CIS 3362 Final Exam Review Fall 2025

Final Exam Date: 12/3/25
Time: 10:00 am – 1:00 pm
Place – BA1-119

Exam Aids: Exam 1 Formula Sheet,
DES/AES Sheets,
Four Pages of Student Created Notes
Calculator

Note: Make sure you understand what a modular inverse means and ow to use the Extended Euclidean Algorithm (as taught in class) to find one.

Outline of Material Covered

I. Classical Monoalphabetic Ciphers
- **A. Shift**
- **B. Affine**
- **C. Mod**
- **D. GCD, Euclidean Algorithm**
- **E. Extended Euclidean Algorithm**
- **C. Regular Substitution**

II. Classical Polyalphabetic/Polygraphic Ciphers
- **A. Vigenere**
- **B. Playfair**
- **C. Transposition**
- **D. ADFGVX**
- **E. Hill Cipher**
- **F. Enigma**
- **G. Navajo Code**

III. Symmetric Block Ciphers
- **A. Coding Bitwise Operators**
- **B. DES**
- **C. AES**
- **D. Symmetric Cipher Modes**

IV. Number Theory for Cryptography
- **A. Primes and Fermat's Theorem**
- **B. Euler Phi Function and Euler's Theorem**
- **C. Fast Modular Exponentiation**
- **D. Miller-Rabin Primality Test**
- **E. Discrete Log Problem**
- **F. Factoring – Fermat and Pollard-Rho**

V. Public Key Ciphers
- **A. Public Key Process**
- **B. Diffie-Hellman Key Exchange**
- **C. RSA**
- **D. El Gamal**
- **E. Elliptic Curves**
- **F. Use of Elliptic Curves for Cryptography**
- **G. Diffie-Hellman Key Exchange with Elliptic Curves**
- **H. How to Map a bitstring message to a point on a given Elliptic Curve (and back)**

VI. Odds and Ends
- **A. Qualities of a Good Hash Function**
- **B. Rationale for use**
- **C. Idea of Adding Salt for Storing Password Hashes**
- **D. El Gamal Digital Signature**

<u>Some Notes</u>

1. I always test something from each of the five quizzes, to get some breadth of coverage.

2. I always test the Extended Euclidean Algorithm in multiple questions, one of which is usually an RSA question where you have to find a corresponding private key, d, given public keys n and e.

3. I will likely have one coding question which will be required to be done in C.

4. Since I spent class time clarifying how a message gets converted to a point on an elliptic curve, I plan on doing a question similar to number 5 from Quiz 5, and this time I'll make sure to provide the proper information in the list of modular exponentiations listed.