CIS 3362 Exam 3 Review – Fall 2026

Exam Date: 11/16/2026
Exam Time: 9:00 am – 10:15 am
Exam Location: VAB-132
Exam Aids: **CALCULATOR AND TWO SHEETS OF NOTES (REGULAR PAPER 11" x 8.5", FRONT AND BACK)**

Old Quizzes/Exams:

https://www.cs.ucf.edu/~dmarino/ucf/transparency/cis3362/quiz/
https://www.cs.ucf.edu/~dmarino/ucf/transparency/cis3362/exam/

For use, just map topics from below to see if an old question is relevant to our exam.

Topics Covered on Exam

1. Number Theory
    a. Prime Factorization and Default Primality Test
    b. Fermat's Theorem
    c. Euler Phi Function, proof of formula
    d. Euler's Theorem
    e. Fast Modular Exponentiation
    f. Miller-Rabin Primality Test
    g. Discrete Log Problem
    h. Square Root Discrete Log Algorithm (sometimes called Baby Step Giant Step)
    i. Fermat Factoring Algorithm
    j. Pollard-Rho Factoring Algorithm
2. Public Key Exchanges and Cryptography
    a. Diffie-Hellman Key Exchange
    b. RSA Cryptosystem
    c. El Gamal Cryptosystem
    d. Elliptic Curves
    e. Elliptic Curve Addition/Multiplication
    f. Elliptic Curve Diffie-Hellman Key Exchange
    g. Elliptic Curve El Gamal Cryptosystem
    h. Conversion of bitstring to Elliptic Curve Point