1) (5 pts) Encrypt "BREAK" using the shift cipher and a key of $k = 7$.

\[
\begin{array}{cccccc}
B & R & E & A & K & = 1 & 17 & 4 & 0 & 10 \\
+ & 7 & 7 & 7 & 7 & 7 \\
\hline
& 8 & 24 & 11 & 7 & 17 \\
\end{array}
\]

Ciphertext = IYLHR (Grading: 1 pt per letter)

2) (5 pts) Decrypt the ciphertext "DHDTHEBUZO" which was encrypted using the Vigenere Cipher with the keyword "DOLPHIN".

\[
\begin{array}{cccccccccccc}
D & H & D & T & H & E & B & U & Z & O & = 3 & 7 & 3 & 19 & 7 & 4 & 1 & 20 & 25 & 14 \\
D & O & L & P & H & I & N & D & O & L & = 3 & 14 & 11 & 15 & 7 & 8 & 13 & 3 & 14 & 11 \\
\hline
& 0 & -7 & -8 & 4 & 0 & -4 & -12 & 17 & 11 & 3 \\
& 0 & 19 & 18 & 4 & 0 & 22 & 14 & 17 & 11 & 3 \\
\end{array}
\]

Plaintext: AT SEA WORLD (Grading: \(\frac{3}{2}\) pt per letter round down)
3) (10 pts) Consider an affine cipher for an alphabet of size 65 with the encryption function 
\[ f(x) = 28x + 33 \mod 65 \]

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

To find the inverse function, we switch \( x \) and \( y \) and solve for \( y \):

\[
x = (28y + 33) \mod 65 \\
28y = (x - 33) \mod 65
\]

We have to find \( 28^{-1} \mod 65 \) via the Extended Euclidean Algorithm:

\[
65 = 2 \times 28 + 9 \\
28 = 3 \times 9 + 1
\]

\[
28 - 3 \times 9 = 1 \\
28 - 3(65 - 2 \times 28) = 1 \\
28 - 3 \times 65 + 6 \times 28 = 1 \\
7 \times 28 - 3 \times 65 = 1, \text{ take this equation mod 65 to yield} \\
7 \times 28 = 1 \pmod{65}, \text{ thus } 28^{-1} = 7 \pmod{65}
\]

Multiply both sides of the previous equation by 7:

\[
7(28y) = 7(x - 33) \mod 65 \\
y = 7x - 231 \mod 65 \\
y = (7x + 29) \mod 65
\]

It follows that the decryption function \( f^{-1}(x) = (7x + 29) \mod 65 \)

**Grading:** 2 pts to get to \( 28y = (x - 33) \), 2 pts Euclidean, 4 pts Extended, 2 pts to finish it. Give 9 out of 10 if final answer is \( 7x - 231 \), Give 8 out of 10 if final answer is \( 7(x - 33) \).
4) (10 pts) Using the ADFGVX cipher encrypt the plaintext

"AT3AMGOTO2865MILLSAVEWITHTHEPACKAGE"

with the keyword "GRANOLA" and the following matrix key:

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>D</th>
<th>F</th>
<th>G</th>
<th>V</th>
<th>X</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>D</td>
<td>P</td>
<td>Y</td>
<td>2</td>
<td>G</td>
<td>M</td>
</tr>
<tr>
<td>D</td>
<td>S</td>
<td>U</td>
<td>J</td>
<td>B</td>
<td>4</td>
<td>V</td>
</tr>
<tr>
<td>F</td>
<td>L</td>
<td>H</td>
<td>X</td>
<td>Letter O</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>3</td>
<td>Number 1</td>
<td>A</td>
<td>7</td>
<td>9</td>
<td>E</td>
</tr>
<tr>
<td>V</td>
<td>Letter I</td>
<td>W</td>
<td>Z</td>
<td>5</td>
<td>K</td>
<td>8</td>
</tr>
<tr>
<td>X</td>
<td>Q</td>
<td>F</td>
<td>N</td>
<td>T</td>
<td>C</td>
<td>Number 0</td>
</tr>
</tbody>
</table>

AT3AMGOTO = GF XG GA GF AX AV FX XG FX
2865MILLSAVE = AG VX FF VG AX VA FA FA DA GF DX GX
WITHTHEPACKAGE = VD VA XG FD XG FD GX AD GF XV VV GF AV GX

Now, write down the keyword, followed by numbering the columns in alphabetical order, followed by the message with ADFGVX written in rows:

<table>
<thead>
<tr>
<th>G</th>
<th>R</th>
<th>A</th>
<th>N</th>
<th>O</th>
<th>L</th>
<th>A</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>7</td>
<td>1</td>
<td>5</td>
<td>6</td>
<td>4</td>
<td>2</td>
</tr>
</tbody>
</table>

| G | F | X | G | G | A | G |
| F | A | X | A | V | F | V |
| X | G | F | V | A | G | V |
| X | F | F | V | G | A | X |
| V | A | F | A | F | A | D |
| A | G | F | D | X | G | X |
| V | D | V | A | X | G | F |
| D | X | G | F | D | G | X |
| A | D | G | F | X | V | V |
| V | G | F | A | V | G | X |

Reading down the columns in numerical order, we get the following:

XXFFFFVGGF GVVXDFXXVX GFXXVAVDVV AFGAGGGVG GAVVADAFFA

GVAGFXXDXV FAGFAGDXXG

Grading: 3 pts for the ADFGVX conversion (just spot check)
3 pts for writing key word and corresponding numbers
2 pts for copying in ADFGVX text row first
2 pts for reading off the columns
Just spot check, if process is right but there are minor errors give 9/10.
5) (4 pts) Consider the following IP matrix for a DES-like cipher with a block size of 16 bits:

$$IP = \begin{bmatrix}
14 & 9 & 8 & 3 \\
6 & 12 & 1 & 11 \\
16 & 7 & 5 & 15 \\
2 & 4 & 10 & 13
\end{bmatrix}$$

If the input to the IP matrix in HEX is 4F79, what is the output, represented in HEX?

Convert the input to binary: 0100 1111 0111 1001

Take the bits designated: 0 0 1 0 1 1 0 1 1 1 0 1 0 1 1

Converting to HEX we get: 2 D E B

Grading: 1 pt per HEX char. Give 2 of 4 if answer left in binary

6) (8 pts) Let the input to the S-boxes in DES be 60D 5C7 281 E39, in hex. What is the output produced by the S-boxes. Express your result in hex.

Inp: 0110 0000 1101 0101 1100 0111 0010 1000 0001 1110 0011 1001
Inp(in6): 011000 001101 010111 000111 001010 000001 111000 111001

S1(011000) = S1(row 0, col 12) = 5
S2(001101) = S2(row 1, col 6) = 8
S3(010111) = S3(row 1, col 11) = 14(E)
S4(000111) = S4(row 1, col 3) = 5
S5(001010) = S5(row 0, col 5) = 10(A)
S6(000001) = S6(row 1, col 0) = 10(A)
S7(111000) = S7(row 2, col 12) = 0
S8(111001) = S8(row 3, col 12) = 3

Output in Hex = 58E5AA03.

Grading: 1 pt per hex char all or nothing.
7) (4 pts) Let the state matrix to AES right before the ShiftRows step be the matrix shown below. Show the state of the matrix right AFTER the ShiftRows step:

<table>
<thead>
<tr>
<th>5F</th>
<th>02</th>
<th>37</th>
<th>1A</th>
</tr>
</thead>
<tbody>
<tr>
<td>23</td>
<td>5F</td>
<td>30</td>
<td>E6</td>
</tr>
<tr>
<td>BB</td>
<td>74</td>
<td>8A</td>
<td>CD</td>
</tr>
<tr>
<td>7F</td>
<td>45</td>
<td>D3</td>
<td>4E</td>
</tr>
</tbody>
</table>

Grading: 1 pt per row

8) (15 pts) One way to calculate $\phi(n)$ is to find each unique prime number, $p_i$ that is a factor of $n$, and multiply $n$ by each term of the form $(p_i - 1)/p_i$. Notice that since $p_i$ is a divisor of $n$, one can first do the division and then the multiplication and the answer will be accurate without risk of overflow. In the algorithm we maintain two “accumulators” a running value of $n$ and a running value of $\phi$. Both are initialized to $n$ and both will get reduced in different ways over the course of the algorithm, which is described below.

Consider using this algorithm to calculate $\phi(300)$. We first discover that 2 is a prime factor of 300. So take 300 and multiply by $1/2$, yielding 150, our running value of phi. In addition, divide out each factor of 2 from 300 to yield 75, what remains after dividing out each copy of 2, our running value of $n$. Next, we discover that 3 is a prime factor of 75. Thus, we take 150 and multiply by $2/3$ yielding 100. In addition, we take 75 and divide out all copies of 3, yielding 25. Finally, we find that 5 is a prime factor of 25, so we multiply 100 by $4/5$ yielding 80. Once we divide out all copies of 5 from 25 and get 1, we find that we are done. It follows that $\phi(300) = 80$, which is what our function should return in this instance.

In some instances, we will be left with a prime number instead of 1. Consider, if after dividing by 5 we had 37 left. Then, after dividing by 6, we see that we’ve tried all values less than or equal to the square root of 37, so we know there’s no point in continuing the trial division. In this case, we would multiply our running value of phi by $36/37$ after exiting our main loop. (Note: if you continue trial division all the way to $n$ instead of stopping early and do everything else correct, you’ll earn 12 of 15 points on this question.)

Write a C function that implements the calculation of phi using the algorithm described above. (Note: no array is needed for this function, just two accumulator variables and a set of nested loops that do the process described above.

Write your function on the next page. (Note: You probably won’t use all of the space, but it’s provided anyway.)
int phi(int n) {
    int res = n; // 1 pt
    int i = 2; // 1 pt

    while (i*i <= n) { // 3 pts
        int exp = 0; // 1 pt
        while (n%i == 0) { // 2 pts
            n /= i; // 1 pt
            exp++; // 1/2 pts
        }
        if (exp > 0) // 1 pt
            res = res/i*(i-1); // 1 pt
        i++; // 1 pt
    }
    if (n > 1) // 1 pt
        res = res/n*(n-1); // 1 pt
    return res; // 1/2 pt
}
9) (10 pts) In an RSA system, \( n = 551 \) and \( e = 275 \). Determine both \( \phi(n) \) and \( d \). (Put a box around both answers and clearly mark them.)

\[ n = 551 = 19 \times 29 \text{ (use trial division to get this)} \]

\[ \phi(19 \times 29) = (19 - 1)(29 - 1) = 18 \times 28 = \boxed{504} \]

\[ d = 275^{-1} \mod 504 \]

\[ 504 = 1 \times 275 + 229 \\
275 = 1 \times 229 + 46 \\
229 = 4 \times 46 + 45 \\
46 = 1 \times 45 + 1 \]

\[ 46 - 1 \times 45 = 1 \\
46 - (229 - 4 \times 26) = 1 \\
46 - 1 \times 229 + 4 \times 46 = 1 \\
5 \times 46 - 1 \times 229 = 1 \\
5(275 - 229) - 1 \times 229 = 1 \\
5 \times 275 - 5 \times 229 - 1 \times 229 = 1 \\
5 \times 275 - 6 \times 229 = 1 \\
5 \times 275 - 6(504 - 275) = 1 \\
5 \times 275 - 6 \times 504 + 6 \times 275 = 1 \\
11 \times 275 - 6 \times 504 = 1 \]

Taking this equation \( \mod 504 \) we get:

\[ 11 \times 275 \equiv 1 \text{ (mod 504)} \]

It follows that \( d = 11. \)
10) (10 pts) Consider signing a message using the El Gamal Signature Scheme. Calculate the signature \((S_1, S_2)\) given that the public elements of the system are (prime) \(q = 41\), (generator) \(\alpha = 6\), the private key \(X_A = 5\) and the message you are signing has a hash value \(m = 24\). When you sign, select the random value \(K = 9\) (to make grading easier!) **Note: Do NOT show the work of verifying this signature. Rather, only do the work to produce the signature.**

\[ S_1 = \alpha^K \mod q = 6^9 \mod 41, \text{ by hand we do:} \]

\[ S_1 = 6^9 = (6^2)^4(6) \equiv 36^4(6) \equiv (-5)^4(6) \equiv 625(6) \equiv 10(6) \equiv 60 \equiv 19 \pmod{41} \]

Next step, compute \(K^{-1} \mod q-1\), so we must compute \(9^{-1} \mod 40\) via the Extended Euclidean Algorithm:

\[ 40 = 4 \times 9 + 4 \]
\[ 9 = 2 \times 4 + 1 \]

\[ 9 - 2 \times 4 = 1 \]
\[ 9 - 2(40 - 4 \times 9) = 1 \]
\[ 9 - 2 \times 40 + 8 \times 9 = 1 \]
\[ 9 \times 9 - 2 \times 40 = 1 \]

Taking this equation \(\mod 40\) we get:

\[ 9^{-1} \equiv 9 \pmod{40} \]

\[ S_2 = K^{-1}(m - X_AS_1) \mod q-1 \]
\[ = 9(24 - 5(19)) \mod 40 \]
\[ = 9(24 - 95) \mod 40 \]
\[ = 9(-71) \mod 40 \]
\[ = 9(9) \mod 40 \]
\[ = 1 \]

The correct signature for these choices is signature is \((19, 1)\).
11) (10 pts) Consider the elliptic curve $E_{37}(2, 3)$. Let the point $P$ on the curve be $(15, 2)$ and the point $Q$ on the curve be $(25, 29)$. Calculate $P + Q$.

$$\lambda = \frac{29 - 2}{25 - 15} = (27 \times 10^{-1}) \mod 37$$

We must use the Extended Euclidean Algorithm to find $10^{-1} \mod 37$:

37 = 3 x 10 + 7
10 = 1 x 7 + 3
7  = 2 x 3 + 1

7 – 2 x 3 = 1
7 – 2(10 – 7) = 1
7 – 2 x 10 + 2 x 7 = 1
3 x 7 – 2 x 10 = 1
3(37 – 3 x 10) – 2 x 10 = 1
3 x 37 – 9 x 10 – 2 x 10 = 1
3 x 37 – 11 x 10 = 1
Take this equation \mod 37 to yield:
-11 x 10 ≡ 1 (mod 37)

It follows that $10^{-1} ≡ -11$ (mod 37)

So,

$$\lambda = (27 \times 10^{-1}) \equiv (27 \times (-11)) \equiv -297 \equiv 36 \equiv -1 \mod 37$$

$$x_R = (\lambda^2 - x_P - x_Q) = ((-1)^2 - 15 - 25) \equiv (1 - 40) \equiv -39 \equiv 35 \mod 37$$

$$y_R = (\lambda(x_P - x_R) - y_P) = -1(15 - 35) - 2 \equiv 20 - 2 \equiv 18 \mod 37$$

Thus, the sum of points $(15, 2)$ and $(25, 29)$ on the Elliptic Curve $E_{37}(2, 3)$ is the point $(35, 18)$.

**Grading:** 1 pts set up lambda value, 4 pts get $10^{-1}$ mod 37, 1 pt lambda, 2 pts $x_R$, 2 pts $y_R$
12) (8 pts) For the purposes of this question, assume that the probability any arbitrary person’s birthday is a particular month is exactly $\frac{1}{12}$, for each month. If 4 people are chosen at random, what is the probability that 2 of the people are born in one month and the other 2 people are born in a different month? Express your answer as a fraction in lowest terms.

The sample space is $12^4$, since each of the 4 people in the sample can have any one of 12 birthdays. Now, we must count how many of these items in the sample space are where 2 birthdays are in one month and two birthdays in a different month.

We can pick the months in 12 times 11 ways. (12 for the first unique month, 11 for the second unique month).

Then, we want to count the number of molds of the birthdays, AABB. There are 6 such molds: AABB, ABAB, ABBA, BBAA, BABA, and BAAB.

But, because 2 of the frequencies are the same, the molds over count. For example, the mold AABB counts Dec, Dec, Nov, Nov AND Nov, Nov, Dec, Dec. But then, the mold BBAA also counts both of these two. So, we must divide our answer by 2.

Our final answer is $\frac{12 \times 11 \times 6}{12^4 \times 2} = \frac{11}{12^2 \times 2^2} = \frac{11}{144} = \frac{11}{576}$

Grading: 2 pts sample space, 2 pts perm 2 months, 1 pt molds, 2 pts double count, 1 pt fraction in lowest terms

13) (1 pt) Who was the lead singer of Huey Lewis and the News? **Huey Lewis (give to all)**