Fall 2021 CIS 3362 Final Exam (12/8/2021) Part A Solutions

1) (5 pts) Decrypt the following ciphertext produced by the shift cipher: `KPRPIXDCIXBT`.

Just try the first few letters with each shift:

```
KPRP      OTVT      SXZX
LQSQ      PUWU      TYAY
MRTR      QVXV      UZBZ
NSUS      RWYW      VACA
```

```
…this last one, VACA, looks promising, let's try it! (So the
encryption key was +15, to decrypt, subtract 15 or add 11.)
```

```
K(10) + 11 = 21                (V)
P(15) + 11 = 26 ≡ 0 mod 26     (A)
R(17) + 11 = 28 ≡ 2 mod 26     (C)
P(15) + 11 = 26 ≡ 0 mod 26     (A)
I(8)  + 11 = 19                (T)
X(23) + 11 = 34 ≡ 8 mod 26     (I)
D(3)  + 11 = 14                (O)
C(2)  + 11 = 13                (N)
I(8)  + 11 = 19                (T)
X(23) + 11 = 34 ≡ 8 mod 26     (I)
B(1)  + 11 = 12                (M)
T(19) + 11 = 30 ≡ 4 mod 26     (E)
```

VACATION TIME (Grading: 1 pt off per incorrect letter cap at 0.)

2) (5 pts) A bin of candy has 30 Snickers bars, 25 Reece's Pieces packages, 50 Twix bars and 20 Skittles packages. Serena takes two of the items from the bin at random. What is the probability that she gets two of the same type of candy? **Please express your answer as a fraction in lowest terms.**

This is the same definition of index of coincidence! (Or you can just apply your knowledge of probability…)

$$p(Same\ 2) = \frac{30 \times 29 + 25 \times 24 + 50 \times 49 + 20 \times 19}{125 \times 124} = \frac{870 + 600 + 2450 + 380}{15500}$$

$$= \frac{4300}{15500} = \frac{\mathbf{43}}{\mathbf{155}}$$

(Grading: 2 pts numerator, 1 pt denominator, 2 pts to reduce to lowest terms)

3) (10 pts) Consider an affine cipher for an alphabet of size 79 with the encryption function

$$f(x) = (28x + 49) \bmod 79$$

Determine the corresponding decryption function $f^{-1}(x)$.

Place x where f(x) is and $f^{-1}(x)$ where x is:

$x = (28f^{-1}(x) + 49) \bmod 79$
$(x - 49) = 28f^{-1}(x) \bmod 79$

Determine 28^{-1} mod 79 via Extended Euclidean Algorithm:

$79 = 2 \times 28 + 23$
$28 = 1 \times 23 + 5$
$23 = 4 \times 5 + 3$
$5 = 1 \times 3 + 2$
$3 = 1 \times 2 + 1$

$3 - 2 = 1$
$3 - (5 - 3) = 1$
$2 \times 3 - 1 \times 5 = 1$
$2(23 - 4 \times 5) - 1 \times 5 = 1$
$2 \times 23 - 8 \times 5 - 1 \times 5 = 1$
$2 \times 23 - 9 \times 5 = 1$
$2 \times 23 - 9(28 - 23) = 1$
$2 \times 23 - 9 \times 28 + 9 \times 23 = 1$
$11 \times 23 - 9 \times 28 = 1$
$11(79 - 2 \times 28) - 9 \times 28 = 1$
$11 \times 79 - 22 \times 28 - 9 \times 28 = 1$
$11 \times 79 - 31 \times 28 = 1$
Taking this equation mod 79 we find that $-31 \times 28 \equiv 1 \pmod{79}$, so $28^{-1} \equiv -31 \equiv 48 \pmod{79}$.

$48(x - 49) \equiv 48(28f^{-1}(x)) \bmod 79$
$f^{-1}(x) \equiv 48x - 2352 \pmod{79}$

$f^{-1}(x) = (48x + 18) \pmod{79}$

Grading: Swapping x, $f^{-1}(x)$ places - 1 pt
Getting to step before EEA - 1 pt
Euclidean Algorithm - 2 pts
Extended, extract inverse - 4 pts
Mult through - 1 pt
Map inverse function into range - 1 pt

4) (5 pts) Using the Playfair cipher with the padding character 'X' to encrypt the plaintext: "MISSISSIPPIMADNESS" using the secret key: "VIRGINIA"

First create the encryption key matrix:

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

Next, split the plaintext into digraphs, padding as necessary:

MI SX SI SX SI PX PI MA DN ES SX

and encrypt:

HN QY PG QY PG QW WB FE EG DT QY

Without spaces, we have **HNQYPGQYPGQWWBFEEGDTQY**

Grading: 2 pts for square, 1 pt for all the padding chars in the right place, 2 pts for correct application of all the rules (Award a whole number of points, only giving full credit if the answer is completely correct. So, most minor errors will get 4 of 5.)

5) (5 pts) What is the corresponding decryption key for the encryption key $\begin{pmatrix} 13 & 8 \\ 2 & 17 \end{pmatrix}$ for the Hill cipher using an alphabet of size 26?

The determinant of the matrix is 13 x 17 - 2 x 8 = 221 - 16 = 205 ≡ -3 (mod 26). The inverse of this value mod 26 is -9 ≡ 17 (mod 26). (Just use the provided look up chart for inverses mod 26. Either look up the inverse of 3 or 23 and use accordingly.)

It follows the corresponding decryption matrix is $17\begin{pmatrix} 17 & -8 \\ -2 & 13 \end{pmatrix} = \begin{pmatrix} 289 & -136 \\ -34 & 221 \end{pmatrix}$, mapping each of these values mod 26 we get $\begin{pmatrix} \mathbf{3} & \mathbf{20} \\ \mathbf{18} & \mathbf{13} \end{pmatrix}$.

Grading: 2 pts for determinant, 1 pt for its inverse mod 26, 1 pt for plugging into the formula, 1 pt for reducing

Fall 2021 CIS 3362 Final Exam (12/8/2021) Part B Solutions

6) (8 pts) Let the input to the S-boxes in DES be 9FC 65B 05A D38, in hex. What is the output produced by the S-boxes. **Express your result in hex.**

9 F C 6 5 B 0 5 A D 3 8 converted to binary is

1001 1111 1100 0110 0101 1011 0000 0101 1010 1101 0011 1000

Now, split into groups of size 6 and give as inputs to the corresponding S-boxes:

S_1(100111) = 2 (row 11 = 3, col 0011 = 3)
S_2 (111100) = 2 (row 10 = 2, col 1110 = E)
S_3(011001) = C (row 01 = 1, col 1100 = C)
S_4(011011) = A (row 01 = 1, col 1101 = D)
S_5(000001) = E (row 01 = 1, col 0000 = 0)
S_6(011010) = 7 (row 00 = 0, col 1101 = D)
S_7(110100) = 6 (row 10 = 2, col 1010 = A)
S_8(111000) = F (row 10 = 2, col 1100 = C)

Final Output is **22CAE76F.**

Grading: 1 pt per each hex character, **NO EXCEPTIONS!!!**

7) (5 pts) How many bits are each of the following pieces of data in the DES algorithm:

(a) Plaintext Input Block Size: **64**

(b) Key Size: **56**

(c) Round Key Size: **48**

(d) Size of Output from Function f **32**

(e) Size of buffer for cyclic key shifts (there are 2) in the key scheduling algorithm. **28**

Grading: 1 pt per answer, must be correct to get the point.

8) (10 pts) If the state matrix is the following right before the Mix Columns step of AES, what is the entry in row 4, column 2, right after the Mix Columns step? **Please provide your answer as two HEX characters.** ***(Note: Please be very, very, very careful that you work out the correct entry. If you find the entry of row 2, column 4, you will earn a maximum of 3 points out of 10.)***

$$\begin{pmatrix} 3A & BC & CD & 12 \\ 2C & 65 & 96 & 4F \\ 97 & F3 & A0 & 62 \\ B2 & C9 & 7E & D3 \end{pmatrix}$$

Note that the fixed matrix multiplier for the Mix Columns step in AES is $\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix}$.

The term we want to calculate is 03 x BC + 01 x 65 + 01 x F3 + 02 x C9. Let's calculate the first and last terms:

```
03 x BC = 02 x BC + 01 x BC

02 x BC = 1 0111 1000          03 x BC =  1011 1100
                                        + 0110 0011
        =   0111 1000                   -----------
          +    1 1011                     1101 1111 (DF)
          -------------
            0110 0011

02 x C9 = 1 1001 0010

        =   1001 0010
          +    1 1011
            ---------
            1000 1001 (89)
```

Adding in HEX we get (DF + 65) + (F3 + 89) = BA + 7A = **C0**

Grading: 2 pts to write out correct product, 3 pts for first term, 2 pts for second term, 2 pts to XOR, 1 pt to convert to hex. Max 3 pts out of 10 if the wrong initial product is written out.

Fall 2021 CIS 3362 Final Exam (12/8/2021) Part C Solution

9) (10 pts) Define $\phi_k(n)$ to be the Euler Phi Function composed with itself k times. For example, $\phi_3(n) = \phi(\phi(\phi(n)))$ and $\phi_5(n) = \phi(\phi\left(\phi\left(\phi(\phi(n))\right)\right))$. Define f(n) to be the minimum value of k such that $\phi_k(n) = 1$. For example, f(5) = 3 since $\phi(\phi(5)) = 2$ and $\phi\left(\phi(\phi(5))\right) = 1$. Find the smallest value of n such that f(n) = 5. (Note: $\phi(1) = 1$.) **(Note: Full credit will only be given with ample proof.)**

The key observation to solving this problem quickly is to note that if f(φ(n)) = k, then f(n) = k+1. Thus, we can just calculate the values of f(n) in ascending order, noting that f(1) = 0. This table can be filled out from left to right:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
φ(n)	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16
f(n)	0	1	2	2	3	2	3	3	3	3	4	3	4	3	4	4	5

It follows that the desired smallest value of n is **n = 17.**

Note the following chain:

φ(17) = 16, φ(16) = 8, φ(8) = 4, φ(4) = 2, and φ(2) = 1.

Note: We use the usual formula for φ(n) when making the calculations above. The numbers are small enough that we can prime factorize each value of n mentally and plug into the formula for φ accordingly. As an example, $12 = 2^2 \times 3$, so $\varphi(12) = (2^2 - 2^1)(3^1 - 3^0) = 2 \times 2 = 4$.

Grading: 3 pts for giving the answer 17.
2 pts for showing that f(17) = 5
5 pts for showing that f(n) < 5 for all n < 17.

Note: Points may be awarded on a discretionary basis for answers that aren't correct but show some progress towards a solution or understanding of the question being posed.

10) (10 pts) In an RSA system, n = 527 and e = 197. Determine both φ(n) and d. (Put a box around both answers and clearly mark them.) **Full credit will only be given if work for the Extended Euclidean Algorithm is show.**

First, we must prime factorize 527. We can do this by guess and check with the calculator, or Fermat Factoring. $\sqrt{527}$ is pretty close to 23, so let's try

$23^2 - 527 = 2$ (not a square)
$24^2 - 527 = 49$ (perfect square)
$24^2 - 527 = 7^2$, so $24^2 - 7^2 = 527$ and $527 = (24 - 7)(24 + 7) = 17 \times 31$.

It follows that p = 17, q = 31 and φ(n) = (17 - 1)(31 - 1) = 16 x 30 = 480

We must find $d = 197^{-1} \bmod 480$ via the Extended Euclidean Algorithm:

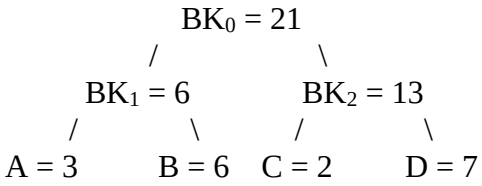
480 = 2 x 197 + 86
197 = 2 x 86 + 25
86 = 3 x 25 + 11
25 = 2 x 11 + 3
11 = 3 x 3 + 2
3 = 1 x 2 + 1

3 - 2 = 1
3 - (11 - 3 x 3) = 1
3 - 1 x 11 + 3 x 3 = 1
4 x 3 - 1 x 11 = 1
4(25 - 2 x 11) - 1 x 11 = 1
4 x 25 - 8 x 11 - 1 x 11 = 1
4 x 25 - 9 x 11 = 1
4 x 25 - 9(86 - 3 x 25) = 1
4 x 25 - 9 x 86 + 27 x 25 = 1
31 x 25 - 9 x 86 = 1
31(197 - 2 x 86) - 9 x 86 = 1
31 x 197 - 62 x 86 - 9 x 86 = 1
31 x 197 - 71 x 86 = 1
31 x 197 - 71 (480 - 2 x 197) = 1
31 x 197 - 71 x 480 + 142 x 197 = 1
173 x 197 - 71 x 480 = 1

Take this equation mod 480 to yield $173 \times 197 \equiv 1 \pmod{480}$. It follows that **d = 173.**

Grading: 2 pts prime factorization (any way),
1 pt phi,
2 pts Euclidean,
4 pts Extended,
1 pt final answer

11) (9 pts) Consider a Group Diffie-Hellman Key Exchange using the public elements p = 23 and g = 5. Let the current structure of the keys and users A, B, C and D be as follows:



Imagine that user B wants to sponsor a new user E to create a new shared key BK_3 in the tree structure where B is currently located using new secret keys B = 10 and E = 14. In this process, the blind keys BK_3, BK_1 and BK_0 each need to be recalculated, respectively. Write down the modular exponentiation calculation to figure out each of the blind keys, in sequence, and show the result of each (as an integer in between 0 and 22, inclusive.)

First we calculate $BK_3 = 5^{10(14)} = 5^{140} \equiv 5^{22(6)+8} \equiv (5^{22})^6 5^8 \equiv 1^6 5^8 \equiv \mathbf{16} \pmod{23}$, via Fermat's formula and use of the calculator. (Note: $5^8 = 390625 \equiv 16 \pmod{23}$.)

Next, we recalculate BK_1 using the secret keys for A and BK_3. So we get:

$BK_1 = 5^{3(16)} = 5^{48} \equiv 5^{22(2)+4} \equiv (5^{22})^2 5^4 \equiv 1^2 5^4 \equiv \mathbf{4} \pmod{23}$.

Finally, we recalculate BK_0 as follows:

$BK_0 = 5^{4(13)} = 5^{52} \equiv 5^{22(2)+8} \equiv (5^{22})^2 5^8 \equiv 1^2 5^8 \equiv \mathbf{16} \pmod{23}$.

$BK_3 = \mathbf{16}$ $BK_1 = \mathbf{4}$ $BK_0 = \mathbf{16}$

Grading: 3 pts per value, try to give credit for correct work after an error, if possible. (So if there's only one error but it cascades to change the other 2 values, just take off a point for that error.)

Fall 2021 CIS 3362 Final Exam (12/8/2021) Part D Solutions

12) (10 pts) Consider the elliptic curve $E_{47}(10, 17)$. Let the point P on the curve be (24, 13) and the point Q on the curve be (35, 7). Calculate P + Q.

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P} = \frac{7 - 13}{35 - 24} = (11^{-1})(-6)\ mod\ 47$$

Use the Extended Euclidean Algorithm to find 11^{-1} mod 47:

47 = 4 x 11 + 3
11 = 3 x 3 + 2
3 = 1 x 2 + 1

3 - 1 x 2 = 1
3 - (11 - 3 x 3) = 1
4 x 3 - 1 x 11 = 1
4(47 - 4 x 11) - 1 x 11 = 1
4 x 47 - 16 x 11 - 1 x 11 = 1
4 x 47 - 17 x 11 = 1, take this equation mod 47 to yield that -17 x 11 ≡ 1 (mod 47)

It follows that $11^{-1} \equiv -17 \pmod{47}$, now, complete solving for lambda:

$$\lambda = (11^{-1})(-6)\ mod\ 47 \equiv (-17) \times (-6) \equiv 102 \equiv 8\ (mod\ 47)$$

$x_{P+Q} = (\lambda^2 - x_P - x_Q) = 8^2 - 24 - 35 = 5$

$y_{P+Q} = \lambda(x_P - x_{P+Q}) - y_P = 8(24 - 5) - 13 = 8(19) - 13 = 139 \equiv 45\ (mod\ 47)$

It follows that (24, 13) + (35, 7) = **(5, 45).**

Grading: 2 pts lambda set up, 3 pts EEA, 1 pt lambda value, 2 pts plug in for x, 2 pts plug in for y.

13) (5 pts) Why is the following hash function, which produces an 8 bit output, a bad hash function?

```
#include <string.h>
int f(char* word) {
    int len = strlen(word);
    int res = (int)word[0];
    for (int i=1; i<len; i++)
        res = (res & ((int)word[i]));
    return res;
}
```

Not each of the 256 possible outputs are equally likely. This is because if you take the bitwise and of several random characters, it's very unlikely that there will be any 1s (unless the data has a lot of the same values) because eventually, in most bit locations, you'll see at least one 0, which would result in that bit being permanently turned to 0 in the output result.

Grading: 1 pt for stating that not all outputs are equally likely, 4 pts for the reasoning.

14) (3 pts) Who is the host of the Kelly Clarkson Show? **Kelly Clarkson**, give to all