# CPSC5555   Selected Topics in Computer Science

# CRYPTOGRAPHY

# CRNs 22463(U) and 22128(G) Spring 2014

# Class Meets: WF 11-12:15pm in CCT 405 and 407 on announced dates

### 

### **INSTRUCTOR INFORMATION**

### Name: Dr. Yeşem Kurt Peker

### Office: Center for Commerce and Technology (CCT) Room 422

### Office hours:

### Mon: 11–12pm, 2-3pm Tue: 11-12pm, 1-2pm

### Wed: 1-4pm

### Thu: 11-12pm, 1-2pm

### Fri: 12:30-1:30pm

### and by appointment

### CATALOG DESCRIPTION OF COURSE

This course features a rigorous introduction to modern cryptography, with an emphasis on the fundamental cryptographic primitives of symmetric and public-key encryption, basic cryptanalysis, hash functions, and digital signatures. The course requires some “maturity” in computational thinking; that is mathematical thinking and programming.

**Prerequiste:** CPSC2108 (completed with a grade of C or better) or consent of the instructor.

**Textbook:**

|  |  |
| --- | --- |
| http://www.justtextbook.com/images/9780136097044.jpg | ***Title:*** [Cryptography and Network Security, 5th Edition](http://bcs.wiley.com/he-bcs/Books?action=index&bcsId=5327&itemId=0470509481)  ***Author:* William Stallings**  ISBN 10: 0-13-609704-9  ISBN 13: 978-0-13-609704-4 |

**Note that the book has to be the 5th edition.**

Supplementary Books and Materials

* Materials on course website in CougarView
* Class handouts & notes
* Software and manuals found in the computer labs and on the Internet

**Software** Java and Mathematica

###### COURSE OBJECTIVES

### The goal of this course is to provide an introduction to cryptography, its mathematical foundations, its relation to security, and implementation of protocols used in applications.

###### COURSE OUTCOMES & ASSESSMENT METHODS

* Students will demonstrate knowledge of cryptography concepts, mathematics behind them, and their role in information security.
  + Strategies and Actions used to produce the outcome:
    - Study of necessary background in mathematics
    - Study of necessary background in information security
    - In-class activities
  + Program Objectives covered: 1 and 2
  + Assessment Methods: Written and programming assignments; exams; reading and presenting research papers
* Students will demonstrate knowledge of basic cryptographic protocols as well as the ability to implement them.
  + Strategies and Actions used to produce the outcome:
    - Study of necessary background in information security
    - Study of concepts in designing cryptographic protocols
    - In-class activities
    - Read and write complex programs in a programming language.
  + Program Objectives covered: 2 and 3
  + Assessment Methods: Written and programming assignments and exams.
* Students will demonstrate knowledge of cryptanalysis of symmetric and asymmetric cryptosystems and implementation of algorithms for cryptanalysis of symmetric ciphers
  + Strategies and Actions used to produce the outcome:
    - Study necessary background in mathematics
    - Study necessary background in information security
    - In-class activities
    - Read and write complex programs in a programming language.
  + Program Objectives covered: 1,2,3
  + Assessment Methods: Written and programming assignments and exams.
* Students will demonstrate knowledge of contemporary issues in cryptography and the ability to communicate them effectively
  + Strategies and Actions used to produce the outcome:
    - Study necessary background in mathematics
    - Study necessary background in information security
    - In-class activities
  + Program Objectives covered:1, 2 and 4
  + Assessment Methods: Written and programming assignments, exam, reading and presenting research papers.

###### CS Program Objectives

Our graduates will have achieved:  
1) A broad general education assuring an adequate foundation in science and mathematics relevant to computing.   
2) A solid understanding of concepts fundamental to the discipline of computer science.  
3) Good analytic, design, and implementation skills required to formulate and solve computing problems.  
4) The ability to function and communicate effectively as ethically and social responsible computer science professionals

###### MAJOR TOPICS

* Mathematical background – Modular arithmetic, discrete probability, elementary number theory, basics of finite fields
* Symmetric key cryptography: early and modern ciphers
* Cryptanalysis –attack models
* Public key cryptography
* Key agreement
* Encryption/decryption
* Hash functions
* Digital Signatures
* Other applications of cryptography

###### ASSESSMENT CRITERIA

* **Short Assignments** (100 pts.)Approximately one short assignment (written or programming) will be assigned every week to be turned in the next week. Solutions to assignments will be typed in an electronic file and submitted through the dropbox. The assignments will require group work when indicated.
* **Programming Assignments** (200pts.) These assignments will be moderately complex programming assignments where you will implement some of the cryptographic algorithms and their cryptanalysis. . The assignments will require group work when indicated.
* **Midterm test** (100 pts.) **(Friday, March 14)**
* **FINAL EXAM** (200 pts.)
  + Exams test material from the lectures, readings and programming exercises. The exams may include multiple choice, fill in the blanks, short answer questions and programming questions (*you will be asked to write code*). All exams are closed book, closed notes, no calculators. If you miss any quiz or exam or are absent for that class, it will not be made up.
* **Literature review, reading research papers, and presentations** (100pts)
  + Students will do a literature review on current issues in cryptography; read in detail some of the papers, and give a presentation to class on their findings. Students can pick a topic of their choice. They need to consult with the instructor throughout the process.
* **Class Participation** – will be considered for students who are on the borderline between two grades

 The letter grades will be assigned according to the following criteria:

**A (90-100)**: The student fulfills or exceeds all of the assigned content requirements. The student’s knowledge of the subject is accurate throughout. The student exhibits convincing range and quality of knowledge, having done appropriate research, if applicable.

**B (80-89**): The student fulfills all of the important assigned content requirements. The student’s knowledge of the subject is accurate throughout except in minor details. The student seems informed on the subject, having done appropriate research, if applicable

**C (70-79**): The student fulfills most of the important assigned content requirements. The student’s knowledge of the subject is generally accurate, though flawed. The student exhibits limited range or quality of knowledge, having done limited appropriate research, if applicable.

**D (60-69**): The student fulfills some of the important assigned content requirements. The student’s knowledge of the subject is generally accurate, though flawed. The student exhibits limited range or quality of knowledge, having done minimal appropriate research, if applicable.

**F (0-59**): The student fails to address the important requirements of the course.  
The student’s knowledge of the subject is generally inaccurate. The student’s knowledge of the subject lacks range or quality

###### ****Instructional Methods and Techniques****

1. The class will meet twice a week for seventy-five minute lecture / discussion / lab periods each week. Tuesday classes will be in class and Thursday classes will be in the lab every two weeks starting with the first week.
2. Each student is expected to attend all class lectures, to read the textbook chapters and other required material, and to make notes. Students will be expected to participate in classroom discussions, both in class and online.
3. Students must have access to computers for doing assignments.
4. The ACM recommends the following: “As a general guideline, the amount of out-of-class work is approximately ***three times*** the in-class time. Thus, a unit that is listed as requiring 3 hours typically entails a total of 12 hours (3 in class and 9 outside).” Students will be expected to spend this time outside class reading the book, online materials and other materials; writing solutions to homework exercises and programming projects.

**How to Access the Course**

CougarVIEW uses a course management system called Desire2Learn (D2L). For our purposes, the terms CougarVIEW and D2L will mean the same thing. The CougarView Starter Guide is available for your review at [www.columbusstate.edu/cougarviewstarterguide](http://www.columbusstate.edu/cougarviewstarterguide).

This course includes CougarView. You can access CougarView at: https://colstate.view.usg.edu/

Your CougarVIEW username is the same as your CougarNet login ID & password.

Students who add courses during the first week of the semester, should be able to access their newly added course within 24-36 hours.  
For additional help contact the CSU Help Desk (CCT building level 1, phone: 706-507-8199).

Once you've entered CougarView, you will see a list of courses you have access to. The CPSC 555 course is listed as "Selected Topics in CS". Next to this, you should see my name as the instructor. You may also see new calendar postings and email messages. Clicking on the name of the course will take you to the course's home page. If you do not see the "Selected Topics in CS". course in the list, please e-mail me immediately.

Note: One common reason for not being able to see the course in CougarView after you log in is late enrolment in the course. From past experience, it usually takes a couple of days after enrolment for the updated student database to be reflected in CougarView.

Once you have clicked on the course's name and accessed the course, you will find a home page with a navigational bar displaying the course title and a set of links that is used to navigate between tools and homepages. Each course and home page has its own navigational bar that links to relevant tools and contents. Contents such as lecture notes and assignments will be progressively added to the course during the semester.

It is your responsibility to frequently look at the course website in CougarView to keep your knowledge of class activities current. I may occasionally forget to announce details in class, but they may have been already posted on the site and/or in CougarView. If so, you will still be held responsible for them. For example, assignment due dates, corrections of errors, announcements, exam dates, changes to policies, and so on.

###### ****Student Responsibilities****

As a student in this course, you are responsible to:

* manage your time and maintain the discipline required to meet the course requirements,
* come to class prepared to ask questions to maximize your understanding of the material,
* complete all readings,
* complete all assignments,
* complete all exams,
* actively participate in discussions,
* attempt all exercises given during the class,
* submit the “one-minute paper” after each class, and
* read any e-mail sent by the instructor and respond accordingly within 48 hours.

*“I didn’t know”* is **NOT** an acceptable excuse for failing to meet the course requirements. If you fail to meet your responsibilities, you do so at your own risk.

###### ****Instructor Responsibilities****

As your instructor in this course, I am responsible to:

* introduce the topic to be learned each week and explain concepts and techniques
* clarify topic issues and answer students’ questions,
* post homework assignments in CougarView and introduce them in the class,
* respond to students questions and concerns expressed in the “one-minute paper”,
* grade assignments, quizzes, and exams, and post scores within one week of the end of the week in which they are submitted, and
* read any e-mail sent by you and respond accordingly within 48 hours.

Although I will read every posted discussion question and response, I will not necessarily respond to every post.

CLASS ATTENDANCE: Class attendance is the responsibility of the student, and it is the student's responsibility to independently cover any materials missed. Class attendance and participation may also be used in determining grades. At my discretion, I may drop you from the course for more than ***four(4)*** absences. Missing an exam or quiz is considered an absence. Missed classes caused by participation in documented, formal, University-sponsored events will not count as absences provided you notify me of such anticipated absences in advance and as soon as possible.

**You** are responsible for all class work missed, regardless of the reason for the absence(s). Late assignments will **not** be accepted. No makeup exams or quizzes will be given, so please make sure you are present for all exams/quizzes. Refer to the CSU Catalog (<http://ace.columbusstate.edu/advising/a.php#AttendancePolicy>) for more information on class attendance and withdrawal.

|  |
| --- |
| **Academic dishonesty** Academic dishonesty includes, but is not limited to, activities such as cheating and plagiarism. It is a basis for disciplinary action. Collaboration is not permitted on assignments or exams/quizzes in this course. Any work turned in for individual credit must be entirely the work of the student submitting the work. **All work must be your own.** You may share ideas but submitting identical assignments (for example) will be considered cheating. **You may discuss the material in the course and help one another with debugging, however, I expect any work you hand in for a grade to be your own. .** A simple way to avoid inadvertent plagiarism is to talk about the assignments, but don't read each other's work or write solutions together. Keep scratch paper and old versions of assignments until after the assignment has been graded and returned to you. **If you have any questions about this, please see me immediately.**  For assignments, access to notes, textbook, books and other publications is allowed. Stealing, giving or receiving any code, diagrams, drawings, text or designs from another person (CSU or non-CSU) is not allowed. Having access to another person’s work on the system or giving access to your work to another person is not allowed. It is your responsibility to keep your work confidential.  No cheating in any form will be tolerated. The penalty for the first occurrence of academic dishonesty is a zero grade on the assignment or exam/quiz; the penalty for the second occurrence is a failing grade for the course. For exams/quizzes, access to any type of written material or discussion of any kind (except with me) is not allowed. (<http://ace.columbusstate.edu/advising/a.php#AcademicDishonestyAcademicMisconduct>)  **Getting help**  Student assistants at the Helpdesk in level 1 of the CCT building can help you with basic computer-related problems such as logging on to the network, saving your work, etc., but they are not obligated to help you with your assignments. For course-related questions see the instructor during announced office hours. |

**Electronic Devices and Academic Integrity**: All cell phones MUST be turned off prior to entering the classroom or lab. The use of any electronic device during a test or quiz is prohibited. This includes cell phones, handheld calculators, and laptops. Any use of such a device during a test or quiz will be considered a breach of academic integrity.

**CSU ADA statement**   
"If you have a documented disability as described by the Americans with Disabilities Act (ADA) and the Rehabilitation Act of 1973, Section 504, you may be eligible to receive accommodations to assist in programmatic and/or physical accessibility. We recommend that you contact the Office of Disability Services located in Schuster Student Success Center, room 221, [706-507-8755](tel:706-507-8755) as soon as possible. The Office of Disability Services can assist you in formulating a reasonable accommodation plan and in providing support. Course requirements will not be waived but accommodations may be able to assist you to meet the requirements. Technical support may also be available to meet your specific need."

###### COURSE OUTLINE (tentative)

|  |  |  |
| --- | --- | --- |
| **DATE** | **Chapter / Description** | **Assignments/Quizzes** |
| Week 1: (1/13-1/17) | What is cryptography?  Mathematical Background: Modular arithmetic | What do these flags say? |
| Week 2: (1/20-1/24) | Early symmetric ciphers:  Caesar Cipher, Substitution cipher, Transposition cipher, Vigenere cipher, | **Programming Assignment 1:** Implementing a symmetric cipher |
| Week 3: (1/27-1/31) | Mathematical background: Probability  Cryptanalysis of symmetric ciphers  Attack models |  |
| Week 4: (2/3-2/7) | More on cryptanalysis of symmetric ciphers |  |
| **Monday, February 3 - LAST DATE TO WITHDRAW WITH A ‘W’** | | |
| Week 5: (2/10-2/14) | A modern symmetric cipher: DES | **Programming Assignment 2:** Breaking a cipher |
| Week 6: (2/17-2/21) | Mathematical background: Elementary number theory and finite fields |  |
| Week 7: (2/24-2/28) | State of the art AES |  |
| **Spring Break (no classes) – March 3-7** | | |
| Week 8: (3/10-3/14) | Problem of key distribution  What is public key cryptography? | **Midterm Exam (3/14)** |
| Week 9: (3/17-3/21) | Mathematical background: More elementary number theory  Key agreement – Diffie-Hellman | **Programming Assignment 3:** Implementing a modern symmetric cipher |
| Week 10: (3/24-3/28) | Public key encryption - RSA |  |
| Week 11: (3/31-4/4) | More on RSA and public key cryptography in practice |  |
| Week 12: (4/7-4/11) | Hash functions  MACs |  |
| Week 13: (4/14-4/18) | Digital signatures |  |
| Week 14: (4/21-4/25) | Key management |  |
| Week 15: (4/28-5/2) | Other applications of cryptography |  |
| Week 16: (5/5-5/9) | No Class - Study Day - May 6 | **Programming Assignment 4:** Implementing a public key scheme |
|  | **FINAL EXAM - Date to be announced** |  |

**Please return the following information to me as soon as possible.**

**CPSC 5555 (CRNs 22463 and 22128) Spring 2014**

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (please print)

 Where can I reach you in case it becomes necessary? \*\*

 Email address that you use regularly: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 Phone number(s): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 Declaration: I have read, understood and agree to abide by the policies mentioned in the syllabus pertaining to the course. In particular, I agree to abide by the assignment policy/late work policy, attendance policy, academic dishonesty policy, website policy and exam policy.

 (You must sign and date below).

 Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 \*\* Optional information

<http://computer.howstuffworks.com/computers-videos-playlist.htm>