Fairfax Collegiate

703 481-3080 · www.FairfaxCollegiate.com

Cryptography 5-6 Syllabus

Course Goals

1 Understand Different Ciphers
Students learn the history and mathematics behind various types of ciphers and the pros and cons to using them

2 Make and Break Ciphers
Students practice making and breaking their own codes using ciphers discussed in class

3 Develop Original Ciphers
Students create their own code using an existing method of their choice or a new method

Course Topics

1 Cryptography overview
Students learn the basic components behind cryptography and why codes have been used historically.

2 Making and Encrypting Caesar Ciphers
Students learn the methods to make Caesar Ciphers and write their own secret messages using the ciphers.

2.1 Alphabet Shift
Students learn the methods to make alphabetical shifting Caesar Ciphers and write their own secret messages using the ciphers. They also make cipher wheels to help write and break codes more easily.

2.2 Letter to Number Relations
Students learn the methods to make Letter and Number corresponding Caesar Ciphers and write their own secret messages using the cipher.

3 Breaking Caesar Ciphers
Students learn methods to crack Caesar ciphers when the shift key is not known.

4 Making and Encrypting Keyword Substitution Ciphers
Students understand and practice making their own codes using keyword substitution ciphers, which are slightly harder to crack than Caesar Ciphers.

5 Relative Frequencies of Letters
Students learn discrepancies of the English language to help them while cracking codes. They study the common letters used and average frequencies of letters or letter combinations in order to help them crack tough codes.

6 Breaking Keyword Substitution Ciphers
Students learn to decrypt a keyword substitution cipher when given the keyword and key letter. By using relative frequencies, students also learn to crack keyword substitution ciphers when they don't know the keyword or key letter.

7 Making Vigenère Ciphers
Students learn the history behind Vigenère ciphers and learn methods to make Vigenère Ciphers. Students write their own secret messages using this cipher.

8 Breaking Vigenère Ciphers
Students use prime factorization to crack Vigenère ciphers when the keyword is not known.

9 Cracking Codes to Solve Crimes
Students learn of historical codes that helped America during WWI and WWII as well as codes used by famous criminals. Students play a game with codes to solve "murders" committed by one of their own!

10 Modular Arithmetic
Students learn to use modular arithmetic in order to make stronger codes.

11 Multiplication Ciphers
Students learn to make and break multiplication shifted ciphers using modular arithmetic.

12 Linear Systems
Students learn to solve linear systems using substitution and elimination in order to crack tougher codes.

13 Affine Ciphers
Students learn to make and encrypt codes using multi-step affine ciphers to make a stronger code. They also learn to decrypt affine ciphers by writing and solving linear systems of equations.

14 Prime Numbers
Students learn, recall and expand on their knowledge of prime numbers by finding many large prime numbers to make stronger codes. They learn about relatively prime numbers in order to find good key numbers for RSA ciphers.

15 Exponents
Students expand on their knowledge of exponents with exponential multiplication and simplification in order to understand computations for RSA ciphers.

16 RSA Ciphers
Students develop and encrypt RSA ciphers and learn how to decrypt ones sent to them. Students learn how these ciphers are used today.

17 Making Your Own Codes
Students create their own codes using existing ciphers, combining others, or creating an entirely original one. This project allows students to develop personal secret messages or recreate historical messages using a new type of encryption method.

Course Schedule

Day 1

Introduction to class and rules
Instructor and students get to know each other and the rules through ice breakers and introductions.

Cryptography Discussion
Class discussion of what cryptography means and why it's used. Students also discuss their goals for the class and what they'd like to learn.

Discuss and Practice Caesar Ciphers
Students learn the history of Caesar Ciphers and the practice making simple words and phrases into codes.

Make a Cipher Wheel
Students use paper plates to make a cipher wheel that will help for easy encrypting and decrypting later in the session.

Practice Caesar Cipher
Students practice encrypting and decrypting problems from the textbook.

Cipher Tag 1
Students play a game in which they take turns encrypting and decrypting words and phrases on the white board.

Day 2

Number Caesar Ciphers
Students learn about another type of Caesar Cipher which involves corresponding each letter in the alphabet to a number.

Practice Number Caesar Ciphers
Students practice encrypting and decrypting problems from the textbook.

Cipher Tag 2
Students play cipher tag again with number Caesar Cipher codes.

Discuss and Practice Breaking Caesar Ciphers
Students learn how to crack Caesar Cipher codes.

Practice Breaking Caesar Ciphers
Students practice encrypting and decrypting problems from the textbook.

Day 3

Keyword Substitution Ciphers
Students learn and discuss how keyword ciphers are different from the others and how they may be more or less secure.

Practice Keyword Substitution Ciphers
Students practice encrypting and decrypting problems from the textbook.

Make Your Own Keyword Cipher
Students practice making their own keyword cipher using any keyword they'd like. They then practice decrypting a partners message. They discuss how some keywords may be more or less secure if coding a secret message.

Finding Relative Frequencies
Students use newspaper articles to calculate the frequency of letters commonly used in the English language.

Letter Frequency and Substitution Ciphers
Students discuss how to crack substitution ciphers using what they know about letter frequency.

Practice Breaking Keyword Ciphers

Students practice encrypting and decrypting problems from the textbook.

Day 4

Vigenère History and Introduction
Students learn the history of Vigenère and how they work, they receive a helpful Vigenère square to assist with decrypting these ciphers.

Practice Vigenère Ciphers
Students practice encrypting and decrypting problems from the textbook.

Cipher Tag 3
Students play cipher tag again with Vigenère ciphers.

Cracking Vigenère with Known Keyword Length
Students learn how to crack a Vigenère cipher when the keyword length is known but the exact keyword is not.

Practice Cracking Vigenère with Known Keyword Length
Students practice cracking Vigenère ciphers when they know the length of the keyword but nothing else.

Remember Factoring
Students recall how to factor down to prime numbers in order to help them crack tougher codes later on.

Cracking Vigenère Ciphers
Students use prime factorization to crack Vigenère ciphers when they don't know the length of the keyword.

Day 5

Review Covered Codes
Students review the codes and ciphers they've learned up to this point.

Codes Used in History
Students learn about codes used throughout history during wars to hide national secrets. They also learn of criminals using codes to taunt detectives in the past century.

Preparation for "Mafia"
Students write codes describing themselves in preparation for the game.

Abridged Mafia
Students play a game that resembles the code taunting used by criminals in the 20th century.

Week One Wrap Up
Students read cipher books and play logic games to conclude the first week.

Day 6

Introduction to Modular Arithmetic
Students learn modular arithmetic in order to help encrypt and decrypt more codes.

The Mod Game
Students play a game to understand modular arithmetic and reducing to different mods.

Practice Modular Reductions
Students practice encrypting and decrypting problems from the textbook.

Introduction to Multiplication Ciphers
Students learn about multiplication ciphers and how this relates to modular reduction.

Practice Multiplication Ciphers and Reducing
Students practice encrypting and decrypting problems from the textbook.

Finding the "Good" Keys
Students investigate in groups of three to determine which numbers make good multiplication cipher keys in the English alphabet.

Practice Finding "Good" Keys
Students practice by doing problems from the textbook.

Using Inverses in Modular Arithmetic
Students discuss the difference between inverses/reciprocals in regular arithmetic and inverses in modular arithmetic. Students do problems from the textbook to further understand this complicated concept.

Practice Finding Inverses
Students practice finding inverses by doing problems from the textbook.

Cipher Tag 4
Students play cipher tag again with multiplication ciphers.

Day 7

Introduction to Affine Ciphers
Students learn about affine ciphers, using two different operations on a message to encrypt it further and make it stronger.

Solving Linear Equations
Students recall and expand on their knowledge of solving linear systems of equations to further help crack codes.

Solving Systems to Crack Ciphers
Students use relative frequencies and systems of equations to crack affine ciphers

Practice Cracking Affine Ciphers
Students practice problems from the textbook.

Day 8

Prime Numbers
Students discuss what they know about prime numbers and how to determine if a large number is prime or composite. Students practice determining if numbers are prime or composite.

Exponent Rules
Students learn rules of exponents when multiplying and dividing. Students practice reducing and expanding exponents.

Examples of RSA Messages
Students learn introductory information of how RSA ciphers work in the real world today. Students practice making encrypting and decrypting RSA messages.

Class RSA message
As a class, students practice encrypting and decrypting longer RSA messages.

Day 9

Make Your Own Code
Students make their own code using a combinations of ciphers learned or creating a new one entirely. Students will share their code and allow the class to decrypt it, they may possibly need to help the class decrypt it.

Day 10

Make Your Own Code
Students make their own code using a combinations of ciphers learned or creating a new one entirely. Students will share their code and allow the class to decrypt it, they may possibly need to help the class decrypt it.

Updated on 3/9/2018