Fall 2025 CIS 3362 Final Exam (12/3/2025)

Last Name: _____ First Name: _____

1) (10 pts) You have discovered this incomplete encryption chart for a substitution cipher:

Plain	A	B	C	D	E	F	G	H	I	J	K	L	M
Cipher	P		S	L	D		F	J		H	Y		
Plain	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher	E	W	M		X	N	B						

Using this partial information, decrypt the following ciphertext (note: the spaces do not represent word breaks, they are just every five letters to make the ciphertext easier to read.) Please put in the proper word breaks in your answer.

```
bjgng nzvdn bgwee vradx wed
```

---

2) (5 pts) For the regular English alphabet, there are 312 possible Affine cipher keys. Each key can be represented as an ordered pair (a, b), where gcd(a, 26) = 1 and $0 \leq a, b \leq 25$. If we sort these ordered pairs by a in increasing order and break ties sorting by b in increasing order, what is the 200^{th} ordered pair? (The first ordered pair in the list is (1, 0) and the 312^{th} ordered pair in the list is (25, 25).)

(_____ , _____)

3) (5 pts) Using the Vigenere Cipher encrypt the plaintext "DECEMBERTHIRD" with the secret keyword "LYNX".

---

4) (5 pts) A big part of how the Enigma was broken was noting that for a fixed ordering of the rotors, those rotors could be set in 26^3 possible positions (corresponding to all possible 3 letter strings), and for each individual position, the machine performed a substitution cipher. Marian Rejewski found out that there was a "unique signature" for every one of these 26^3 substitution ciphers. What was this unique signature, that when uncovered, allowed the Polish and then the Allies the ability to determine where the machine's rotors were set at the beginning of a message, which then allowed for the decryption of a day's worth of messages. Clearly describe this signature and give one concrete example of a possible signature.

5) (12 pts) The function below takes in a string storing a plaintext and a valid encryption key for the Hill Cipher (size 3 x 3). **You may assume that the plaintext string consists of lowercase letters only and has a length that is a multiple of 3.** Complete the function so that it returns the encryption of the plaintext string using the key passed into the function. All the necessary dynamic memory allocation has been taken care of for you. Please hard-code the use of the number 3 to save space.

```
char* encrypt(char* plain, int key[][3]) {

    int n = strlen(plain);
    char* cipher = calloc(n+1, sizeof(char));

    // Please pay attention to the increment statement.
    for (int i=0; i<n; i+=3) {









    cipher[n] = '\0';
    return cipher;
}
```

6) (8 pts) The input to the S-boxes during a potion of DES, represented in hexadecimal is

52CB 9E16 75AF

What is the 4 byte output from the S-boxes, expressed in 8 hexadecimal characters? (Note: no need to write any binary output.) Please clearly indicate which S box, row and column you are looking in for each of the eight answers.

___ ___ ___ ___ ___ ___ ___ ___

7) (10 pts) Using your knowledge of the field used for AES calculations, multiply the two polynomials $f(x) = x^5 + x^3 + 1$ and $g(x) = x^4 + x^2 + x + 1$ in the field, displaying your answer first as a polynomial, and then as 2 hexadecimal characters.

Polynomial form: _____

Hexadecimal equivalent: ___ ___

8) (10 pts) Gerald wants to know the number of integers in between 1 and 1000 inclusive, that are relatively prime to 520. Using the Euler Phi Function, and a small amount of brute force, determine the answer to Gerald's query. Credit will be given for utilizing the tools taught in the number theory section of the course to reduce the total amount of work necessary to solve the problem. (The answer is worth a relatively small portion of the credit.)

9) (12 pts) An RSA system is set up with n = 667 and e = 419. What is the corresponding value of d?

d = _____

10) (12 pts) In an El-Gamal cryptosystem, Alice has posted her public elements as q = 521 (prime), $\alpha = 269$ (generator) and $Y_A = 168$. Bob has sent Alice the ciphertext message:

$C_1 = 269$, $C_2 = 380$

Eve has intercepted the message. Due to a poor choice made by Bob, Eve is able to decrypt the message and reveal the plaintext (an integer in between 0 and 520). Do the same work Eve did and determine that plaintext.

M = _____

11) (10 pts) Consider the task of encoding a 4-bit value (a hex character) on the Elliptic Curve $E_{83}(4, 7)$. We learned a technique in class to store an arbitrary bit string in class as a point on an Ellipitic Curve. **Using the same technique in class determine the Point encoding of the plaintext message m = 15 on the curve $E_{83}(4, 7)$.** Since this is computationally intensive, some facts will be given below that you may use to solve the problem. Use the facts as necessary. (Note: some of the facts are intentionally irrelevant, so part of what I am testing is to see if you can figure out what you actually need to use. Also, there is one calculation that I think is easy enough to do on your calculator for which I haven't provided the result.)

$15^{41} \equiv 82 \pmod{83}$
$19^{41} \equiv 82 \pmod{83}$
$31^{41} \equiv 1 \pmod{83}$
$39^{41} \equiv 82 \pmod{83}$
$42^{41} \equiv 82 \pmod{83}$
$47^{41} \equiv 82 \pmod{83}$
$61^{41} \equiv 1 \pmod{83}$
$63^{41} \equiv 1 \pmod{83}$

$15^{21} \equiv 20 \pmod{83}$
$19^{21} \equiv 8 \pmod{83}$
$31^{21} \equiv 23 \pmod{83}$
$39^{21} \equiv 58 \pmod{83}$
$42^{21} \equiv 46 \pmod{83}$
$47^{21} \equiv 6 \pmod{83}$
$61^{21} \equiv 12 \pmod{83}$
$63^{21} \equiv 48 \pmod{83}$

(_____ , _____)

12) (1 pt) What color predominately appears in the Orange Theory Fitness logo?

_____