

**Fall 2022 CIS 3362 Final Exam Part B – Quiz 1 – 4 Material (12/9/2022) – 90 pts Solutions**

1) (5 pts) The following ciphertext was encrypted using the shift cipher with an encryption key of 19. What is the corresponding plaintext?

AHEBWTRMBFX

- (A)  $0 - 19 = -19 = 7 \pmod{26}$  (H)
- (H)  $7 - 19 = -10 = 16 \pmod{26}$  (O)
- (E)  $4 - 19 = -15 = 11 \pmod{26}$  (L)
- (B)  $1 - 19 = -18 = 8 \pmod{26}$  (I)
- (W)  $22 - 19 = 3 \pmod{26}$  (D)
- (T)  $19 - 19 = 0 \pmod{26}$  (A)
- (R)  $17 - 19 = -2 = 24 \pmod{26}$  (Y)
- (M)  $12 - 19 = -7 = 19 \pmod{26}$  (T)
- (B)  $1 - 19 = -18 = 8 \pmod{26}$  (I)
- (F)  $5 - 19 = -14 = 12 \pmod{26}$  (M)
- (X)  $23 - 19 = 4 \pmod{26}$  (E)

**HOLIDAYTIME**

**Grading: 1 pt off per error, cap at 5.**

2) (5 pts) How many possible keys are there for an affine cipher with an alphabet size of 210? Please express your answer as a single integer (multiplied out).

b can be one of 210 possible values.

a must be relatively prime to b.

Thus, a can be one of  $\phi(210) = \phi(2 \times 3 \times 5 \times 7) = \phi(2) \times \phi(3) \times \phi(5) \times \phi(7) = 1 \times 2 \times 4 \times 6 = 48$  possible values.

Since each possible a can be paired with each possible b, there are a total of  $210 \times 48 = \underline{\underline{10080}}$  possible keys.

**Grading: 1 pt for # of bs, 3 pts for # of as, 1 pt for final answer**

3) (10 pts) One way to store a substitution cipher key in code would be to store a string of length 26, where the first letter is what 'A' encrypts to, the second letter is what 'B' encrypts to, and so forth. Complete the function below in C, which takes in an encryption key (first parameter), and stores the corresponding decryption key in the second input parameter. You may assume that the first parameter is a string of 26 unique uppercase letters. You are to fill the second parameter with the corresponding contents of the decryption key. (For example, if the first parameter was "QWERTYUIOPASDFGHJKLZXCVBNM", then the second parameter should be filled with the contents "KXVMCNOHQRSZYIJADLEGWBUFT".) Code has been added for you to take care of the null character (last line).

```
void setDecryptKey(char* encKey, char* decKey) {
    for (int i=0; i<26; i++)
        decKey[encKey[i]-'A'] = (char) ('A'+i);
    decKey[26] = '\\0';
}
```

**Grading: 1 pt loop, 1 pt to 26**  
**1 pt dec of something on LHS, 1 pt if any char is on RHS**  
**2 pts access encKey[i], 1 pt subtract 'A', 1 pt index decKey**  
**1 pt 'A' or RHS, 1 pt add i to it**

4) (5 pts) Show the playfair encryption box for the encryption key: "CHATTANOOGA".

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

**Grading: 1 pt for each error, cap at 5 (hopefully everyone gets this!)**

5) (10 pts) Consider a set T with n,  $n \geq 2$ , unique letters,  $L_1, L_2, L_3, \dots, L_n$  such that there are exactly i copies of the letter  $L_i$  for all integers  $1 \leq i \leq n$ . Determine, in simplified form, the index of coincidence of the set T.

(You may find the following formulas useful:  $\sum_{i=1}^n i = \frac{n(n+1)}{2}$ ,  $\sum_{i=1}^n i(i-1) = \frac{(n-1)n(n+1)}{3}$ .)

The total number of letters is  $\sum_{i=1}^n i = \frac{n(n+1)}{2}$ . Thus, we can get the index of coincidence of the set of letters by plugging into the formula:

$$\begin{aligned} \frac{\sum_{i=1}^n i(i-1)}{\frac{n(n+1)}{2} \times \left(\frac{n(n+1)}{2} - 1\right)} &= \\ \frac{4\left(\frac{(n-1)n(n+1)}{3}\right)}{n(n+1)(n(n+1) - 2)} &= \\ \frac{4(n-1)n(n+1)}{3n(n+1)(n^2 + n - 2)} &= \\ \frac{4(n-1)n(n+1)}{3n(n+1)(n-1)(n+2)} &= \\ \frac{4}{3(n+2)} \end{aligned}$$

**Grading: 1 pt to count the total number of letters, 2 pts to correctly use this to plug into the denominator. 1 pt to write the summation for the numerator, 1 pt to plug into the given formula for the numerator, 5 pts for the algebra (can give partial)**

6) (6 pts) Encrypt the plaintext “FRIDAY” using the Hill cipher key  $\begin{pmatrix} 11 & 6 \\ 8 & 7 \end{pmatrix}$ .

$$\begin{pmatrix} 11 & 6 \\ 8 & 7 \end{pmatrix} \begin{pmatrix} 5 \\ 17 \end{pmatrix} = \begin{pmatrix} 11 \times 5 + 6 \times 17 \\ 8 \times 5 + 7 \times 17 \end{pmatrix} = \begin{pmatrix} 55 + 102 \\ 40 + 119 \end{pmatrix} = \begin{pmatrix} 157 \\ 159 \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 3 \end{pmatrix} \rightarrow BD$$

$$\begin{pmatrix} 11 & 6 \\ 8 & 7 \end{pmatrix} \begin{pmatrix} 8 \\ 3 \end{pmatrix} = \begin{pmatrix} 11 \times 8 + 6 \times 3 \\ 8 \times 8 + 7 \times 3 \end{pmatrix} = \begin{pmatrix} 88 + 18 \\ 64 + 21 \end{pmatrix} = \begin{pmatrix} 106 \\ 85 \end{pmatrix} \equiv \begin{pmatrix} 2 \\ 7 \end{pmatrix} \rightarrow CH$$

$$\begin{pmatrix} 11 & 6 \\ 8 & 7 \end{pmatrix} \begin{pmatrix} 0 \\ -2 \end{pmatrix} = \begin{pmatrix} 11 \times 0 + 6 \times (-2) \\ 8 \times 0 + 7 \times (-2) \end{pmatrix} = \begin{pmatrix} 0 - 12 \\ 0 - 14 \end{pmatrix} = \begin{pmatrix} -12 \\ -14 \end{pmatrix} \equiv \begin{pmatrix} 14 \\ 12 \end{pmatrix} \rightarrow OM$$

### BDCHOM

**Grading: 2 pts per pair (give 2 pts if correct, 1 pt if right process but arithmetic error, 0 pt otherwise)**

7) (6 pts) A double column transposition was applied to a plaintext, first using the key word “HEAT”, followed by the keyword “CAMP”. The resulting ciphertext is: EMOTYRTSNIHGAMSL. What was the original plaintext?

Luckily the text is 16 characters and both keywords are length 4 and 16 is divisible by 4, so we won't have to worry about unbalanced rows or columns. Everything will fit perfectly. First, write down the second keyword “CAMP” and write down the corresponding permutation associated with it: (2, 1, 3, 4). Then copy the letters from the cipher text into the grid, writing down the first four letters in the column labeled 1, the next four letters in the column labeled 2, and so on:

2	1	3	4	
Y	E	N	A	
R	M	I	M	
T	O	H	S	
S	T	G	L	(So YENARMIMTOHSSTGL is the output.)

This was the output of applying the keyword HEAT. This keyword's corresponding permutation is (3, 2, 1, 4). So, we can do the same thing here, writing 4 letters at a time into the columns:

3	2	1	4
T	R	Y	S
O	M	E	T
H	I	N	G
S	M	A	L

Reading this in the usual way we arrive at the plaintext:

### TRYSOMETHINGSMAL

**Grading: 1 pt permutation for CAMP, 2 pts to get middle grid, 1 pt permutation HEAT, 2 pts to get grid and get plaintext.**

8) (4 pts) Let the input to the Expansion matrix E in DES be 9F6BC47A, in hexadecimal. What is the corresponding output, also represented in hexadecimal?

First write out the bits in the input:

1001 1111 0110 1011 1100 0100 0111 1010

Now, grab the bits asked for, here they are listed in groups of 6:

010011 111110 101101 010111 111000 001000 001111 110101

Regroup the bits into groups of size 4 and convert to hex:

0100 1111 1110 1011 0101 0111 1110 0000 1000 0011 1111 0101  
 4 F E B 5 7 E 0 8 3 F 5

4FEB57E083F5

**Grading: 4 pts correct answer, 3 pts correct answer in binary, 3 pts for hex with minor errors, 2 pts for binary with minor errors or hex with 3-5 errors, 1 pt if some semblance of process is correct but quite a few errors, 0 otherwise.**

9) (8 pts) Let the state matrix right before the Mix Columns stage of AES be  $\begin{bmatrix} 3F & C3 & 1E & 9D \\ 27 & 8B & 54 & 32 \\ D8 & 44 & B0 & E6 \\ 94 & D6 & A6 & 7C \end{bmatrix}$ .

What's the entry in row 3 column 2, right after this stage completes? (Answer in HEX.)

The desired entry is  $01 \times C3 + 01 \times 8B + 02 \times 44 + 03 \times D6$ .

$$01 \times C3 = C3$$

$$01 \times 8B = 8B$$

$$02 \times 44 = 1000\ 1000 = 88, \text{ left shift of original by 1 bit}$$

$$03 \times D6 = 02 \times D6 + 01 \times D6$$

$$\begin{array}{l} 02 \times D6 = 1\ 1010\ 1100 = 1010\ 1100 \\ \quad \quad \quad \wedge\ 0001\ 1011 \\ \quad \quad \quad = 1011\ 0111 \end{array} \quad \begin{array}{l} 03 \times D6 = 1011\ 0111\ (02 \times D6) \\ \quad \quad \quad \wedge\ 1101\ 0110\ (01 \times D6) \\ \quad \quad \quad = 0110\ 0001 \end{array}$$

It follows that  $03 \times D6 = 61$

Thus, our final result is  $(C3 \oplus 8B) \oplus (88 \oplus 61) = (48) \oplus (E9) = A1$

**Grading: max 3 of 10 if wrong term,**

**1 pt C3, 1 pt 8B, 2 pts 88, 2 pts 2 x D6, 2 pts final ans 3 x D6, 2 pts final XOR  
 -1 if answer is in binary**

10) (4 pts) What is the remainder when  $73^{4683}$  is divided by 521?

521 is a prime number. (Try division must be done by 2, 3, 5, 7, 11, 13, 17 and 19 because  $23^2 = 529$ .) Thus, Fermat's Theorem applies. Note that  $\phi(521) = 520$ , so  $73^{520} \equiv 1 \pmod{521}$ . Thus, we have:

$$73^{4683} = \text{when } 73^{4680+3} = 73^{4680}73^3 = (73^{520})^9 73^3 \equiv 1^9 73^3 \equiv 389017 \equiv 351 \pmod{521}$$

Note: factorization of 4680 and multiplication of  $73^3$  were done in the calculator, as well as the final mod.

**Grading: 2 pts for stating Fermat's as it applies, 1 pt to break down exponent, 1 pt to simplify to the correct answer.**

11) (6 pts) Consider using the Pollard-Rho factoring algorithm to factor 221. The algorithm runs a while loop until a particular condition. Each time through the while loop, two variables, a and b, are updated. In the chart below, show the values of a and b after each iteration. Two more "work" columns have been provided for you to use as you see fit. When the function returns, explain why the loop stops and determine the divisor of 221 that the algorithm returns. (The other can be ascertained by dividing this return value into 221.) Note: more rows than necessary are provided.

Iteration	a	b	Work Col #1	Work Col #2
0	2	2		
1	5	26	$26 - 5 = 21$	$\text{gcd}(221, 21) = 1$
2	26	197	$197 - 26 = 171$	$\text{gcd}(221, 171) = 1$
3	14	104	$104 - 14 = 90$	$\text{gcd}(221, 90) = 1$
4	197	145	$197 - 145 = 52$	$\text{gcd}(221, 52) = 13$
5				
6				
7				
8				

Divisor returned by Algorithm: **13**

How was the divisor determined in the last loop iteration? **By running GCD with the original number, 221, and the difference of a and b, 52.**

12) (10 pts) In an El Gamal system, Alice has the public keys  $q = 139$ , primitive root  $\alpha = 101$ , and  $Y_A = 68$ . Show the following steps of Bob sending Alice the message  $M = 16$  with the random integer  $k = 48$ :

1. Bob's calculation of  $K$
2. Bob's calculation of  $C_1$ .
3. Bob's calculation of  $C_2$ .

Much of what is being graded is being able to input modular exponentiations into the calculator by calculating the pieces necessary via the fast modular exponentiation algorithm. Show the work of the algorithm, but then just put each require result by multiplying and modding in the calculator.

$$K = Y_A^k \text{ mod } q = 68^{48} \text{ mod } 139.$$

Do this by calculating 68 raised to the powers 1, 2, 4, 8, 16 and 32 mod 139, using a calculator. (We get the next entry in the table by squaring the previous one and modding it):

Exp	1	2	4	8	16	32
$68^{\text{exp}} \text{ mod } 139$	68	37	118	24	20	122

It follows that  $K = 68^{16} 68^{32} \equiv (20 \times 122) \equiv 2440 \equiv 77 \pmod{139}$ .

$$C_1 = \alpha^k \text{ mod } q = 101^{48} \pmod{139}$$

Do this by calculating 101 raised to the powers 1, 2, 4, 8, 16 and 32 mod 139, using a calculator. (We get the next entry in the table by squaring the previous one and modding it):

Exp	1	2	4	8	16	32
$101^{\text{exp}} \text{ mod } 139$	101	54	136	9	81	28

It follows that  $K = 101^{16} 101^{32} \equiv (81 \times 28) \equiv 2268 \equiv 44 \pmod{139}$ .

$$C_2 = KM = 77 \times 16 = 1232 \equiv 120 \pmod{139}$$

$$\mathbf{K = 77, C_1 = 44, C_2 = 120}$$

**Grading: 4 pts K, 4 pts C1, 2 pts C2**  
**For K and C1, 1 pt answer, 3 pts process**

13) (10 pts) Consider the elliptic curve  $E_{53}(13, 19)$ . One point on this curve is  $P = (8, 30)$ . Determine  $4P$ .

First, let's find  $2P$ .  $\lambda = \frac{3x_p^2+a}{2y_p} = \frac{3 \times 8^2+13}{2(30)} = \frac{205}{60} = \frac{41}{12} \equiv 41 \times (12^{-1}) \pmod{53}$ .

Run the Extended Euclidean to find  $12^{-1} \pmod{53}$

$$\begin{aligned} 53 &= 4 \times 12 + 5 & 5 - 2 \times 2 &= 1 \\ 12 &= 2 \times 5 + 2 & 5 - 2(12 - 2 \times 5) &= 1 \\ 5 &= 2 \times 2 + 1 & 5 \times 5 - 2 \times 12 &= 1 \\ & & 5(53 - 4 \times 12) - 2 \times 12 &= 1 \rightarrow 5 \times 53 - 22 \times 12 = 1 \\ & & \text{It follows that } 12^{-1} &\equiv -22 \equiv 31 \pmod{53} \end{aligned}$$

Thus,  $\lambda = 41 \times (12^{-1}) \equiv 41 \times 31 \equiv 1271 \equiv 52 \equiv -1 \pmod{53}$

$x_{2P} = (\lambda^2 - 2x_p) = 1 - 2(8) = -15 \equiv 38$

$y_{2P} = (\lambda(x_p - x_{2P}) - y_p) = (-1(8 - 38) - 30) = 30 - 30 = 0$ .

**This means that  $2P = (38, 0)$ .**

In trying to calculate  $4P$  we run into the problem of lambda dividing by 0. If you remember from class, each point has a cycle length – if you keep on adding it to itself, you eventually get the origin, and then the whole sequence  $P, 2P, 3P$ , etc. repeats. In that print out, the halfway point (if there is one) is always a point of the form  $(x, 0)$ . In short, adding  $(x, 0)$  to itself, since it has infinite slope, so to speak, creates the point at infinity, which is the origin. Thus,  **$4P$  is the origin.**

**Grading: 1 pt lambda set up, 1 pt to get to either  $41 \times 12^{-1}$  or  $205 \times 60^{-1}$   
 4 pts for extended Euclidean to get the inverse (60 inverse is -15 or 38.)  
 1 pt for x for 2p, 1 pt for y of 2p, 2 pts for answer for 4P from there.**

14) (1 pt) What beverage does the company Yogi Tea make? **Tea (Grading: Give to all)**