**Exam #2 Review Question Solutions**

1) What is the prime factorization of 175?

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

2) Prove that 2 is a generator mod 13.

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

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?

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

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) Factor 20701 using the Fermat Factoring method.

\[
\sqrt{20701} \approx 143.9, \text{ so}
\]

\[
\begin{align*}
144^2 - 20701 &= 35 \text{ (not a perfect square)} \ (3 \text{ pts}) \\
145^2 - 20701 &= 324 = 18^2. \quad (3 \text{ pts})
\end{align*}
\]

It follows that:

\[
\begin{align*}
145^2 - 18^2 &= 20701 \ (1 \text{ pt}) \\
(145 - 18)(145 + 18) &= 20701
\end{align*}
\]

Thus, 20701 factored is 127x163. (1 pt)
5) 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:

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

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

\( d = 185 \)

6) 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 \( 121 = 2 \mod 17 \).
7) If the input into all of the S-boxes in DES in hex is AB1 845 E72 865, what is the output, in hex?

Answer: 6B1BA6E

8) 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?

$$03^\circ B7 = 01^\circ B7 + 02^\circ B7 = (1011 0111) + (1 0110 1110)$$

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.

9) 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?

| 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 |