

# Advanced Cryptology CTY Course Syllabus

## Resources:

- [1] “Cryptological Mathematics” by Robert Edward Lewand. 2000, The Mathematical Association of America.
- [2] “Handbook of Applied Cryptography” by Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. 1997, CRC Press LLC.
- [3] “CTY Cryptology Amalgamation” by Stefan Treatman and David Perry. Used as a course guide since the inception of the CTY cryptology course.
- [4] “The Theory of Error-Correcting Codes” by F.J. MacWilliams. 1996, North Holland Publishing Company.
- [5] “An Introduction to Information Theory” by Fazlollah M. Reza. 1961, McGraw-Hill.

## **Week 1: Language Models, Matrix Encryption, Hashing**

Days or time slots marked with REVIEW are primarily review of concepts from CODE in order to support learning more advanced related topics.

### **Monday (DAY 1) REVIEW**

#### *Morning Session*

- Modular Arithmetic [1]
- Modular Arithmetic in Monoalphabetic Coding [1]
- Modular Arithmetic view of Vigenere’s System [1]
- Matrices [1]

#### Afternoon Session

- Modular Matrices [1]
- Hill’s System [1]

#### Evening Session

- Problems on Modular Arithmetic
- Problems on Hill’s Systems

### **Tuesday (DAY 2)**

#### *Morning Session*

- Probability Theory [1]
- Friedmann Test (Poly vs. Mono) [1]
- Brainstorming: Probability vs. Matrix Systems?

#### *Afternoon Session*

- N-gram Language Models: Overview [portions in 1]
- Utilizing n-gram Models on Mono and Poly

- Attacking Small Matrix Systems with n-gram [1]
- Brainstorming: What About Large Matrices?

*Evening Session*

- Friedmann Test Challenge
- N-gram Matrix Challenge

**Wednesday (DAY 3)**

*Morning Session REVIEW*

- Discussion: How Do We Exchange Keys for Symmetric Systems?
- Review of Techniques from CODE [3]
- Fermat's Little Theorem [1]
- Euler's Theorem [1]

*Afternoon Session REVIEW*

- RSA [1]
- Diffie-Hellman [1]
- Massey-Omura [1]
- Computational Complexity of RSA

*Evening Session*

- Students Practice Old PK Techniques in Pairs

**Thursday (DAY 4)**

*Morning Session*

- Alternative Methods of PK Key Exchange [2]
- Do some of the following:
  - Needham-Schroeder Protocol [2]
  - ElGamal Key Agreement [2]
  - MTI/A0 Protocol [2]
  - STS Protocol [2]

*Afternoon Session*

- Students Practice Advanced PK Techniques in Pairs
- Attacks on Key Exchanges
- Active Attack on ElGamal/Diffie-Hellman [2]
- Passive Attack on MTI/A0 [2]
- Begin First Project (3 groups): Key Exchange Development

*Evening Session*

- Students Practice Advanced PK Techniques in Pairs
- Students Work on Projects

**Friday (DAY 5)**

*Morning Session*

- Symmetric Key Establishment
- Shamir's No-Key Protocol [2]
- Advanced Example: Kerberos [2]
- Work on Projects

### Afternoon Session

- Students Practice Shamir in Pairs
- Students Practice Kerberos in Triples
- Work on Projects

### Sunday (DAY 6)

#### *Evening Session*

- Work on Projects

## **Week 2: Error-Correcting Codes, Stream Ciphers, Block Ciphers**

### Monday (DAY 7)

#### *Morning Session*

- Presentation of Projects

#### *Afternoon Session*

- Hash Function Properties [2]
- MDC's Based on Block Ciphers [2]
- Matyas-Meyer-Oseas Hash [2]
- Davies-Meyer Hash [2]
- Class Exercise Using Mini-DES [3] to Construct an MDC via Both MMO and DM Algorithms

#### *Evening Session*

- Students Continue Class Exercise
- Exercises on Hash Functions

### Tuesday (DAY 8)

#### *Morning Session*

- Continuation of Hashing
- MAC's [2]
- The CBC-MAC [2]
- Birthday Attacks [2]
- Application: Mini-DES [3]

#### *Afternoon Session*

- Stream Ciphers
- Vernam Cipher & Pseudo-random Sequences [2]
- Linear Feedback Shift Registers [2]
- Polynomial Theory (Connection Polynomials) [2]

#### *Evening Session*

- Students Design & Test LFSR Stream Ciphers
- Attempt Birthday Attacks on a MAC Hash

### Wednesday (DAY 9)

#### *Morning Session*

- More Polynomial Theory over GF(2) [2], [4]
- Desirable Properties of LFSR's [2]
- Golomb's Randomness Postulates [2]

### *Afternoon Session*

- Non-linear Combination Generators [2]
- Geffe Generator as Example [2]
- Correlation Attacks [2]
- Practice Correlation Attack

### *Evening Session*

- LFSR Attack Challenge

## **Thursday (DAY 10)**

### *Morning Session*

- DES (REVIEW) [2]
- Strengths & Weaknesses [2]
- Modes of Operation for a Block Cipher [2]
  - Electronic Codebook (ECB)
  - Cipher-block Chaining (CBC)
  - Cipher Feedback (CFB)

### *Afternoon Session*

- Practice Modes of Operation with Mini-DES & Baudot [2], [3]
- Use of Modes of Operation in Stream Ciphers
- Practice Modes of Operation with LFSR's

### *Evening Session*

- Breaking Small LFSR Examples with Modes of Operation in Class

## **Friday (DAY 11)**

### *Morning Session*

- Introduction to Error-correction [4]
- Repetition Code [4]
- Hamming (7, 4) Code [4]
- Parity Checks [4]
- Linear Codes [4]

### *Afternoon Session*

- More Linear Codes: Perfect Codes, Systematic Codes [4]
- Syndromes & Decoding [4]
- In-class Examples: Error-correcting With Linear Codes

## **Sunday (DAY 12)**

### *Evening Session*

- Parity Check Game (How Error-Correcting Codes Can Save Your Life)
- Students Design & Test Linear Codes To Specifications in Groups

## **Week 3: Compression, McEliece, Final Exam**

## **Monday (DAY 13)**

### *Morning Session*

- More on Polynomial Algebra over  $GF(2)$  [4]
- Cyclic Codes [4]

- Cyclic Codes: Encoding & Decoding with LFSR's [4]

*Afternoon Session*

- Students Design & Test Cyclic Codes to Specifications in Groups

*Evening Session*

- Students Try to Break Cryptosystems That Have Error-Correction

**Tuesday (DAY 14)**

*Morning Session*

- McEliece Public Key Encryption [2]
- Students Design & Encrypt with Their Linear Codes from Week 2 Using McEliece

*Afternoon Session*

- Students Finish McEliece Encryptions
- Introduction to Information Theory [5]

*Evening Session*

- Review Quiz: Hashing, Error-correction, Block Ciphers, Key Exchange

**Wednesday (DAY 15)**

*Morning Session*

- Begin Optional Topics: Compression/Factoring
- Compression
- Variable-length Compression [Shannon-Fano, Huffman]

*Afternoon Session*

- Dictionary Compression [LZ]

*Evening Session*

- Exercises on Compression
- Brainstorming on Compression Schemes

**Thursday (DAY 16)**

*Morning Session*

- Back to RSA: Weaknesses
- Factoring Algorithms
  - Trials [2]
  - Pollard's Rho [2]
  - Random Square Factoring [2]
- Examples in Class

*Afternoon Session*

- Students Factor Integers Using Different Algorithms
- Students Get Into 3 Groups To Compare Speeds
- Brainstorm About Factoring Algorithms

*Evening Session*

- Party/Games

**Friday (DAY 17)**

*Morning Session*

- Movie