1) (16 pts) Consider a portion of a single DES round where the last 24 bits of input (expressed in HEX) to S boxes $S_5$, $S_6$, $S_7$, $S_8$ is $9A\text{B}6\text{E}$. What are the 16 bits of output from those 4 S-boxes? Express your result in binary. (Note: Partial credit on this question will be limited for obvious reasons, so double check your answers.)

- $S_5(100110) = 11 \ (1011)$
- $S_6(101011) = 5 \ (0101)$
- $S_7(011001) = 2 \ (0010)$
- $S_8(011110) = 7 \ (0111)$

Grading: 4 pts binary conversion written nicely, 1 pt row, 1 pt col, 1 pt result. If result is in HEX and not binary but correct, give 12/16.

1011010100100111

2) (10 pts) Consider an IP matrix for a block cipher with a block size of 16 bits shown below. What is the smallest positive integer $k$ for which, if we apply IP to an input $k$ successive times, the result will be the original input? (For example, if for a block size of four IP = [2 1 4 3], then if we apply IP twice, we have $1 \rightarrow 2 \rightarrow 1$, $2 \rightarrow 1 \rightarrow 2$, $3 \rightarrow 4 \rightarrow 3$, and $4 \rightarrow 3 \rightarrow 4$, so $k = 2$ for this case.) (Note: The value for $k$ for this query is too large to brute force, so don’t try to do so.)

Here are our cycles:

- $1 \rightarrow 11 \rightarrow 5 \rightarrow 3 \rightarrow 10 \rightarrow 1 \ (\text{length 5})$
- $2 \rightarrow 8 \rightarrow 15 \rightarrow 2 \ (\text{length 3})$
- $4 \rightarrow 9 \rightarrow 4 \ (\text{length 2})$
- $6 \rightarrow 16 \rightarrow 13 \rightarrow 7 \rightarrow 12 \rightarrow 14 \rightarrow 6 \ (\text{length 6})$

Thus, we want the smallest integer that is a multiple of 5, 3, 2 and 6. In other words, we want the LCM of these numbers, which is 30.

Grading: 2 pts for listing 1 cycle, 6 pts for listing all cycles, 4 pts for LCM, 0 for any approach without a reasonable justification.

30
3) (18 pts) If the state matrix is the following right before the Mix Columns step of AES, what is the entry in row 1, column 3, right after the Mix Columns step? *(Note: Please be very, very, very careful that you work out the correct entry. If you find the entry of row 3, column 1, you will earn a maximum of 5 points out of 20.)*

\[
\begin{pmatrix}
3A & 95 & CD & 12 \\
2C & 7E & 96 & 4F \\
97 & F9 & A0 & 62 \\
B2 & C8 & 7E & D3 \\
\end{pmatrix}
\]

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 entry in row 1, col 3 is \(02 \times CD + 03 \times 96 + 01 \times A0 + 01 \times 7E\).

\[
02 \times CD = 1100 \ 11010 = 1001 \ 1010 \oplus 0001 \ 1011 \\
1000 \ 0001 = 81
\]

\[
03 \times 96 = 02 \times 96 \oplus 01 \times 96 = 1001 \ 0110 \ 0 + 1010 \ 0110 = 1001 \ 0110 \oplus 1010 \ 0001 = A1
\]

\[
01 \times A0 = A0
\]

\[
01 \times 7E = 7E
\]

Use the Hex XOR chart to simplify: \((81 \oplus A1) \oplus (A0 \oplus 7E) = 20 \oplus DE = FE\)

**Grading:** 4 pts to write out appropriate sum of products, 4 pts for x 2, 6 pts for x 3, 4 pts for final XOR.
4) (16 pts) Consider an RSA system with \(p = 13\), \(q = 19\), and \(e = 175\). Determine \(n\), \(\phi(n)\) and \(d\). Put a box around your answer for each of the three values request. Note that you must express both \(\phi(n)\) and \(d\) with \(0 < d, \phi(n) < n\).

\[n = pq = 13 \times 19 = 247,\] \(\phi(n) = (p - 1)(q - 1) = 12 \times 18 = 216\)

\[d = 175^{-1} \mod 216\]

\[
\begin{align*}
216 &= 1 \times 175 + 41 \\
175 &= 4 \times 41 + 11 \\
41 &= 3 \times 11 + 8 \\
11 &= 1 \times 8 + 3 \\
8 &= 2 \times 3 + 2 \\
3 &= 1 \times 2 + 1 \\

3 - 2 &= 1 \\
3 - (8 - 2 \times 3) &= 1 \\
3 - 8 + 2 \times 3 &= 1 \\
3 \times 3 - 1 \times 8 &= 1 \\
3 \times (11 - 8) - 1 \times 8 &= 1 \\
3 \times 11 - 3 \times 8 - 1 \times 8 &= 1 \\
3 \times 11 - 4 \times 8 &= 1 \\
3 \times 11 - 4(41 - 3 \times 11) &= 1 \\
3 \times 11 - 4 \times 41 + 12 \times 11 &= 1 \\
15 \times 11 - 4 \times 41 &= 1 \\
15(175 - 4 \times 41) - 4 \times 41 &= 1 \\
15 \times 175 - 60 \times 41 - 4 \times 41 &= 1 \\
15 \times 175 - 64 \times 41 &= 1 \\
15 \times 175 - 64(216 - 175) &= 1 \\
15 \times 175 - 64 \times 216 + 64 \times 175 &= 1 \\
79 \times 175 - 64 \times 216 &= 1 \\

\text{Taking this equation mod 216, we find:} \\
79 \times 175 &\equiv 1 \pmod{216} \\
\text{It follows that } d = 79. \\
\end{align*}
\]

Grading: 4 pts Euclidean, 11 pts Extended, 1 pt extract result
5) (12 pts) Alice's Public El Gamal keys are \( q = 37 \), and \( \alpha = 2 \). Alice's secret key is \( X_A = 9 \). Bob wants to send the message \( M = 15 \) to Alice. Create two different ordered pairs \((C_1, C_2)\) that Bob could send Alice to send her the message. Put a different box around both ordered pairs. (Note: before you do anything else you must calculate Alice's public key, \( Y_A \).)

Alice’s public key is \( Y_A = 2^9 \mod 37 = 512 \mod 37 = 31 \).

**Key Set #1:** Randomly select \( k = 2 \), so \( C_1 = 2^2 = 4 \).
   Then calculate \((Y_A)^k = 31^2 \equiv (-6)^2 \equiv 36 \mod 37 \).
   Finally, \( C_2 = 15 \times 36 \equiv 15 \times (-1) \equiv -15 \equiv 22 \mod 37 \).
   So, one valid encryption is \((4, 22)\).

**Key Set #2:** Randomly select \( k = 4 \), so \( C_1 = 2^4 = 16 \).
   Then calculate \((Y_A)^k = 31^4 \equiv (-6)^4 \equiv (36)^2 \equiv (-1)^2 \equiv 1 \mod 37 \).
   Finally, \( C_2 = 15 \times 1 \equiv 15 \mod 37 \).
   So, one valid encryption is \((16, 15)\).

Here are all of the possible ordered pairs (generated by the posted python program elgamal.py):

\((2, 21), (4, 22), (8, 16), (16, 15), (32, 21), (27, 22), (17, 16), (34, 15), (31, 21), (25, 22), (13, 16), (26, 15), (15, 21), (30, 22), (23, 16), (9, 15), (18, 21), (36, 22), (35, 16), (33, 15), (29, 21), (21, 22), (5, 16), (10, 15), (20, 21), (3, 22), (6, 16), (12, 15), (24, 21), (11, 22), (22, 16), (7, 15), (14, 21), (28, 22), (19, 16), (1, 15)\)

**Grading:** 6 pts per pair, within pair 1 pt list \( k \), 1 pt list \( C_1 \), 2 pts calculate \( K \), 2 pts calculate \( C_2 \).

6) (8 pts) Use Euler's Theorem to calculate the remainder when \( 17^{1010} \) is divided by 735.

\[
735 = 5 \times 147 = 5 \times 7 \times 21 = 5 \times 7 \times 7 \times 3 = 3 \times 5 \times 7^2 \\
\varphi(735) = \varphi(3) \times \varphi(5) \times \varphi(7^2) = 2 \times 4 \times (7^2 - 7) = 8 \times 42 = 336
\]

Note that 336 \times 3 = 1008.

\[
17^{1010} = 17^{336(3) + 2} = (17^{336})^3 17^2 = 1^3 17^2 = 289 \mod 735.
\]

Thus, the desired remainder is \( \boxed{289} \).

**Grading:** 4 pts phi calculation 2 pts break down 1010, 2 pts final answer
7) (10 pts) The Miller-Rabin Primality Test is shown below.

Input: \( n > 2 \), an odd integer to be tested for primality;
\( k \), a parameter that determines the accuracy of the test
Output: composite if \( n \) is composite, otherwise probably prime

write \( n - 1 \) as \( 2^s \cdot d \) with \( d \) odd by factoring powers of 2 from \( n - 1 \)
LOOP: repeat \( k \) times:
   pick \( a \) randomly in the range \([2, n - 1]\)
   \( x \leftarrow a^d \mod n \)
   if \( x = 1 \) or \( x = n - 1 \) then do next LOOP
   for \( r = 1 \ldots s - 1 \)
     \( x \leftarrow x^2 \mod n \)
     if \( x = 1 \) then return composite
     if \( x = n - 1 \) then do next LOOP
   return composite
return probably prime

Consider running the test for \( n = 57 \), \( k = 1 \) and \( a = 2 \). Show each value of \( x \) calculated while the algorithm executes and the return value of the algorithm.

\( n - 1 = 57 - 1 = 56 = 2^3 \times 7 \), so \( s = 3 \), \( d = 7 \).
Initial \( x = a^d = 2^7 = 128 \equiv 14 \mod 57 \)
\( r = 1: \ x = 14^2 = 196 \equiv 25 \mod 57 \)
\( r = 2: \ x = 25^2 = 625 \equiv 55 \mod 57 \)
So, the three calculated values of \( x \) are 14, 25 and 55. Since none of these are \( x = 1 \) or \( x = n - 1 \), composite will be returned.

Grading: 2 pts for \( s \), 1 pt for \( d \), 3 pts for first \( x \) value, 2 pts for second \( x \) value, 2 pts for last \( x \) value.
8) (8 pts) Consider the AES Key Schedule where we have
\[ w[28] = 32769810 \]
\[ w[31] = abdefc54 \]
expressed in hex. Calculate \(w[32]\), filling in each intermediate step shown below:

First we do the RotWord to get defc54ab.
The SubWord on these 4 bytes yields 1db02062.
\[ Rcon[32/4] = Rcon[8] = 80000000 \]
\[ 1db02062 \text{ XOR } 80000000 = 9db02062. \]

Finally our last XOR is

\[
\begin{align*}
32769810 \\
9db02062 \\
\hline
afc6b872
\end{align*}
\]

**Grading:** 2 pts RotWord, 2 pts SubWord, 1 pt Rcon, 1 pt XOR, 2 pts final result

9) (2 pts) With what galaxy does the popular candy Milky Way share its name? **Milky Way**

**Grading:** 2 pts give to all