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

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
```

Fill in the known plaintext letters putting dashes for the unknown ones.

```
th-s- s--es t-onn ---er one
```

The letters in yellow are all the same. It's extremely likely the yellow letter is 'I', meaning that the encryption of 'G' is 'I', which is missing in the known chart. This gives us:

```
this is --estion n---er one
```

From, here, play a little wheel of fortune to get:

```
This is question number one.
```

Grading: 10 pts if correct, grader decides partial.

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).)

For each value of a, all 26 possible values of b work. Thus, 200/26 = 7 tells us that 7 x 26 = 182 ordered pairs start with the seven lowest values of a, which are 1, 3, 5, 7, 9, 11, and 15, respectively. It follows that a = 17 for the next 26 ordered pairs, of which one is the 200^{th} ordered pair. Specifically, we are looking for the 18^{th} ordered pair of the form (17, b), since 200 = 182 + 18. (Also, note that 200%26 = 18.) It follows that the desired ordered pair is

(17, 17)

Grading: 3 pts for deducing 17 is a, 2 pts for deducing 17 is also b. Give partial as needed.

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

```
D E C E M B E R T H I R D= 3  4  2  4 12  1  4 17 19  7  8 17  3
L Y N X L Y N X L Y N X L=11 24 13 23 11 24 13 23 11 24 13 23 11
                         ---------------------------------------
                   add 14 28 15 27 23 25 17 40 30 31 21 40 14
                   mod 14  2 15  1 23 25 17 14  4  5 21 14 14
                         ---------------------------------------
               letters  O  C  P  B  X  Z  R  O  E  F  V  O  O
```

OCPBXZROEFVOO

Grading: 1 pt for writing out numbers for plain, 1 pt for writing out numbers for cipher, 1 pt for adding the numbers, 1 pt for modding, 1 pt for converting to letters. If at most a few letters are wrong but the process is right, just give 4 out of 5. (If subtracted give 2 of 5 max)

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 as 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.

All substitution ciphers can be decomposed into cycles. For example, if A encrypts to B, B encrypts to Z, Z encrypts to P, P encrypts to J and J encrypts to A, then A → B → Z → P → J → A forms a cycle in the substitution of size 5. It's guaranteed that for any substitution chart, it can be decomposed this way into one or more cycles, where the cycle lengths add to 26.

On the Engima, each of the different rotor settings induced a substitution cipher with a unique set of cycles. So, if it was known that some setting of the rotors generated the cycle lengths 2, 2, 3, 5, 6 and 8, then it turned out that only one setting of the rotors generated these cycles lengths so once enough messages were intercepted to establish the cycle lengths for the rotor setting for that day code, then a table could be consulted which listed which rotor setting that was. Here is a concrete example with 26 letters of a substitution cipher written in its cycles:

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

Grading: 2 pts for talking about cycle sizes, 2 pts for stating that they directly relate to rotor settings on the Engima, 1 pt for a list of numbers that adds to 26. Detailed list of mappings unnecessary.

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) {

        // 1 pt
        for (int j=0; j<3; j ++) {

            // 1 pt
            int val = 0;

             // 1 pt
            for (int k=0; k<3; k++)

                // 6 pts
                val = (val + key[j][k]*(plain[i+k]-'a'))%26;

            // 3 pts
            cipher[i+j] = 'a' + val;
        }

    }

    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.

Convert to binary:

```
5    2    C    B    9    E    1    6    7    5    A    F
010100 101100 101110 011110 000101 100111 010110 101111

S1[0][10] = 6            S5[1][2]  = 2
S2[2][6]  = D            S6[3][3]  = C
S3[2][7]  = 0            S7[0][11] = 7
S4[0][15] = F            S8[3][7]  = D
```

6D0F2C7D

Grading: 1 pt per hex character all or nothing on each character.

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.

$(x^5 + x^3 + 1)(x^4 + x^2 + x + 1) =$

$x^4 + x^2 + x + 1$

$x^7 + x^5 + x^4 + x^3$

$x^9 + x^7 + x^6 + x^5$

$x^9 + x^6 + x^3 + x^2 + x + 1$, recalling to reduce coefficients mod 2.

The mod polynomial for AES is $x^8 + x^4 + x^3 + x + 1$. In particular, the relevant fact is that $x^8 \equiv x^4 + x^3 + x + 1 \bmod (x^8 + x^4 + x^3 + x + 1)$. Thus, we have:

$x^9 \equiv x(x^8) \equiv x(x^4 + x^3 + x + 1) = x^5 + x^4 + x^2 + x \bmod (x^8 + x^4 + x^3 + x + 1)$, thus we get our final answer to be:

$x^5 + x^4 + x^2 + x + x^6 + x^3 + x^2 + x + 1 \equiv x^6 + x^5 + x^4 + x^3 + 1 \bmod (x^8 + x^4 + x^3 + x + 1)$.

In bits, this is 0111 1001, which, we converted to HEX is 79.

Polynomial form: **$x^6 + x^5 + x^4 + x^3 + 1$**
Hexadecimal equivalent: **79**

Grading: 5 pts for regular multiplication with coefficients mod 2. 3 pts to reduce x^9, 1 pt for poly answer, 1 pt for hex answer

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.)

By definition, φ(n) represents the number of integers in the range [1, n] that share no common factors with n. Thus, φ(520) is the number of integers in the range [1, 520] that share no common integers with 520. Though this isn't the question we're asked to solve, let's go ahead and calculate φ(520) via the prime factorization of 520:

$\varphi(520) = \varphi(2^3 x 5 x 13) = \varphi(2^3) x\ \varphi(5) x\ \varphi(13) = (2^3 - 2^2)(5 - 1)(13 - 1) = 4 \times 4 \times 12 = 192.$

Our key observation is that gcd(520+x, 520) = gcd(x, 520). This is proven in the proof of the Euclidean Algorithm. This means that the number of values in the range [521, 1040] relatively prime to 520 equals φ(520) because we can get the second range by adding 520 to each number in the first range. Thus, we know that there are 192 + 192 = 384 integers relatively prime to 520 in the range [1, 1040].

Thus, we must simply subtract out all the integers in between 1001 and 1040 that share no common factors with 520. Another way to say this is count the number of integers in between 1001 and 1040 that are not divisible by 2, 5 or 13. Remove all the integers in this range divisible by 2 or 5 to get the list:

1001 1003 1007 1009
1011 1013 1017 1019
1021 1023 1027 1029
1031 1033 1037 1039

Now, we must just find the integers on this list divisible by 13 and cross them out. Note that 1001 = 7 x 11 x 13, so 1001, 1014, 1027 and 1040 in the range are divisible by 13. Both 1001 and 1027 have yet to be crossed off. **It follows that 14 integers in the range [1001,1040] are relatively prime to 520.**

Thus, the final answer to the given question is 384 – 14 = **370.**

Grading: 3 pts to calculate phi(520), 2 pts to state that this represents # of values relatively prime to 520 in the range [1, 520]. 2 pts to state that there are 384 values in the range [1, 1040] relatively prime to 520 (no proof needed), 2 pts to manually count the relatively prime values in the range [1001,1040], 1 pt to use subtraction to obtain the final answer.

Addendum to #8 on the following page.

Multiple students came up with an alternative solution (which I thought was pretty cool). For either the range [1, 1000] or the range [521, 1000], the Inclusion/Exclusion Principle can be used. I'll show the solution using the I/E for the range [1, 1000]. Let A be the set of numbers in the range divisible by 2, B be the set of numbers divisible by 5 and C be the set of numbers divisible by 13. We aim to count the values in the range not divisible by any of these, so we can take the total and subtract out the values divisible by at least one of them.

The I/E principle states that:

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

Note that the $A \cap B$ is the set of values divisible by 10 in the range, $A \cap C$ is the set of values divisible by 26 in the range, $B \cap C$ is the set of values divisible by 65 in the range, and $A \cap B \cap C$ is the set of values divisible by 130 in the range. It follows that:

$$|A \cup B \cup C| = \left\lfloor \frac{1000}{2} \right\rfloor + \left\lfloor \frac{1000}{5} \right\rfloor + \left\lfloor \frac{1000}{13} \right\rfloor - \left\lfloor \frac{1000}{10} \right\rfloor - \left\lfloor \frac{1000}{26} \right\rfloor - \left\lfloor \frac{1000}{65} \right\rfloor + \left\lfloor \frac{1000}{130} \right\rfloor$$

Use the calculator and we have:

$$|A \cup B \cup C| = 500 + 200 + 76 - 100 - 38 - 15 + 7 = 630$$

integers that are divisible by 2, 5 or 13 in the range [1,1000].

Thus, there are 1000 – 630 = **370** integers in the range not divisible by any of these values.

Grading Note: These were graded on a case by case basis since there were relatively few students who used this principle and each of them used it just a bit differently.

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

Use a calculator to factor n via trial division with 2, 3, 5, 7, 11, 13, 17, 19 and 23 to find that n = 23 x 29. It follows that $\varphi(667) = \varphi(23) \times \varphi(29) = (23 - 1)(29 - 1) = 22 \times 28 = 616$

$d = 419^{-1} \bmod 616$

Use the Extended Euclidean Algorithm to determine d:

$616 = 1 \times 419 + 197$
$419 = 2 \times 197 + 25$
$197 = 7 \times 25 + 22$
$25 = 1 \times 22 + 3$
$22 = 7 \times 3 + 1$

$22 - 7 \times 3 = 1$
$22 - 7(25 - 22) = 1$
$22 - 7 \times 25 + 7 \times 22 = 1$
$8 \times 22 - 7 \times 25 = 1$
$8(197 - 7 \times 25) - 7 \times 25 = 1$
$8 \times 197 - 56 \times 25 - 7 \times 25 = 1$
$8 \times 197 - 63 \times 25 = 1$
$8 \times 197 - 63(419 - 2 \times 197) = 1$
$8 \times 197 - 63 \times 419 + 126 \times 197 = 1$
$134 \times 197 - 63 \times 419 = 1$
$134(616 - 419) - 63 \times 419 = 1$
$134 \times 616 - 134 \times 419 - 63 \times 419 = 1$
$134 \times 616 - 197 \times 419 = 1$

Take this equation mod 616 to yield
$-197 \times 419 \equiv 1 \pmod{616}$

It follows that $d \equiv -197 \equiv 616 - 197 \equiv$ **419** mod 616.

Grading: 2 pts phi, 3 pts Euclidean 5 pts Extended, 1 pt to get to -197, 1 pt to map to 419 , Automatic 0 out of 12 if did Euclidean with the wrong number.

Note: As you can see, this turned out to be an unusually bad choice for e!

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.

The key observation is that $C_1 = \alpha$. In the El-Gamal Cryptosystem, $C_1 = \alpha^k \bmod q$. This means that Bob made the poor choice of randomly selecting k = 1. Recall that $K = Y_A^k \bmod q$, but since k = 1, we know that K = 168.

Finally, recognize that $C_2 = KM \bmod q$, giving us the equation: $380 \equiv 168M \pmod{521}$

To solve for M, multiply this equation through by $168^{-1} \bmod 521$ via the Extended Euclidean Algorithm:

$521 = 3 \times 168 + 17$
$168 = 9 \times 17 + 15$
$17 = 1 \times 15 + 2$
$15 = 7 \times 2 + 1$

$15 - 7 \times 2 = 1$
$15 - 7(17 - 15) = 1$
$15 - 7 \times 17 + 7 \times 15 = 1$
$8 \times 15 - 7 \times 17 = 1$
$8(168 - 9 \times 17) - 7 \times 17 = 1$
$8 \times 168 - 72 \times 17 - 7 \times 17 = 1$
$8 \times 168 - 79 \times 17 = 1$
$8 \times 168 - 79(521 - 3 \times 168) = 1$
$8 \times 168 - 79 \times 521 + 237 \times 168 = 1$
$245 \times 168 - 79 \times 521 = 1$

Take this equation mod 521 to find that $245 \times 168 \equiv 1 \pmod{521}$, which means that $168^{-1} \equiv 245 \pmod{521}$

Getting back to the equation, we get:
$245 \times 380 \equiv 245 \times 168 \times M \pmod{521}$
$M \equiv 245 \times 380 \equiv 93100 \equiv$ **362** $\pmod{521}$, the intention was for this to be the course number mod 1000.

Grading: 2 pts for deduction that k = 1, 1 pt for deducing K = 168, 1 pt for recognizing that $168^{-1} \bmod 521$ is necessary to find M, 6 pts for Euclidean and Extended Euclidean, 2 pts to finish it off by multiplying the equation through by 245 to find M and reducing M to 362.

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.)

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

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

The code we looked at in class will first try to see if there's a point on the curve with x = 15, by trying the extra bits set to 0. If this value doesn't work, the code tries $x = 2^4 + 15 = 31$. If that doesn't work, then it will try $x = 2 \times 2^4 + 15 = 47$, followed by $x = 3 \times 2^4 + 15 = 63$. To try a value of x, calculate the right hand side of the elliptic curve equation, which, for this problem is $x^3 + 4x + 7 \bmod 83$. Call this value c. The next step is to calculate $c^{\frac{p-1}{2}} mod\ p$. If this value equals 1, there's a point on the curve with the corresponding x value. If this value doesn't equal 1, then there is not. (Recall this only works for primes that are 3 mod 4.) To calculate the corresponding y value when the previous calculation equals 1, calculate calculate $y = c^{\frac{p+1}{4}} mod\ p$. The table below encapsulates all the work for this problem, using the calculator to plug into $x^3 + 4x + 7 \bmod 83$.

x	$c = x^3 + 4x + 7 \bmod 83$	$c^{\frac{p-1}{2}} mod\ 83$	$c^{\frac{p+1}{4}} mod\ p$
15	39	82	
31	42	82	
47	19	82	
63	61	1	12

We get lucky on our fourth attempt. There are two points on this curve with x = 63. One of these points has y = 12. (The other is y = 71, but my code always returns the result $y = c^{\frac{p+1}{4}} mod\ p$.)

(63 , 12)

Grading: 2 pts to calculate 39, 42, 19 and 61, respectively, 2 pts to look up 12 correctly on the chart and answer with the correct point. Will give full credit to (63, 71) also.

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

ORANGE (Grading: Give to all)