Applied Cryptography Syllabus

Table of Contents

1 Basic Information .................................................. 2
   1.1 Schedule ..................................................... 2

2 Overview ................................................................ 3

3 Important Note ..................................................... 3

4 Instructor and Student Roles ..................................... 3

5 Ethics .................................................................. 3
   5.1 Academic Honesty and Student Conduct ............... 4
   5.2 Academic Honesty on Quizzes ......................... 4

6 Syllabus Policy ..................................................... 5

7 Email Policy ......................................................... 5

8 Computer and Internet Access .................................. 5

9 Textbook .............................................................. 5

10 Calculator Requirement ......................................... 5

11 Course Components .............................................. 6
   11.1 Learning Periods and Quiz Periods .................... 6
   11.2 Lessons .......................................................... 6
      11.2.1 Good Practices .......................................... 7
      11.2.2 Lesson Instructions .................................... 7
      11.2.3 Lesson Section Instructions ....................... 8
   11.3 Quizzes .......................................................... 8
      11.3.1 Quiz Schedule .......................................... 8
      11.3.2 How to Take a Quiz ................................. 9
      11.3.3 Written Work .......................................... 9
      11.3.4 Email Submissions of Quiz Work ............... 11
      11.3.5 Make-Up Quizzes ..................................... 11
      11.3.6 Quiz Grading .......................................... 11

12 Getting Help ........................................................ 12
   12.1 Email Help .................................................... 12
   12.2 Live Online Help ............................................ 12

13 Course Grade ....................................................... 13

14 Course Content and Objectives ............................... 13
1. Basic Information

Course: Applied Cryptography, 2030 361-502 (74533)
Course Type: Online
Length: 8/23/2021–12/5/2021
Course Web Site: https://srandby.org/2021-3/361-502/home.html
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

<table>
<thead>
<tr>
<th>Assignment</th>
<th>Due Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Making a PDF</td>
<td>8/27 at 11:59 p.m.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Learning Period Dates</th>
<th>Quiz Period Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 8/23–9/1</td>
<td>9/2–9/3</td>
</tr>
<tr>
<td>2 9/7–9/16</td>
<td>9/17</td>
</tr>
<tr>
<td>3 9/20–9/30</td>
<td>10/1</td>
</tr>
<tr>
<td>4 10/4–10/14</td>
<td>10/15</td>
</tr>
<tr>
<td>5 10/18–10/28</td>
<td>10/29</td>
</tr>
<tr>
<td>6 11/1–11/11</td>
<td>11/12</td>
</tr>
<tr>
<td>7 11/15–11/22</td>
<td>11/23</td>
</tr>
<tr>
<td>8 11/29–12/5</td>
<td>12/6–12/7</td>
</tr>
</tbody>
</table>
2 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 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.

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.

3 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. When you work in the cybersecurity field, you will have to use cryptography every day. You cannot use cryptography properly in cybersecurity unless you have a good understanding of how it works.

Some of the topics in the course will be review material covered in Applied Finite Mathematics. It is important to review this material so that you won’t struggle to remember it.

4 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.

5 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. How to do so appears below.

5.1 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.

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/

5.2 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;
- obtaining any information about the quiz problems or their solutions from any another person (except the instructor) before, during, or after taking a quiz;
- obtaining help solving quiz problems from any other person (except the instructor) before, during, or after taking a quiz;
- sharing any information about the quiz problems or their solutions with any another person (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;
- not being truthful about your actions regarding a quiz.

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

The sanctions for cheating are severe. Make sure that you act ethically when you take a quiz. If you do, you do not need to worry about any sanctions.
6 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 the document which 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, and know when you need to study and take quizzes.

7 Email Policy

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

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

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.
11 Course Components

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

11.1 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.

<table>
<thead>
<tr>
<th>Learning Period Dates</th>
<th>Quiz Period Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 8/23–9/1</td>
<td>9/2–9/3</td>
</tr>
<tr>
<td>2 9/7–9/16</td>
<td>9/17</td>
</tr>
<tr>
<td>3 9/20–9/30</td>
<td>10/1</td>
</tr>
<tr>
<td>4 10/4–10/14</td>
<td>10/15</td>
</tr>
<tr>
<td>5 10/18–10/28</td>
<td>10/29</td>
</tr>
<tr>
<td>6 11/1–11/11</td>
<td>11/12</td>
</tr>
<tr>
<td>7 11/15–11/22</td>
<td>11/23</td>
</tr>
<tr>
<td>8 11/29–12/5</td>
<td>12/6–12/7</td>
</tr>
</tbody>
</table>

11.2 Lessons

Links to the lessons are given on the Lessons page of the course website available at the following address.


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.
<table>
<thead>
<tr>
<th>Learning Period Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 8/23–9/1</td>
</tr>
<tr>
<td>2 9/7–9/16</td>
</tr>
<tr>
<td>3 9/20–9/30</td>
</tr>
<tr>
<td>4 10/4–10/14</td>
</tr>
<tr>
<td>5 10/18–10/28</td>
</tr>
<tr>
<td>6 11/1–11/11</td>
</tr>
<tr>
<td>7 11/15–11/22</td>
</tr>
<tr>
<td>8 11/29–12/5</td>
</tr>
</tbody>
</table>

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.

### 11.2.1 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 following instructions are meant to encourage students to use good learning practices while studying a lesson.

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.

### 11.2.2 Lesson Instructions

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.
11.2.3 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.

11.3 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 and submit their 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 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.

11.3.1 Quiz Schedule

Quizzes will be taken during the following quiz periods.
<table>
<thead>
<tr>
<th>Quiz Period Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 9/2–9/3</td>
</tr>
<tr>
<td>2 9/17</td>
</tr>
<tr>
<td>3 10/1</td>
</tr>
<tr>
<td>4 10/15</td>
</tr>
<tr>
<td>5 10/29</td>
</tr>
<tr>
<td>6 11/12</td>
</tr>
<tr>
<td>7 11/23</td>
</tr>
<tr>
<td>8 12/6–12/7</td>
</tr>
</tbody>
</table>

**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.

### 11.3.2 How to Take a Quiz

1. Before you take a quiz, make sure you have paper, a writing instrument (not red) and a suitable calculator.
2. Log into Brightspace 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. 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.

### 11.3.3 Written Work

Your written work on a quiz will be evaluated. 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 submit one or more PDF files containing all of your written work. Each PDF file of your written work must meet the following 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.

Any of the following will result in a 5 point deduction (10% of 50) from a quiz score.

- Submitting written work that is not in PDF format.
- Submitting written work that does meet all of the above requirements

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.

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 submit 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 making and submitting them in 15 minutes or less.
11.3.4 Email Submissions of Quiz Work

Quiz work that is submitted via email is not accepted. Quiz work files that are sent via email are not opened nor are they graded.

11.3.5 Make-Up Quizzes

Students are required to take a quiz during its quiz period 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) completion of prior quizzes, and (4) 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.

11.3.6 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
12 Getting Help

Instructions for getting help are given on the Help page of the course website available at the following address:


The following information is given on the Help page.

12.1 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.

12.2 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 enter the 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.
3. If Dr. Randby is not in the room, you will have to wait to enter until he starts the session.

Dr. Randby will be in the Teams room during the following online office hours:

- **Monday:** 3:00–4:00 p.m.
- **Tuesday:** 3:00–4:00 p.m.
- **Wednesday:** 3:00–4:00 p.m.

If you want to meet with Dr. Randby in the Teams room at a time not listed above, then send an email to Dr. Randby requesting a live online help session. If possible, please provide more than one starting time suggestion for the session. Dr. Randby will reply and emails will be exchanged until a starting time is agreed on.

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

$$
gnum = \text{the number of quizzes given} \\
gmax = \text{the maximum possible points on a quiz} \\
gsum = \text{the sum of the scores earned on the quizzes}
$$

$$
G = \frac{100 \cdot gsum}{gnum \cdot gmax}
$$

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

<table>
<thead>
<tr>
<th>Grade</th>
<th>Range</th>
<th>Grade</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>$91 \leq G \leq 100$</td>
<td>C</td>
<td>$71 \leq G &lt; 77$</td>
</tr>
<tr>
<td>A−</td>
<td>$90 \leq G &lt; 91$</td>
<td>C−</td>
<td>$70 \leq G &lt; 71$</td>
</tr>
<tr>
<td>B+</td>
<td>$87 \leq G &lt; 90$</td>
<td>D+</td>
<td>$67 \leq G &lt; 70$</td>
</tr>
<tr>
<td>B</td>
<td>$81 \leq G &lt; 87$</td>
<td>D</td>
<td>$63 \leq G &lt; 67$</td>
</tr>
<tr>
<td>B−</td>
<td>$80 \leq G &lt; 81$</td>
<td>D−</td>
<td>$60 \leq G &lt; 63$</td>
</tr>
<tr>
<td>C+</td>
<td>$77 \leq G &lt; 80$</td>
<td>F</td>
<td>$G &lt; 60$</td>
</tr>
</tbody>
</table>

14 Course Content and Objectives

14.1 Bulletin Description

Prerequisite: A grade of C or better in 2030:216. Symmetric cryptography, modular arithmetic, stream and block ciphers, random numbers, Advanced Encryption Standard, public-key cryptography, key exchange, digital signatures, hash functions, message authentication.

14.2 Course Objectives

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

1. an understanding of the basic concepts of symmetric cryptography including symmetric keys, cleartext, ciphertext, and simple encryption methods such as the replacement cipher;
2. an understanding of the basic concepts of cryptanalysis and the methods used to attack an encryption system;
3. the ability to do computations in a ring of integers modulo n and an understanding of ciphers that use such rings;
4. an understanding of simple stream ciphers;
5. an understanding of the different types of random number generators that are used in 
cryptography and the ability to use random number generators to create ciphers such as a 
one-time pad;
6. an understanding of the important modes of operation for block ciphers;
7. a basic understanding of Galois fields and the ability to do computations in \( GF(p^n) \);
8. an understanding of the structure of the Advanced Encryption Standard (AES) and the 
ability to encrypt and decrypt messages using the AES;
9. an understanding of the principles and common applications of public-key cryptography,
and the primary number theory used in public-key cryptography;
10. an understanding of the RSA cryptosystem, the mathematics used in the system, and the 
ability to encrypt and decrypt cleartext using the system;
11. an understanding of the Diffie-Hellman key exchange and its applications;
12. an understanding of the basic digital signature protocol and the ability to use the RSA 
signature scheme;
13. an understanding of the purpose, security requirements, and properties of hash functions 
and the ability to use common hash function algorithms;
14. an understanding of the properties of message authentication codes and the ability to use 
hash functions to build a message authentication code.

14.3 Course Outline

1. Basics of cryptography
2. Symmetric encryption
   • Replacement cipher
3. Basic cryptanalysis
4. Modular arithmetic
   • The ring of integers modulo n
5. Stream ciphers
6. Random numbers
   • Random number generators
   • The one-time pad
7. Encryption using block ciphers
   • Modes of operation
8. The Advanced Encryption Standard (AES)
   • Galois fields
   • Structure of the AES
   • AES decryption
9. Public-key cryptography
   • Principles
   • One-way functions
   • Applications: key establishment, nonrepudiation, identification, encryption
   • The Euclidean and extended Euclidean algorithms
   • Euler’s \( \phi \) function
   • Fermat’s little theorem and Euler’s theorem
10. The RSA cryptosystem
11. Key exchange
   • Diffie-Hellman key exchange
   • Basic group theory (cyclic groups and their subgroups) (optional)
   • The discrete logarithm problem (optional)
   • Security of Diffie-Hellman key exchange (optional)

12. Digital signatures
   • Basic digital signature protocol
   • The RSA signature scheme

13. Hash functions
   • The purpose of hash functions
   • Hash function security requirements and properties
   • Hash function algorithms

14. Message authentication
   • Properties of message authentication codes
   • Building a message authentication code from a hash function

14.4 Bibliography


15 University Policies

15.1 Undergraduate Bulletin

The university policies that affect students are contained in the Undergraduate Bulletin.
15.2 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.

15.3 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, October 10.

16 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 in a timely manner. 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/

17 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.

Click on the following link to see information about obtaining help.

https://uakron.edu/title-ix/get-help/

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/.