

CIS 3362 Exam 1 Review – Fall 2026

Exam Date: 9/23/2026

Exam Time: 9:00 am – 10:15 am

Exam Location: VAB-132

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. Shift Cipher
 - a. How to Encrypt/Decrypt by hand given key
 - b. Determining key space
2. Extended Euclidean Algorithm
 - a. Regular Euclidean Algorithm
 - b. Extended Euclidean Algorithm to find $a^{-1} \bmod n$
 - c. How to do mod math by hand to simplify manual computation. (Useful for many things in the course.)
3. Affine Cipher
 - a. How to Encrypt by hand.
 - b. How to Decrypt by hand given decryption key.
 - c. How to compute the Decryption key given the encryption key.
 - d. How to use 2 matching plaintext-ciphertext pair to reduce key space.
4. Substitution
 - a. Key space
 - b. General cryptanalysis techniques used to break it.
5. Vigenere Cipher
 - a. How to encrypt, given key
 - b. How to decrypt, given key
 - c. Kasiski Test
 - d. Index of Coincidence computation and relevance to breaking Vigenere.
 - e. Mutual index of Coincidence test and relevance to breaking Vigenere.
 - f. Know how to reduce fractions to lowest terms.

6. Playfair Cipher

- a. How to encrypt, given key.
- b. How to decrypt, given key.

7. Transposition

- a. How to encrypt via general column transposition using a keyword.
- b. How to decrypt via general column transposition using a keyword.
- c. Use of mod and integer division in the process above.

8. ADFGVX

- a. How to do the first step of encryption given the key.
- b. How to do the second step of encryption given the key.
- c. How to decrypt the second step given the key.
- d. How to decrypt the first step given the key.

9. Hill cipher

- a. How to encrypt given a key.
- b. How to decrypt, given the decryption key.
- c. Knowing when a key is valid and use of determinant.
- d. Memorize formula to compute 2×2 decryption key, given encryption key.
- e. How to use 2 pairs of matching plain and ciphertext to reduce key space.

10. Enigma

- a. Rough set up of the machine.
- b. Knowing how many settings the machine has (old and newer version)
- c. Knowing how to compute the number of settings based on changes to rotors and/or alphabet.
- d. History of breaking Enigma (who got blueprints, etc.)
- e. Fact and observations we can make about how all permutations can be decomposed into cycles.
- f. Role of the Day Code
- g. Role of the Message Code
- h. Other items that helped Allied forces break Enigma

11. Navajo Code

- a. How code was created.
- b. Three steps in using the code.
- c. High level outline of history in the typed up notes.