Applied Cryptanalysis Syllabus

Table of Contents

1 Basic Information

Course: Applied Cryptanalysis
Course Identifiers: MATH 461-501 (14991)
Course Type: Online
Length: 1/16/2024–5/5/2024
Course Web Site: Applied Cryptanalysis Home
Instructor: Dr. Scott Randby
Email: srandby@uakron.edu
Office: College of Arts and Sciences 263 (CAS 263)
Phone: 330-972-6094
Help: Email help, live online help via web conferencing software

1.1 Schedule

Assignment	Due Date
Making a PDF	1/19 at 11:59 p.m.

	Learning Period Dates	Quiz Period Dates
1	1/16–1/25	1/26
2	1/29–2/8	2/9
3	2/12–2/22	2/23
4	2/26–3/7	3/8
5	3/11–3/21	3/22
6	4/1–4/11	4/12
7	4/15–4/25	4/26
8	4/29–5/5	5/6–5/7

Quiz retake request deadline: 4/19 at 11:59 p.m.

2 Syllabus Policy

A major part of cybersecurity work is reading, studying, and understanding documentation. Documentation is presented in a wide variety of forms, and working with documentation effectively is a skill you need to acquire and refine.

This syllabus is the documentation for this course—it is your guide to the course. This document completely explains the course policies and how the course works. You are required to study this document carefully so that you understand the course policies, know how to learn in the course, know what to do to get help with the course materials, know when you need to study, know when you need to take quizzes, and know how to take the quizzes.

3 Overview

1. The course is an online course. Lessons will be studied during eight *learning periods* and quizzes will be taken during eight *quiz periods*. Each learning period will be followed by a quiz period.
2. Links to the lessons will be posted in the Current Lessons section on the Lessons page of the course website. Each lesson will contain one or more sections. Each lesson section contains a video, the notes made in the video, homework problems, and homework problem solutions.
3. The lessons should be studied in the order they appear in the Current Lessons section of the Lessons page.
4. Each quiz will be worth 50 points and will cover the lessons posted in the Current Lessons section of the Lessons page. Quizzes will be given on Brightspace. You will have 75 minutes to complete a quiz. The first 60 minutes is for taking the quiz, and the final 15 minutes is for making one or more PDF files of your written work, adding the PDF(s) to the quiz responses, and submitting the quiz.
5. Help will be available via email. Live online help (individual or group) will be available using web conferencing software. See the Help page of the course website or the Getting Help section of the syllabus for instructions on obtaining help.

4 Important Note

You are taking this course because numerous professional organizations require cybersecurity programs to have a significant cryptology component, and because cybersecurity would not exist without cryptography and cryptanalysis. When you work in the cybersecurity field, you will have to use cryptosystems every day, and you need to understand the various methods that can be used to analyze those systems.

5 Instructor and Student Roles

The relationship between the instructor and a student will be a professor-student relationship. 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.

6 Ethics

Cybersecurity professionals are entrusted to protect and preserve the confidentiality of data and sensitive information. This mandates that the cybersecurity professional acts ethically at all times without exception. As a potential cybersecurity professional, you are required to act ethically at all times without exception.

It is assumed that students taking the course already understand how to conduct themselves as college students should conduct themselves, and it is assumed that ethical misconduct in the course will be absent or rare. The following subsections are meant to explain in detail how you are required to act in the course, so you should study them carefully even if you are already aware of their content.

Violations of the course ethics policies are taken very seriously. Sanctions for a violation depend on the seriousness and the nature of the violation, and possible sanctions include but are not limited to a reprimand, losing all the points on a quiz problem, a major point deduction from a quiz, a failing grade in the course, and a referral to the Student Conduct and Community Standards office.

6.1 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.

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.

6.2 Academic Honesty on Quizzes

Cheating on a quiz is not permitted at any time. It is your responsibility to know what constitutes cheating on a quiz. Cheating on a quiz includes but is not limited to:

- consulting notes, course materials, websites, books, papers, or other materials that have not been approved by the instructor for use while taking a quiz;
- using a device or program other than an approved calculator to perform computations while taking a quiz (see the Calculator Requirement section of this document);
- presenting a final result of a complex computation without presenting the work required to obtain that result;
- making unauthorized copies of part or all of a quiz (screenshots, videos, notes, etc.);
- obtaining any information about the quiz problems or their solutions from any source except the instructor before, during, or after taking a quiz;
- obtaining help solving quiz problems from any source except the instructor before, during, or after taking a quiz;
- sharing any information about the quiz problems or their solutions with anyone except the instructor before, during, or after taking a quiz;
- helping another student solve quiz problems at any time;
- unauthorized acquisition of quiz problems or their solutions given in the cryptology sequence of courses;
- knowing about cheating activity and failing to report it to the instructor;

- not being truthful about your actions regarding a quiz.

In most cases, you are only permitted to use paper, a writing instrument, and an approved calculator when you take a quiz.

The sanctions for cheating are severe. The minimal sanction for cheating on a quiz is a score of 0 on every problem on which cheating occurred. Make sure that you act ethically when you take a quiz. If you do, you do not need to worry about any sanctions.

6.3 Civility Statement

The University of Akron is an educational community of diverse peoples, processes and programs. While all of us have our individual backgrounds, outlooks, values and styles, we all share certain principles of personal responsibility, mutual respect and common decency.

Our campus culture requires that we maintain and extend those principles, for without them we cannot thrive as a humane and worthwhile university.

We share an expectation to uphold the following principles of culture as part of our responsibility to promote a civil climate for learning on our campus:

- Intellectual culture
- Culture of diversity
- Caring culture
- Culture of civility
- Responsible culture

6.4 Diversity Statement

This class, as well as the broader University of Akron community, respects diversity and strives for equity and inclusion of all students. Diversity includes how we as individuals identify along the lines of race, color, religion, sex, sexual orientation, gender identity or expression, age, national or ethnic origin, citizenship status, disability, status as a parent during pregnancy and immediately after the birth of a child, status as a parent of a young child, status as a foster parent, or genetic information. Inclusion and respect for diversity make the classroom and the larger community stronger and foster dialogue and democratic decision making. As part of ensuring this class is a safe space for all students, please avoid use of negative stereotypes and insensitive or hateful statements toward individuals or groups of people. Please respect your classmates' pronouns. Each of us is responsible for creating a safe and inclusive learning environment.

7 Email Policy

All students are required to check their `uakron.edu` email account at least once a day for email from the instructor. If an email from the instructor has been received, then the email must be read carefully as soon as possible.

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

Students are required to use their `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 `uakron.edu` account.

8 Computer and Internet Access

Sufficient access to the Internet and to a fully functional computer is necessary. Please contact the instructor if you experience difficulty accessing the course online.

9 Textbook

You are not required to purchase a textbook. All course materials (videos, the notes made in the videos, homework problems, homework problem solutions, textbook chapters, etc.) are posted on the course website. All course materials have a Creative Commons Attribution 4.0 International (CC BY 4.0) or later version license, and they may be downloaded for offline use.

10 Calculator Requirement

Cybersecurity professionals rarely perform the computations that are taught in this course—the numbers used in practice are far too large for hand computations. Instead, those computations are performed by cryptography programs that implement the algorithms used for encryption and decryption. But all cybersecurity professionals need to understand exactly how the computations taught in this course are done—relying on an impenetrable black box that performs unfathomable computations is always a mistake in cybersecurity. To ensure that you know exactly how the important computations taught in this course are performed, the type of calculator you may use when you take a quiz is restricted as follows.

You are required to have a suitable non-programmable scientific calculator when you take a quiz. Such a calculator must have minimum functionality equivalent to that of the Texas Instruments TI-30XIIS scientific calculator. If you do not own such a calculator, you can purchase one for under $20.

Acceptable calculator models include the following:

- Texas Instruments TI-30XIIS, TI-30XS MultiView, TI-34 MultiView, TI-36X Pro models;
- Sharp EL-506, EL-531, EL-W516, EL-535 models;
- Casio fx-100MS, fx-100ES, fx-350MS, fx-350ES, fx-350MS, fx-570Es, fx-570MS, fx-82ES, fx-82MS, fx-85-ES, fx-85MS, fx-95ES, fx-95MS, fx-991ES, fx-991MS, fx-115ES, fx-115MS, fx-300ES, fx-300MS models;
- Hewlett Packard HP 10s+.

If a calculator you wish to use while taking a quiz does not appear on the above list, you are required to obtain written approval from the instructor before you use it while taking a quiz.

Performing computations during a quiz using any of the following is strictly prohibited:

- programmable scientific calculators and other programmable calculators;
- graphing calculators;
- calculators which have either a built-in or installed capability to function as a partial or full computer algebra system;
- calculators capable of being connected to a peripheral device;
- calculators, programs, extensions, or apps built into, installed onto, or written for web browsers, cell phones, smartphones, handheld computers, tablet computers, laptop computers, desktop computers, electronic writing pads, pen-input devices, and other electronic devices that are not solely non-programmable scientific calculators;
- cloud sevices including the results of a web search.

It is your responsibility to ensure that your calculator operates properly when you take a quiz. Keeping a properly functioning back-up calculator readily available is recommended. Mishaps due to a malfunctioning calculator are not given any consideration when a quiz is graded.

11 Working Offline

The course is designed so that most of your work can be done offline if you wish. All the lesson materials can be downloaded and saved for offline study.

It is possible to create a complete offline record of your work and progress in the course. You can do this by downloading the PDF file containing your grades when it is updated and downloading each graded quiz PDF.

It is a good idea to download and save all the lesson materials as well as creating a complete offline record of your work and progress. You will lose access to the lesson materials, the PDF file containing your grades, and the graded quiz PDFs shortly after the course ends.

This online course is designed to minimize the number of times you have to be online. It is designed so that you can concentrate on the course content instead of messing around too much with an online interface.

12 Course Components

All lessons and other course materials are posted online on the Applied Cryptanalysis website.

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

The course website contains the syllabus, lesson materials, 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.

12.1 Learning Periods and Quiz Periods

Lessons will be studied during eight *learning periods* and quizzes will be taken during eight *quiz periods*. Each learning period will be followed by a quiz period.

	Learning Period Dates	**Quiz Period Dates**
1	1/16–1/25	1/26
2	1/29–2/8	2/9
3	2/12–2/22	2/23
4	2/26–3/7	3/8
5	3/11–3/21	3/22
6	4/1–4/11	4/12
7	4/15–4/25	4/26
8	4/29–5/5	5/6–5/7

12.2 Lessons

Links to the lessons are given on the Lessons page of the course website.

Links to new lessons will be posted in the Current Lessons section of the Lessons page by the first the day of a learning period. Links to lessons studied previously will appear in the Previous Lessons section of the Lessons page.

Current lessons will be studied during the learning period dates that appear in the Current Lessons section. There are eight learning periods. The learning period dates appear below.

	Learning Period Dates
1	1/16–1/25
2	1/29–2/8
3	2/12–2/22
4	2/26–3/7
5	3/11–3/21
6	4/1–4/11
7	4/15–4/25
8	4/29–5/5

Lessons should be studied in the order they appear in the Current Lessons section.

Important: You are required to complete the lessons during the learning periods.

12.2.1 Good Practices

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 as soon as they are posted. Set aside ample time each day of the learning period to study the current lessons. By the end of a learning period, 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 sufficient time to ask the instructor questions, and you will understand the course material well enough to earn a good grade on a quiz.

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 good practices you should use to study the lessons use the principles of (1) *deliberate practice*, and (2) *practice at retrieval*. I will not present the principles in detail. Instead, the following instructions present a study process that uses both principles.

Do not consider a lesson to be completed until you thoroughly understand it. If there is something about a lesson you do not understand, then ask for help.

12.2.2 Lesson Description

A lesson consists of videos, the notes made in the videos, homework problems, homework problem solutions, and a textbook chapter.

The lesson videos, notes, homework problems, homework problem solutions, and textbook chapter can all be downloaded if you wish to work offline.

A lesson is divided into sections. Study the sections in the order they appear.

12.2.3 Lesson Section Instructions

1. Watch the video as if you were attending a class in a classroom.
    - Do not use other electronic devices (except for a calculator) or visit other web sites (unless the lesson requires it) when you are studying the video.
    - Take thorough, complete, and good notes as you watch the video.
        - Taking notes is an effective memory-retention technique that improves learning.
        - Do not be discouraged if there are items you do not understand. Working on the homework problems will help you learn the material, and you can always request help from Dr. Randby.
        - A link to the notes written in the video appears below the video. If you don't wish to take notes from scratch, you can download the notes, print them, and write your own annotations on the printed copy.
    - Pause the video when you want to perform a computation or some other task.

2. Once you have finished studying the video, work through the homework problems referring to your notes, and the lesson notes when necessary. Use the homework problem solutions only when you get completely stuck and when you check your work. Ask for help if you need it.
3. **Important:** Redo the homework problems until you can do them without referring to any other materials. It is best to do this several times.

12.3 Quizzes

Eight 50 point online quizzes will be given on Brightspace according to the schedule shown below.

Each quiz will cover the material covered in the lessons posted in the Current Lessons section on the Lessons page of the course website.

Students will be given 75 minutes to complete a quiz. The first 60 minutes is for taking the quiz, and the final 15 minutes is for making one or more PDF files of the written work, adding the PDF(s) to the quiz responses, and submitting the quiz.

The instructor will grade the quizzes, post graded quizzes on Brightspace as quiz feedback, and post the quiz grades on Brightspace in student grades files.

12.3.1 Quiz Schedule

Quizzes will be taken during the following quiz periods.

	Quiz Period Dates
1	1/26
2	2/9
3	2/23
4	3/8
5	3/22
6	4/12
7	4/26
8	5/6–5/7

Important: You are required to be prepared to take a quiz by the end of each learning period.

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

12.3.2 How to Take a Quiz

1. Before you take a quiz, make sure you have paper, a non-red writing instrument, and an approved calculator.
2. Log in to the course Brightspace site and click on the Quizzes link in the navigation bar.

3. Click on the link to the quiz, read the page, and start the quiz.
    - You will have 75 minutes to complete the quiz and submit your written work. The first 60 minutes is for taking the quiz, and the final 15 minutes is for making one or more PDF files of your written work, adding the PDF(s) to the quiz responses, and submitting the quiz.
    - If you submit the quiz after the time limit expires, there will be an automatic 10 point deduction (20%) from your quiz score. In addition, 5 points (10%) will be deducted for every 5 minute period that exceeds the time limit.
4. DO NOT enter ANY text into the response area that appears below the quiz. Your work and results will be submitted as one or more PDF files (submission instructions appear after the quiz problems).
5. DO NOT copy the quiz questions on your written work. Copy only the essential information you need to use to solve the problems.
6. Here are the requirements for your written work:
    - Clearly number each problem and each part of a problem.
    - All work and answers must appear.
    - Show all relevant work.
    - Do not use a red pen or red pencil.
    - Do not circle, underline, or box answers.
7. When you are finished, (1) make one or more PDF files that show your written work, (2) open the PDF files in a PDF reader to make sure they meet course requirements, (3) click on the Add a File button below the response box and add the PDF files that show your written work, and then (4) click on the Submit Quiz button to submit the quiz.

12.3.3 Creating Written Work Files

Your written work on a quiz will be evaluated and graded. Here are the requirements for that work:

- Clearly number each problem and each part of a problem.
- All work and answers must appear.
- Show all relevant work.
- Do not use a red pen or red pencil.
- Do not circle, underline, or box answers.

When you take a quiz, you will have to attach one or more PDF files containing all of your written work. Each PDF file of your written work must meet the following six requirements.

1. Proper orientation. This means that the writing must be able to be read from left to right when the file is opened.
2. Each page of the PDF has portrait orientation. This means that each page is taller than it is wide. For example, a letter-size page with portrait orientation will have width 8.5 inches and height 11 inches. A letter-size page with landscape orientation, which is unacceptable, has width 11 inches and height 8.5 inches.
3. The edges of a piece of paper are exactly or very close to the boundary of a page of the PDF. Images should be of the entire sheet of paper. Do not cut off parts of a sheet of paper or zoom in to show only part of a sheet of paper.

4. A sheet of paper should be flat when an image is taken of it, and the image should be taken directly above the sheet of paper. This means that using a notebook from which pages cannot be removed won't work.
5. Writing should be dark enough to be easily read (no red please), and the sheet of paper should be white or a light color. Please try to avoid shadows when you make an image of a sheet of paper.
6. A PDF reader program should also be able to open the file.

I also want you to try to create PDFs that meet the following goals. These goals are not requirements. If you cannot determine a quick and easy way to meet some or all of the goals, you will not be penalized.

1. The size of each page of a PDF is letter size (8.5 inches x 11 inches) or close to that size. It is very helpful if you meet this goal. Some programs that people use make PDFs that have A4 size which is okay, but, in this country, we use letter size in most cases.
2. File size under 5 MB. Actually, you should be able to keep the file size under 1 MB. If you don't know how to reduce the file size of a PDF and your PDFs have large file size, then you might have trouble uploading your PDF before the time limit on a quiz is exceeded.

There are many ways of converting written work to PDF files. Here are a few:

Method 1: (1) Take a picture of each page of your written work using your phone, (2) open up each picture and print it to a PDF on your phone (explained for Android phones below), (3) download the PDF files to your computer and submit them in Brightspace.

Method 2: (1) Take a picture of each page of your written work using your phone, (2) download each picture to your computer, (3) open up each picture in an application that permits printing and print to PDF.

Method 3: Use handwriting note taking software and write your work directly into the computer. Convert the result to PDF.

Method 4: Scan pages directly to PDF if you have a scanner that can do such a thing.

Warning: If you use software to record quiz work instead of writing your work on paper, no reprieve will be given if the software malfunctions and your work is lost.

Here is the Method 1 process for Android phones:

1. Take a good picture of a page of your work.
2. Open the picture. Press on the three vertical dots on the upper right side and select Print.
3. Print to a PDF file. The process may vary slightly depending on your phone.
4. Repeat steps 1–3 for the remaining pages of your work.
5. Download all of the PDF files that show your written work on the quiz from your phone to your computer.

Important: You will have 15 minutes after you take a quiz to create and attach your written work as one or more PDF files. Before you take a quiz, practice making PDF files of written work to ensure you can complete the process of creating and attaching them in 15 minutes or

less.

Before the PDFs of your quiz work are graded, they are downloaded and processed using the command line utilities `pdfunite` and `gs` to create a single good quality PDF that has relatively small file size and letter size pages. The utility `pdfunite` is part of Poppler, and `gs` is part of Ghostscript. The PDFs are processed as follows:

1. Join the PDF files if necessary.

   ```
   pdfunite quiz-file-1.pdf quiz-file-2.pdf joined.pdf
   ```

2. Reduce the file size of `joined.pdf` and scale its pages to letter size.

   ```
   gs -sDEVICE=pdfwrite -dFIXEDMEDIA -dPDFFitPage -dAutoRotatePages=/None
   -sPAPERSIZE=letter -dPDFSETTINGS=/ebook -dNOPAUSE -dQUIET -dBATCH
   -sOutputFile=processed.pdf joined.pdf
   ```

The the file `processed.pdf` is opened using Xournal++, graded, the graded Xournal++ file is exported to `graded.pdf`, and `graded.pdf` is uploaded to Brightspace.

12.3.4 Quiz Submission Policies

When you take a quiz, you will see a response box. You may not enter any text into the response box. The reason for this requirement is to ensure that you receive a warning if you try to submit a quiz without adding the PDF files that show your written work. You do not receive the warning if you've entered text into the response box.

Entering text into the quiz response box will result in a one point deduction from your quiz score.

The time you have for working on a quiz and attaching your work ends when you submit the quiz. Just as you cannot turn in an exam after you've left the exam room, you cannot turn in quiz work after you've left the online "quiz room." The only place you can turn in your quiz work is inside the quiz room. Work turned in after you've submitted a quiz does not count as quiz work and is not accepted.

If you try to submit a quiz without attaching the PDF files that show your written work, a warning will appear unless you entered text into the response box (see figure 1). If you ignore the warning and submit the quiz instead of returning to it to attach your written work and click on the Submit Quiz button again, then you will have turned in no work.

Submitting a quiz without attaching the files that contain your written quiz work can have a major negative impact on your final course grade, an impact which might result in not passing the course. Make sure that you always attach the PDF files that contain your written quiz work before you submit a quiz.

After you've submitted a quiz, you will see a screen that verifies that that quiz has been submitted (see figure 2).

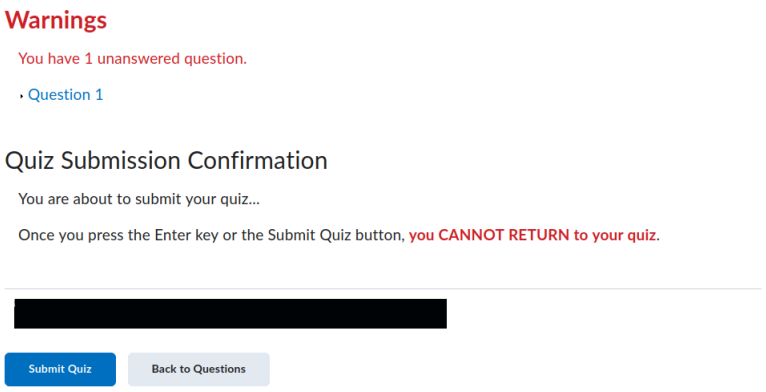

Figure 1: Brightspace quiz warning

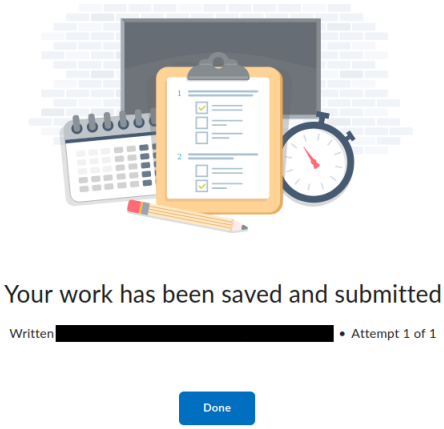

Figure 2: Brightspace quiz submitted screen

Only the files you attach before you submit a quiz will be graded. If you attach the wrong files, then you won't receive any credit for the work you included in the correct files.

Any of the following will result in a deduction of between 1 and 5 points from a quiz score:

- Turning in written work that is not in PDF format
- Turning in written work that does meet all six of the PDF requirements
- Turning in PDF files that cannot be easily processed and converted to a gradable form

12.3.5 Failing to Attach Written Quiz Work

If you submit one of the first six quizzes without attaching the files that contain your written quiz work and it is the first time you failed to attach your work, then you might be eligible to retake the quiz. If you are not eligible to retake the quiz, then your score on the quiz will be 0. See the following section for more information.

If you submit one of the first six quizzes without attaching the files that contain your written quiz work and it is not the first time you failed to attach your work, then your score on the

quiz will be 0.

If you submit Quiz 7 or Quiz 8 without attaching the files that contain your written quiz work, then your score on the quiz will be 0.

12.3.6 Retaking a Quiz

All students are permitted to retake one and only one of the first six quizzes. A request to retake a quiz must be made via email. You may submit a request to retake a quiz any time before 11:59 p.m. on Friday, April 19. Requests submitted after that deadline will not be granted.

If you make a request to retake a quiz and the request is granted, then your score on the retake replaces your score on the quiz. This means you should be absolutely sure that retaking a quiz is the right decision. Some of the reasons justifying retaking a quiz include:

- you didn't take the quiz,
- you didn't attach your work when you took the quiz,
- you failed the quiz.

If you make a request to retake a quiz and the request is granted, then Dr. Randby will set the date of the retake based on the information you supplied in the request email and the amount of time it will take Dr. Randby to construct the retake.

The difficulty level of a retaken quiz will be equivalent to the difficulty level of the quiz.

If you retake a quiz and fail to attach the files that contain your written quiz work, then your score on the quiz will be 0.

You may not retake a quiz on which you were caught cheating.

12.3.7 Make-up Quizzes

If you miss a quiz, then you may request a make-up quiz. If you request a make-up quiz, then you must have an excusable reason for missing the quiz. Dr. Randby reserves the right to require you to provide additional information or documentation when you request a make-up quiz. Making the request does not guarantee that a make-up quiz will be granted.

Make-up quizzes are not meant to deal with failures to meet course requirements without an excusable reason. Make-up quizzes are meant to deal with emergencies, illnesses, mandatory attendance at university-sponsored events, and other events that are beyond your control.

It your responsibility to request a make-up quiz. Make-up quiz requests must be made via email. Make-up quiz requests should be made as soon as possible.

If you access a quiz on Brightspace, then you are not eligible for a make-up quiz.

Please be aware of the fact that missing a quiz without having an excusable reason for missing it will have a major negative impact on your final course grade, an impact which might result in not passing the course.

12.3.8 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

- Perfect work: -0
- A work with minor errors: -0.1
- B work: -0.2
- C work: -0.3
- D work: -0.4
- F work: -0.5 to -1
- Required work missing: -0.4 to -1
- No work: -1

12.3.9 The Purpose of Quizzes

Quizzes are not learning tools, they are where learning is demonstrated. Quiz solutions are not distributed, and you should not expect to learn from your mistakes on a quiz.

13 Getting Help

Instructions for getting help are given on the Help page of the course website. The following information is given on the Help page.

13.1 Email Help

Students may send questions about the course lessons and homework problems to Dr. Randby via email. Questions should be sent to `srandby@uakron.edu` from a `uakron.edu` account.

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.

13.2 Live Online Help

Students may obtain live online individual or group help (audio, video, chat, screen sharing, etc.) with Dr. Randby in a Teams room. Do the following to schedule a meeting with Dr. Randby in a Teams room:

1. Log in to Brightspace and enter the course.
2. Follow the instructions given in the LIVE ONLINE HELP section of the home page.

Live online help sessions are not recorded. The notes made during a live online help session are sent to participants via email.

14 Course Grade

All grades will be posted on Brightspace. To view your grades, do the following:

1. Log into the course on Brightspace.
2. Click on the Grades link in the navigation bar.
3. Download the PDF file containing your grades.

Use the following to determine your *numerical course grade* G.

$qnum =$ the number of quizzes given
$qmax =$ the maximum possible points on a quiz
$qsum =$ 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	$91 \leq G \leq 100$	C	if	$71 \leq G < 77$
A−	if	$90 \leq G < 91$	C−	if	$70 \leq G < 71$
B+	if	$87 \leq G < 90$	D+	if	$67 \leq G < 70$
B	if	$81 \leq G < 87$	D	if	$63 \leq G < 67$
B−	if	$80 \leq G < 81$	D−	if	$60 \leq G < 63$
C+	if	$77 \leq G < 80$	F	if	$G < 60$

15 Course Content and Objectives

15.1 Course Description

Course: MATH 461 Applied Cryptanalysis
Credits: 3
Prerequisite: MATH 361 Applied Cryptography with a grade of C or better
Course Description: Cryptanalysis concepts; cryptanalysis of symmetric and public key cryptosystems, key exchange systems, and digital signatures; hash function collision resistance; cryptanalysis with quantum computers.

15.2 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.

15.3 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

15.4 Bibliography

1. Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography, Third Edition*, Chapman & Hall/CRC Cryptography and Network Security Series. CRC Press, 2021.
2. J Vacca. *Computer and Information Security Handbook, 2nd Edition*. Elsevier, 2013.
3. Margaret Cozzens and Steven Miller. *The Mathematics of Encryption: An Elementary Introduction*. Mathematical World, V. 29. American Mathematical Society, 2013.
4. Samuel Wagstaff. *The Joy of Factoring*. Student Mathematical Library, V. 68. American Mathematical Society, 2013.
5. Alasdair McAndrew. *Introduction to Cryptography with Open-Source Software*, Discrete Mathematics and its Applications series. CRC Press, 2011
6. Niels Ferguson, Bruce Schneier, Tadayoshi Kohno. *Cryptography Engineering: Design Principles and Practical Applications*. Wiley, 2010.
7. Christof Paar and Jan Pelzl. *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer, 2010.
8. M. Jason Hinek. *Cryptanalysis of RSA and Its Variants*, Cryptography and Network Security Series. Chapman & Hall/CRC, 2009.
9. Antoine Joux. *Algorithmic Cryptanalysis*, Cryptography and Network Security Series. Chapman and Hall/CRC, 2009.
10. Christopher Swenson. *Modern Cryptanalysis: Techniques for Advanced Code Breaking*. Wiley, 2008.
11. Jeffrey Hoffstien, Jill Pipher, and Joseph Silverman. *An Introduction to Mathematical Cryptography*. Springer, 2008.
12. Shafi Goldwasser and Mihir Bellare. *Lecture Notes on Cryptography*. Available at https://cseweb.ucsd.edu/~mihir/papers/gb.pdf, 2008.
13. Niels Ferguson. *Practical Cryptography*. Wiley, 2003.
14. Bruce Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. John Wiley & Sons, Second Edition, 1996.
15. Albrecht Beutelspacher. *Cryptology*. Mathematical Association of America, 1994.

16 University Policies

16.1 Undergraduate Bulletin

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

16.2 Incomplete Policy

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

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

16.3 Withdrawal Policy

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

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

The withdrawal deadline for this course is **Sunday, March 3**.

17 Accessibility, Support, Counseling, and Health Services

Pursuant to the Section 504 of the Rehabilitation Act of 1973, and Title II of the Americans with Disabilities Act (ADA) of 1990, The University of Akron does not discriminate against any student because of a disability, and the university does not exclude any qualified student with a disability from participation in or from receiving the benefits of the services, programs, or activities of the University.

The preceding paragraph means that the university recognizes its responsibility for creating an institutional atmosphere in which students with disabilities have the opportunity to be successful. Any student who feels a need for an accommodation based on the impact of a disability should contact the Office of Accessibility at 330-972-7928 or `access@uakron.edu`. The office is located in Simmons Hall Room 105.

After a student's eligibility for services is determined, that student's instructors will be provided with a letter which outlines the student's accommodations.

ZipAssist is a central information hub that shares available resources, and provides support and assistance to help students be successful at the university.

Currently enrolled students may obtain free psychological services at the Counseling & Testing Center.

Individual counseling is available at the Psychology Department Counseling Clinic.

Counseling services for individuals, couples, families and groups across all ages, cultures and mental health concerns in the Greater Akron community are available at the Clinic for Individual and Family Counseling.

Currently enrolled students may obtain low cost health services at Student Health Services.

18 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.

Information about obtaining help is available on the Types of help for sexual misconduct web page.

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 the Title IX at The University of Akron web page.

19 Ohio Revised Code Section 3345.026

Pursuant to Ohio Revised Code Section 3345.026 you may request a religious accommodation to be excused from class up to three (3) days for reasons of faith or religious or spiritual belief system to participate in organized activities conducted under the auspices of a religious denomination, church, or other religious or spiritual organization.

The request for excusal must be made, in writing, during the first fourteen (14) days of the semester and include the date(s) of each proposed absence or request for alternative accommodation. The request must clearly state that the proposed absence is to participate in religious activities. The request must also provide the particular accommodation(s) you desire.

You will be notified by me if your request is approved, or, if it is approved with modification.

For more information regarding this Policy you may contact the University EEO Office at:

Office of Equal Employment Opportunity and Affirmative Action
University of Akron
The Administrative Services Building
185 East Mill Street
Room 138
Akron, OH 44325
(330) 972-7300 | Phone
(330) 972-5816 | Fax
EEOcompliance@uakron.edu