students demonstrate learning. If there appears to be a grading error on a quiz or if the grading is not understood, then a student should meet with Dr. Randby to discuss the grading.
10 Getting Help

Instructions for getting help are given on the Help web page available at the following address:


The following information is given on the Help page.

10.1 Office Hours

Dr. Randby will be available in Polsky 131F during the following days and times:

Monday: 1:45–3:45 p.m.
Wednesday: 1:45–3:45 p.m.

If Dr. Randby is not in his office during one of the above times and he has not previously announced that he will not be there, then students should assume there is a legitimate reason for his absence. Students may either wait to see if Dr. Randby returns to his office before the end of the help period, obtain help during the next scheduled help period, or send an email to srandby@uakron.edu asking for help in Dr. Randby’s office at a different time.

If a student wishes to meet with the Dr. Randby at a time not listed above, then that student should see him in person to arrange a meeting or send an email requesting a meeting to srandby@uakron.edu.

Students may come to Polsky 131F anytime, not just during office hours. If Dr. Randby is in the office when a student arrives and he is not working on something urgent, then he will be happy to help the student.

Please note that office hours are for discussing homework problems, clarifying concepts discussed in class, and discussing general mathematical issues.

Whenever a student goes to Dr. Randby’s office for help, the student should bring relevant class notes, a copy of any relevant homework assignments, any work the student has done, a calculator, a writing instrument, and paper.

10.2 Online Help

Students may communicate in real time (audio, video, chat, screen sharing) with Dr. Randby in a Jitsi Meet room. You may access the room by clicking on the following link:

https://meet.jit.si/DrRandbyOnlineOffice

Dr. Randby’s online office hours are as follows:

Monday: 1:45–3:45 p.m.
Wednesday: 1:45–3:45 p.m.

Students who wish to meet with Dr. Randby in his online office during the online office hours
listed above must notify Dr. Randby by email prior to the office hours, and they must receive a response from Dr. Randby confirming reception of the email. Otherwise, Dr. Randby will not be in his online office during online office hours.

If a student wishes to meet with Dr. Randby in his online office at a time not listed above, then that student should send an email requesting an online meeting to srandby@uakron.edu.

10.3 Email Help

Students may send questions about the course lessons and homework assignments to Dr. Randby via email. Questions should be sent to srandby@uakron.edu from a zips.uakron.edu account. Questions sent from accounts other than zips.uakron.edu accounts will not receive a response.

Questions sent via email will receive a response within 24 hours after they are sent unless special circumstances prevent Dr. Randby from replying during that time period.

11 Course Grade

All quiz grades will be posted on the learning management system operated by the university. Use the following to determine your numerical course grade $G$.

\[
qnum = \text{the number of quizzes given} \\
qmax = \text{the maximum possible points on a quiz} \\
qsum = \text{the sum of the scores earned on the quizzes}
\]

\[
G = \frac{100 \cdot qsum}{qnum \cdot qmax}
\]

Use the numerical course grade and the following list to determine your course letter grade.

- A if $91 \leq G < 100$
- A– if $90 \leq G < 91$
- B+ if $87 \leq G < 90$
- B if $81 \leq G < 87$
- B– if $80 \leq G < 81$
- C+ if $77 \leq G < 80$
- C if $71 \leq G < 77$
- C– if $70 \leq G < 71$
- D+ if $67 \leq G < 70$
- D if $63 \leq G < 67$
- D– if $60 \leq G < 63$
- F if $G < 60$

12 Course Content and Objectives

12.1 Bulletin Description

Prerequisite: 2030:361 with a grade of C or better. Cryptanalysis concepts; cryptanalysis of symmetric and public key cryptosystems, key exchange systems, and digital signatures; hash function collision resistance; cryptanalysis with quantum computers.
12.2 Course Objectives

After completing this course the student should have the following competencies:

1. an understanding of the basic concepts of cryptanalysis and the methods used to attack an encryption system;
2. the ability to implement an exhaustive key search against a symmetric cryptosystem;
3. an understanding of basic factoring algorithms and the ability to use those algorithms;
4. an understanding of how to attack the RSA cryptosystem using a factoring algorithm;
5. an understanding of how to find a brute force solution to the discrete logarithm problem, and the ability to conduct a man-in-the-middle attack against the Diffie-Hellman key exchange;
6. an understanding of how to attack the RSA signature scheme;
7. an understanding of the concept of collision resistance and The Birthday Attack;
8. an understanding of what the development of quantum computers will mean to the security of public key cryptography.

12.3 Course Outline

1. General mathematical cryptanalysis concepts
   - Key recovery vs. decryption
   - Kerckhoffs’ Principle
2. Cryptanalysis of symmetric cryptosystems
   - Symmetric cryptosystems
   - Brute force attacks
     - Exhaustive key search
     - Key lengths and security levels
3. Public key cryptography review
4. Review of the RSA cryptosystem
5. Factoring algorithms
6. Mathematical attacks on RSA
   - Preventing mathematical attacks
7. Key exchange
   - Review of the Diffie-Hellman key exchange
   - The discrete logarithm problem
     - Brute force solutions
   - The generalized Diffie-Hellman problem
   - Man-in-the-middle attack against the Diffie-Hellman key exchange
8. Digital signatures
   - Review of the principles of digital signatures
   - Review of the RSA signature scheme
   - Attacks against the RSA signature scheme
9. Hash functions
   - Collision resistance
   - The Birthday Attack
10. Implications of quantum computers on public key cryptography
12.4 Bibliography


13 University Policies

13.1 Undergraduate Bulletin

The university policies that affect students are contained in the *Undergraduate Bulletin*.

https://bulletin.uakron.edu/undergraduate/

13.2 Attendance Policy

The official attendance policy of the university is presented on the *Important Policies* page of the *Undergraduate Bulletin*.
A student is expected to attend all class meetings for which the student is registered. A student may be dropped from a course in the current term by the dean if absence is repeated and the instructor recommends this action; a student can gain re-admission only with permission of both the instructor and the dean. A student dropped from a course receives an “F” which counts as work attempted whenever grade-point ratio calculations are made.

13.3 Incomplete Policy

The official incomplete policy of the university is presented on the Grade Policy and Credit page of the Undergraduate Bulletin.

https://bulletin.uakron.edu/undergraduate/important-policies/grade-policy-credit/

Students are expected to read and understand the official incomplete policy.

13.4 Withdrawal Policy

The official withdrawal policy of the university is presented on the Important Policies page of the Undergraduate Bulletin.

https://bulletin.uakron.edu/undergraduate/important-policies/

Students are expected to read and understand the official withdrawal policy.

The withdrawal deadline for this course is **Sunday, March 1**.

14 Academic Honesty and Student Conduct

Students are required to maintain the highest level of academic honesty in this course. The university’s academic honesty expectations are outlined in the Academic Misconduct section on the Grade Policy and Credit page of the Undergraduate Bulletin.

https://bulletin.uakron.edu/undergraduate/important-policies/grade-policy-credit/

Students are required to follow The University of Akron’s Code of Student Conduct. The Code of Student Conduct is contained in section 3359-41-01 of the University Rules.


Additional information regarding academic honesty and student conduct expectations and procedures is available on the website of the Student Conduct and Community Standards office.

https://www.uakron.edu/studentconduct/
15 Accessibility, Counseling, and Health Services

Students who require special services and/or accommodations in the course should submit a request to the Office of Accessibility (OA) in a timely manner. The OA is located in Simmons Hall Room 105, and it may be contacted at 330-972-7928 (v), 330-972-5764 (tdd), or access@uakron.edu. Click on the following link for more information.

https://www.uakron.edu/access/

Currently enrolled students may obtain free psychological services at the Counseling & Testing Center. Click on the following link for more information.

https://www.uakron.edu/counseling/

Currently enrolled students may obtain free or low cost health services at Student Health Services. Click on the following link for more information.

https://www.uakron.edu/healthservices/

16 Title IX at UA

The University of Akron is committed to providing an environment free of all forms of discrimination, including sexual violence and sexual harassment. This includes instances of attempted and/or completed sexual assault, domestic and dating violence, gender-based stalking, and sexual harassment. If you (or someone you know) has experienced or experiences sexual violence or sexual harassment, know that you are not alone. Help is available, regardless of when the violence or harassment occurred, and even if the person who did this is not a student, faculty or staff member.

Confidential help is available. If you wish to speak to a professional, in confidence, please contact one of the following:

Rape Crisis Center
Website: https://hopeandhealingresources.org/rape-crisis-center-services/
24-Hour Hotline: 330-434-7273
Hours: 24/7

University Counseling and Testing Center
Website: https://uakron.edu/counseling/
Phone: 330-972-7082
Hours: 8 am–5 pm, Monday–Friday

Help is also available from the following:

University of Akron Police
Website: https://uakron.edu/safety/police/
Phone: 330-972-2911 (9-1-1 in an emergency)
Hours: 24/7
Dean of Students Office

Website: https://uakron.edu/deanofstudents/
Phone: 330-972-6048
Hours: 8 am–5 pm, Monday–Friday

Please understand that the majority of University of Akron employees, including faculty members, are considered to be “responsible employees” under the law and are required to report sexual harassment and sexual violence. If you tell me about a situation, I will be required to report it to the Title IX Coordinator and possibly the police. You will still have options about how your case will be handled, including whether or not you wish to pursue a law enforcement or complaint process. You have a range of options available and we want to ensure you have access to the resources you need.

Additional information, resources, support and the University of Akron protocols for responding to sexual violence are available at https://uakron.edu/Title-IX/.