Cryptology – Syllabus

Teacher: Mr. Evans
Room: B310

Email: mark.evans@hcps.org

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 course will also introduce and use many mathematics topics that are not typically covered in High School. Technical paper will be used to expose students to the most current topics.

Course outline: The below outline is a loose guide.

- Introduction to cryptology (*Day 1*)
- Classic cryptology
    - Monoalphabetic ciphers (shift, affine, keyword, multilateral) (*Days 2 through 6*)
        - Frequency analysis tool (Microsoft Excel)
        - Decryption assignment (keyword)
        - Congruence modulo *n*
            - Intro to modular
            - Modular arithmetic
            - Extended Euclidean algorithm
        - Programming assignment (Affine, using VB)
    - Polyalphabetic ciphers (Vigenere, Autokey, Nihilist, Cylinder, Rotor) (*Days 7 through 10*)
        - Decryption (Vigenere)
    - Polygraphic ciphers (Playfair, Hill, Beale Cipher) (*Days 11 through 12*)
        - Matrix multiplication, inverse matrices, reduced row echelon form, inverse matrices in $\mathbb{Z}_m$
        - Hill tool (Mathematica®)
    - Classical transposition ciphers (Permutation, Column permutation, double-transposition) (*Days 13-17*)
        - Tools for decryption (VB)
        - Decryption (Column permutation)
- Contemporary ciphers
    - Stream ciphers (*Days 18-23)*
        - Binary practice (binary conversions, XOR, etc.)
        - LSFR
            - Primitive polynomials
            - Maximal LFSRs
        - Programming assignment RC4

        - NIST Special Publication 800-22, *A Statistical test suite for random and pseudorandom number generators for cryptographic applications* (http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22rev1a.pdf)
        - eSTREAM (Project to identify new stream ciphers)
    - Block ciphers (*Days 24-28*)
        - DES
        - 3DES
        - Galois fields
            - Addition and subtraction in GF (2^m)
            - Multiplication in GF (2^m)
            - Inversion in GF (2^m)
        - AES
    - Public key ciphers (*Days 29-31*)
        - Intro to number theory
        - RSA
        - Primality tests (Rabin-Miller)
        - Diffie-Hellman key exchange
    - Digital signatures (*Day 32 & 35*)
        - RSA signature scheme
        - Digital Signature Algorithm (DSA)
    - Hash functions (*Day 33-34*)
        - MD5
        - SHA-1
    - Message authentication codes (MACs) (*Day 35*)
    - Quantum Cryptography

- Other days
    - Guest lecturer, (1-2 day)
    - Tests, one per quarter (2 days)
    - Final 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
- **Programming assignments:** 30-50 points
- **Other class assignments:** 10-20 points