

CIS 3362 Final Exam Review

Date: 12/9/2020 (Wednesday)

Time: 10:00 am – 12:50 pm

Format: Four Timed Sections

Part A: 10:00 am – 10:35 am, late 10:45 am

Part B: 10:40 am – 11:15 am, late 11:25 am

Part C: 11:20 am – 11:55 am, late 12:05 pm

Part D: 12:00 pm – 12:40 pm, late 12:50 pm

Exam Aids: All Course Notes,

All posted reference sheets (Exam 1, DES, AES)

Calculator

Strongly Suggested to Type So there aren't issues with timing.

Any part not received gets a 0.

If you need a make up, you need to tell me BEFORE the exam.

(Depending on the situation and timing, I will either do the make up before finals end, or assign an incomplete and give the final when it makes sense.)

Part A: Classical Cryptography (before computers)

1. Shift Cipher
2. Affine Cipher
 - a. # of possible keys
 - b. Given encryption keys, figure out the decryption keys
 - c. Given 2 matching plain/cipher text characters, how to set up equations to solve for the key
3. GCD, Extended Euclidean Algorithm
4. Substitution Cipher
 - a. Frequency Analysis
 - b. Repeated Di/Trigrams
 - c. Structural patterns of vowels, consonants
 - d. Queen Mary Story – null characters, multiple ciphertexts to replace a more frequent plain text character, backspace

5. Vigenere Cipher
 - a. Why hard to cryptanalyze at first.
 - b. Index of Coincidence Test
 - c. Kasiski Test
 - d. Mutual Index of Coincidence Test
6. Playfair
 - a. Know how to encrypt, decrypt
 - b. Know that it's always an even length and no two repeated characters ever appear (things about the cipher)
 - c. Can be attacked if we know a bit of matching plain and cipher text
7. ADFGVX
8. Hill Cipher
 - a. 2 x 2 how to find the inverse (make sure you know how to do this for different alphabet sizes.)
 - b. Know how to set up equations for known plain/cipher text.
 - c. Know what makes a key valid
9. Transposition
 - a. Single
 - b. Double
10. Enigma, Navajo Code

Part B: Private Key Encryption (DES, AES)

1. DES Algorithm
 - a. How to apply IP
 - b. Given IP, calculate IP^{-1}
 - c. Applying the permutation P
 - d. Applying the S-boxes
 - e. Details about the key schedule
 - f. Calculating the amount of time a brute force search might take
 - g. Knowledge of the key parity bits

- h. Knowing how many bits each component in the algorithm is.
2. AES Algorithm
 - a. Applying the big S-box
 - b. Shift Rows
 - c. Shift Cols (just test calculating one entry...make sure you calculate the one that is asked for)
 - d. Add Round Key
 - e. Basic Understanding of multiplication in the AES field
 3. Coding bitwise operators
 - a. $\&$, $|$, \wedge
 - b. \ll , \gg
 - c. Lowest one bit
 - d. Highest one bit
 - e. Number of bits set to 1