

Cryptology Overview

Developed/Adapted By

Steven Zollinger (steve.zollinger@snow.edu) Snow College

One sentence description of the assignment or activity

Students will learn some purposes for cryptology today, what makes a code secure, and the basic workings of some historical ciphers.

Course for which this is used

- PreAlgebra (Math 0950)
- Beginning Algebra (Math 0990)
- Intermediate Algebra (Math 1010)
- College Algebra (Math 1050)

Key topics taught in this activity

Cryptology

Prerequisites

Modular arithmetic

Lesson Plan – Detailed Description

Begin the lesson by having students brainstorm what they think of when they hear the word “code”. Then discuss the basics of cryptology, vocabulary, security issues, and historical ciphers, using the information in the “Cryptology-Overview-InstructorNotes” document as a guide. As an alternative to discussing the historical ciphers, you may also assign the students to research one of the historical ciphers and prepare a short presentation on their cipher for the class. A description of this research presentation assignment can be found in the “Cryptology-Overview-ResearchPresentation” document.

Following this overview of cryptology, the students will have a chance to practice encrypting and decrypting messages using some simple ciphers. For each section of the cryptology practice assignment sheet, the teacher should provide basic instruction on how encryption and decryption work for the section’s cipher. Then students will complete the encryption and decryption tasks for that section.

Activity Grading/Assessment

Students will be assessed based on their lesson participation and on their completion of the research presentation (if assigned).

Class Time Required

- 45-60 minutes for class overview discussion
- 45-60 minutes for research presentations (if assigned)
- 45-60 minutes for cryptology practice instruction and assignment

Out-of-Class Time Required

0-60 minutes researching a historical cipher (if assigned).

Materials Required

Research Presentation assignment (if assigned)

Supplemental Web Resources

- <http://www.pbs.org/wgbh/nova/decoding/>
- <http://www.ciphersbyritter.com/LEARNING.HTM>
- <http://www.cs.trincoll.edu/~crypto/index.html>
- http://www.simonsingh.net/The_Black_Chamber/chamberguide.html

