You may use a pocket calculator that does not have internet access. You can work on the problems in any order you like. Show your work! All problems carry the same weight. Calculation steps and explanation for statements made are a crucial part of a solution. Partial credit will be given sparingly – rather complete one problem than start two only partially.

1) You are participating in a Diffie-Hellman key exchange for $p = 101$ and $g = 2$. You have chosen the secret exponent $a = 8$.
   a) What number should you send to your partner?
   b) Your partner sends you the number 99. What is the secret key shared by your partner and you? Explain the calculations you are doing.

   a) $2^8 = 256 \equiv 54 \pmod{101}$

   b) $99 \equiv \text{mod} p$. Calculate ($99^2 \equiv -2 \pmod{101}$)

   $99^2 \equiv 4 \pmod{101}$

   $99^4 \equiv (99^2)^2 \equiv 16 \pmod{101}$

   $99^8 \equiv (99^4)^2 \equiv 16^2 \equiv 256 \equiv 54$
2) Find a number \( a \) that satisfies the following three congruences:

\[
\begin{align*}
    a & \equiv 0 \pmod{3} \\
    a & \equiv 4 \pmod{7} \\
    a & \equiv 2 \pmod{11}
\end{align*}
\]

First two equations: \( 1 = \gcd(3, 7) = 1 \cdot 7 - 2 \cdot 3 \)

Assume \( c_2 = c_1 + y \cdot 3 = 0 + y \cdot 3 \equiv 4 \pmod{7} \)

\( \Rightarrow y \cdot 3 \equiv 4 \pmod{7} \)

\( \Rightarrow y \equiv -8 \equiv 6 \pmod{7} \)

So \( c_2 = 2 \cdot 6 = 12 \)

Next step: \( 2 \cdot 2 = 21, 1 = \gcd(21, 11) = 21 - 1 \cdot 21 \)

Assume \( c_3 = 18 + y \cdot 21 \equiv 2 \pmod{11} \)

\( \Rightarrow y \cdot 21 \equiv 2 - 18 \equiv -16 \equiv 5 \pmod{11} \)

\( \Rightarrow y \equiv 5 \pmod{11} \)

\( 2 \cdot 1 = -1 \)

\( \Rightarrow c_3 = 18 + 5 \cdot 21 = [123] \)
3) Let $p = 701$, then $p$ is prime, $p - 1 = 2^3 5^2 7$ and 2 is a primitive root modulo $p$.

a) Determine all $e$ such that $\text{OrderMod}_p(2^e) = 5$. (Note that this question asks for the values of $e$, not for those of $2^e$. You also may keep values for $e$ in product form and do not need to multiply these products out.)

b) For how many $e$ will you have that $\text{OrderMod}_p(2^e) = 25$? (You do not need to write down all values of $e$, the problem just asks for a count!) Justify your answer.

\[ \frac{p - 1}{5 \cdot 28} = \frac{p - 1}{140} = 5. \] This order $\text{Mod}_p(2^{140}) = 5$

For the other exponents, simply take exponents coprime to 5; i.e., $e = 140, e = 2 \cdot 140, e = 3 \cdot 140, e = 4 \cdot 140$

b) There are $\phi(25) = 4 \cdot 5 = 20$ such elements.
4) Let \( p = 307 \), then \( g = 5 \) is a primitive root modulo \( p \) and \( p - 1 = 17 \cdot 18 \). Determine an exponent \( e \) such that \( g^e \equiv 100 \pmod{p} \).

**Hints:** You might find the following facts useful: \( \text{OrderMod}_p(100) = 153 = 9 \cdot 17 \) and \( 100 = 81 \cdot 168 \) with \( \text{OrderMod}_p(81) = 17 \) and \( \text{OrderMod}_p(168) = 9 \). Furthermore \( 5^{18} \equiv 81 \pmod{p} \) and \( 5^{17} \equiv 139 \pmod{p} \), so the main calculation is a discrete logarithm of 168 for base 139 mod \( p \) where \( \text{OrderMod}_p(139) = 18 \), a Babystep-Giantstep calculation with step width \( \lceil \sqrt{18} + 1 \rceil = 5 \). As a help, you are given the following list of values of \( 139^{-1} \cdot 168 \pmod{p} \) for \( i = 0..4: \) [168, 306, 53, 261, 289]. and \( 139^{-1} \equiv 254 \pmod{p} \).

(Make sure that your final answer is a number \( e \) such that \( g^e \equiv 100 \pmod{p} \).)
5) Show that there is no \( n \) such that \( n = 5 \cdot \varphi(n) \). (Hint: Write \( n = 5^a \cdot b \) with \( \gcd(5, b) = 1 \). Show that you would need \( \varphi(5^a) = 5^a/5 = 5^{a-1} \) or \( \varphi(b) = b/5 \). Then show that neither of these two conditions is possible.) Remember that

\[
\varphi\left( \prod p_i^{e_i} \right) = \prod (p_i - 1) \cdot p_i^{e_i - 1}.
\]

If \( n = 5^a \cdot b \) with \( \gcd(5^a, b) = 1 \), then

\[
\varphi(n) = \varphi(5^a) \cdot \varphi(b).
\]

Thus if \( n = 5 \cdot \varphi(n) \)

\[ n = 5^a \cdot b = 5 \cdot \varphi(5^a) \cdot \varphi(b). \]

Thus \( n = 5^{a-1} \cdot b = \varphi(5^a) \cdot \varphi(b) \).

But \( \varphi(5^a) = 5^{a-1} \cdot 4 \), so \( b = 4 \cdot \varphi(b) \). Therefore

\[
b = \prod p_i^{e_i-1} \implies \varphi(b) = \prod (p_i - 1) \cdot p_i^{e_i-1} \implies \frac{b}{\varphi(b)} = \prod \frac{p_i}{p_i-1}.
\]

To get \( \frac{b}{\varphi(b)} = 4 \), this can only happen from \( p_i = 2 \)

but then \( \frac{p_i}{p_i-1} = 2 \neq 4 \), contradicting.