1) What is the prime factorization of 175?

\[175 = 5^2 \times 7\]

2) Prove that 2 is a generator mod 13.

\[
\begin{align*}
2^1 &\equiv 2 \mod 13 & 2^7 &\equiv 11 \mod 13 \\
2^2 &\equiv 4 \mod 13 & 2^8 &\equiv 9 \mod 13 \\
2^3 &\equiv 8 \mod 13 & 2^9 &\equiv 5 \mod 13 \\
2^4 &\equiv 3 \mod 13 & 2^{10} &\equiv 10 \mod 13 \\
2^5 &\equiv 6 \mod 13 & 2^{11} &\equiv 7 \mod 13 \\
2^6 &\equiv 12 \mod 13 & 2^{12} &\equiv 1 \mod 13
\end{align*}
\]

This shows that the smallest positive integer for which \(2^k \equiv 1 \mod 13\) is 12, this 2 is a generator.

3) What is the remainder when \(37^{129}\) is divided by 80?

\[
\varphi(80) = \varphi(5(16)) = \varphi(5) \varphi(16) = (5 - 1)(16 - 8) = 32. \ (4 \text{ pts})
\]

Thus, \(37^{32} \equiv 1 \mod 80\).

\[
\begin{align*}
37^{129} &\equiv (37^{32})^4(37) \mod 80 \ (3 \text{ pts}) \\
&\equiv (1)^4(37) \mod 80 \\
&\equiv 37 \mod 80 \ (1 \text{ pt})
\end{align*}
\]
4) In an RSA system, $n = 391$ and $e = 137$, what is $d$?

We need to solve for $d$ in the equation $137d = 1 \mod 352$.

So, we must run the Extended Euclidean Algorithm:

\[
352 = 2 \times 137 + 78 \\
137 = 1 \times 78 + 59 \\
78 = 1 \times 59 + 19 \\
59 = 3 \times 19 + 2 \\
19 = 9 \times 2 + 1 \\
2 = 2 \times 1
\]

Now, we have:

\[
19 - 9 \times 2 = 1 \\
19 - 9 \times (59 - 3 \times 19) = 1 \\
19 - 9 \times 59 + 27 \times 19 = 1 \\
28 \times 19 - 9 \times 59 = 1 \\
28 \times 78 - 9 \times 59 = 1 \\
28 \times 78 - 37 \times 19 + 37 \times 59 = 1 \\
28 \times 78 - 37 \times 137 + 37 \times 78 = 1 \\
65 \times 78 - 37 \times 137 = 1 \\
65 \times (352 - 2 \times 137) - 37 \times 137 = 1 \\
65 \times 352 - 130 \times 137 - 37 \times 137 = 1 \\
65 \times 352 - 167 \times 137 = 1
\]

Thus $d = -167 = (352 - 167) = 185 \mod 352$.

$d = 185$

5) In a Diffie-Hellman Key Exchange, Alice and Bob agree upon the public keys $p = 17$ and $g = 3$. Alice picks the secret key $a = 4$ and Bob picks the secret key $b = 7$. What value does Alice send Bob? What value does Bob send Alice? What is their shared secret key?

Alice sends Bob $3^4 \mod 17 = 81 \mod 17 = 13$.
Bob sends Alice $3^7 \mod 17 = (27)(27)(3) \mod 17 = (10)(10)(3) \mod 17 = 11$.

Their shared key (calculated by Alice) is $11^4 \mod 17 = (121)(121) \mod 17 = 4 \mod 17$, since $121 = 2 \mod 17$. 
6) If the input into all of the S-boxes in DES in hex is AB1 845 E72 865, what is the output, in hex?

Input to each S-box:  S1  S2  S3  S4  S5  S6  S7  S8
Input written in binary: 101010 110001 100001 000101 111001 110010 100001 100101

Row and columns of S1 – row 2, col 5  6
Row and columns of S2 – row 3, col 8  B
Row and columns of S3 – row 3, col 0  1
Row and columns of S4 – row 1, col 2  B
Row and columns of S5 – row 3, col 12  A
Row and columns of S6 – row 2, col 9  0
Row and columns of S7 – row 3, col 0  6
Row and columns of S8 – row 3, col 2  E

Answer: 6B1BA6E

7) Using multiplication in the field defined in AES (GF 2^8 with polynomial x^8 + x^4 + x^3 + x + 1), what is the result (in hex) of multiplying the byte 03 by the byte B7?

03°B7 = 01°B7 + 02°B7 = (1011 0111) + (1 0110 1110)
Adding, we get

\[
\begin{array}{c}
1011 0111 \\
1 0110 1110 \\
\hline
1 1101 1001
\end{array}
\]

Reducing mod the AES polynomial we get

\[
\begin{array}{c}
1101 1001 \\
+ 0001 1011 \\
\hline
1100 0010
\end{array}
\]

In Hex, this is C2.

8) Let the round 3 key in AES be 01234567 89ABCDEF FEDCBA98 76543210 in hex. What will the first four bytes of the round 4 key be, represented in hex?

\[
\begin{align*}
temp & = 76543210 \\
RotWord(temp) & = 54321076 \\
SubWord(RotWord(temp)) & = 2023CA38 \\
Rcon[4] & = 04000000 \\
temp after XOR & = 2423CA38 \\
w[i-4] & = 01234567 \\
temp XOR w[i-4] & = 25008F5F
\end{align*}
\]