

Cryptology – Syllabus

Teacher: Mr. Evans

Room: B310

Email: mark.evans@hcps.org (for class assignments email to, evans@scienceandmathacademy.com)



Webpage: www.scienceandmathacademy.com/academics/electives/cryptology and <http://crypto.scienceandmathacademy.com>

Course Description: This is a semester course which will teach the basics of cryptology. Students will gain an understanding of classic and contemporary encryption algorithms. Cryptanalysis techniques of classic ciphers will be studied and implemented. Some of the weaknesses of contemporary ciphers will be discussed. Students will also write simple visual basic (VB) programs to encrypt and decrypt text (other computer languages will be used where appropriate). The class will be actively creating a “wiki” for this course.

Course outline: The below outline is a loose guide.

- Introduction to Cryptology
 - Lecture (1 day)
- Classical Cryptology
 - Classical Monoalphabetic Ciphers – (Keyword, affine, multilateral)
 - Lecture (1 day)
 - Decryption assignment #1: Keyword (1 day)
 - Programming assignment #1: Affine Cipher, using VB (4 days)
 - Classical Polyalphabetic Ciphers – (Vigenere, Autokey, Nihilist, Cylinder, Rotor)
 - Lecture (2 days)
 - Decryption assignment #2: Vigenere (1 day)
 - Classical Polygraphic Ciphers – (Playfair, Hill, Beale Cipher)
 - Lecture (1 day)
 - Decryption assignment #3: Hill (1 day)
 - Classical Transposition Ciphers – (Permutation, Column Permutation, Double-Transposition)
 - Lecture (1 day)
- Contemporary Ciphers
 - Stream Ciphers
 - Lecture (2 days)
 - Programming assignment #2: Stream Cipher, using VB (4 days)
 - Block Ciphers
 - Lecture (2 days)
 - Introduction to Number Theory
 - Lecture (2 days)
 - Public Key Ciphers
 - Lecture (2 days)
 - Decryption assignment #4: Public Key (1 day)
 - Programming assignment #3: Public Key Cipher, using Word and VBA (4 days)

- Message Authentication: Key Management, Digital Signatures, Hash Functions, & Certificates
 - Lecture (2 days)
- Quantum Cryptography
 - Lecture (1 day)
- Other days
 - Guest lecturer, (1-2 day)
 - Tests, one per quarter (2 days)
 - Midterm Review (1 day)
 - Midterm (1 day)
 - Extra days may be inserted from time to time.

Grading: All grades are determined by total points.

- **Tests:** 50 points each (History, basic understanding of ciphers, and some VB code)
- **Decryption assignments:** 30 points each
 - Keyword cipher
 - Vigenere cipher
 - Hill cipher
 - Public Key
- **Programs:** 50 points each
 - Affine cipher
 - Stream cipher
 - Public key
 - There will be other programming assignments
- **Other class assignments:** 10-20 points
- **Wiki updates:** About 60 points per quarter
 - Students will be responsible for making appropriate edits
 - Students must have a signed permission form to be able to have a login for the wiki.