1) (8 pts) What is \( \varphi(2^53^45^6) \)? Express your answer in prime factorized form.

\[
\varphi(2^53^45^6) = (2^5 - 2^4)(3^4 - 3^3)(5^6 - 5^5) = 2^4(2-1)3^3(5-1) = 2^4 3^3 2^2 = 2^7 3^3 5^2.
\]

Grading: 3 pts for initial formula application (any form), 3 pts to do some algebra with it, 2 pts for the answer being in the proper form (prime factorized)

2) (12 pts) Using Fermat’s Theorem, determine \( 1234^{69941} \mod 6359 \). (Note: 6359 is a prime number.

Using Fermat’s Theorem, we know that \( 1234^{6358} \equiv 1 \pmod{6359} \).

\[
1234^{69941} = 1234^{11(6358) + 3} = (1234^{6358})^{11} \times 1234^3 \equiv 1^{11} \times 1234^3 \equiv 2763 \pmod{6359}
\]

Note: \( 1234^3 \) was entered in the calculator and the mod was determined by dividing by 6359, subtracting the integral part and multiplying the fractional part by 6359.

Grading: 4 pts for stating what's true based on Fermat's Theorem
3 pts for the appropriate exponential breakdown
2 pts for subbing 1 where appropriate
3 pts for working out remaining term
3) (12 pts) Using Euler’s Theorem, determine $309^{147003} \mod 42875$.

Note: On some of the exams, this question was $309^{147003} \mod 42875$. For this corrected version, we would do the following:

$42875 = 25 \times 1715 = 25 \times 5 \times 343 = 5^3 7^3$.

$\phi(42875) = \phi(5^3 7^3) = (5^3 - 5^2)(7^3 - 7^2) = 100 \times 294 = 29400$

Thus, using Euler’s Theorem, we have $309^{29400} \equiv 1 \pmod{42875}$, since gcd(309, 42875) = 1.

$309^{147003} \equiv 309^{5(29400) + 3} \equiv (309^{29400})^5 \times 309^3 \equiv 1^5 \times 29503629 \equiv 5629 \pmod{42875}$

Note: We used the calculator to determine $309^3$ and performed the mod by dividing on the calculator, subtracting out the integral part and multiplying the fractional part by 42875.

**Grading for this version:**
6 pts for stating what's true based on Euler's Theorem
3 pts for the appropriate exponential breakdown
1 pt for subbing 1 where appropriate
2 pts for working out remaining term

On the main version of the exam, the question was $308^{147003} \mod 42875$.

Notice that if we check the divisors of 308, we find 308 = $2^2 \times 7 \times 11$.
We also find that 42875 = $5^3 \times 7^3$. Thus, gcd(308, 42875) = 7 and Euler's formula doesn't apply.

If anyone noticed this, they automatically got full credit. Alternatively, if they did the following work:

$308^{147003} \equiv 308^{5(29400) + 3} \equiv (308^{29400})^5 \times 308^3 \equiv 1^5 \times 29218112 \equiv 20237 \pmod{42875}$

Then full credit was given as well. **Note:** it turns out that $308^{147003} \equiv 20237 \pmod{42875}$. Though I am not 100% sure, I think it's possible in cases like these to prove that utilizing Euler’s Theorem in this fashion yields the correct answer so long as the exponent isn't an exact multiple of phi(n).

**Grading:**
12 pts if it's noted that gcd(308, 42875) = 7.

OR

6 pts for stating what's true based on Euler's Theorem if gcd(308, 42875) were equal to 1
3 pts for the appropriate exponential breakdown
1 pt for subbing 1 where appropriate
2 pts for working out remaining term
4) (10 pts) In the Diffie-Hellman Key Exchange, let the public keys be \( p = 23 \) and \( g = 5 \). Let Alice’s private key be 9 and Bob’s private key be 13. Using both Fermat’s Theorem (to reduce your work) and your knowledge of the Diffie-Hellman Key Exchange, determine the shared key that Alice and Bob will exchange. (First, express the shared key as \( g^x \mod p \) for some integer \( x \). Then, use Fermat’s to reduce this to a smaller calculation. Then calculate this result via calculator.)

Note that via Fermat’s Theorem, \( 5^{22} \equiv 1 \) (mod 23).

The shared key is \( (5^9)^{13} = 5^{117} \equiv 5^{110+7} = 5^{110} \times 5^7 \equiv (5^{22})^5 \times 5^7 \equiv 1^5 \times 78125 \equiv 17 \) (mod 23).

Thus, the shared key is 17.

Grading: 5 pts for getting that shared key is \( 5^{117} \), 3 pts for breaking it down to \( 5^{110}5^7 \), 2 pts for solving.

Alternatively, 4 pts to calculate \( 5^9 \) properly, another 4 pts to take that the 13\(^{th}\) power and 2 final points to reduce to the right answer. (The order can also be flipped to do \( 5^{13} \) first and then take that to the 9\(^{th}\) power.)
5) (12 pts) In an RSA scheme, \( p = 31, q = 37 \) and \( e = 203 \). What is \( d \)?

\[
\begin{align*}
n &= pq = 31 \times 37 = 1147 \\
\phi(n) &= (p - 1)(q - 1) = 30 \times 36 = 1080 \\
d &= e^{-1} \pmod{\phi(n)} \\
d &= 203^{-1} \pmod{1080}
\end{align*}
\]

Run the Extended Euclidean Algorithm to find \( d \):

\[
\begin{align*}
1080 &= 5 \times 203 + 65 \\
203 &= 3 \times 65 + 8 \\
65 &= 8 \times 8 + 1
\end{align*}
\]

\[
\begin{align*}
65 - 8 \times 8 &= 1 \\
65 - 8(203 - 3 \times 65) &= 1 \\
65 - 8 \times 203 + 24 \times 65 &= 1 \\
25 \times 65 - 8 \times 203 &= 1 \\
25(1080 - 5 \times 203) - 8 \times 203 &= 1 \\
25 \times 1080 - 125 \times 203 - 8 \times 203 &= 1 \\
25 \times 1080 - 133 \times 203 &= 1
\end{align*}
\]

Take this equation mod 1080 to yield

\[
\begin{align*}
0 - 133 \times 203 &\equiv 1 \pmod{1080} \\
203^{-1} &\equiv -133 \equiv 947 \pmod{1080}
\end{align*}
\]

\[
d = 947.
\]

**Grading:** 3 pts for finding \( \phi(n) \), 1 pt for stating which inverse must be found, 2 pts Extended Euclidean, 4 pts Extended Euclidean, 2 pts to extract out answer (-1 if answer is -133 for not mapping back to \([0, 1079]\)).

6) (8 pts) How many generators does the prime \( p = 67 \) have?

As previously proved on homework assignment #5, a prime \( p \) has \( \varphi(p-1) \) generators. Solving, we find:

\[
\varphi(66) = \varphi(2 \times 3 \times 11) = (2 - 1)(3 - 1)(11 - 1) = 20
\]

Thus, 67 has 20 generators.

**Grading:** 4 pts for stating fact of the # of generators for a prime \( p \). 4 pts for solving for \( \varphi(66) \). If the answer is 66, automatically give 3 out of 8 points.
7) (20 pts) Alice's Public El Gamal keys are $q = 37$, $\alpha = 22$ and $Y_A = 19$. Alice's secret key $X_A = 29$. Give one possible ciphertext $(C_1, C_2)$ that corresponds to the plaintext $M = 11$, using these public keys. Then, use the ciphertexts and show the work that Alice would do to decrypt the message to recover it.

To make life easy, let's choose $k = 2$:

$$K = 19^2 \equiv 361 \equiv 28 \pmod{37}$$
$$C_1 = 22^2 \equiv 484 \equiv 3 \pmod{37}$$
$$C_2 = K \cdot M = 28 \cdot 11 \equiv 308 \equiv 12 \pmod{37}$$

So, one valid ciphertext is $(3, 12)$.

Now, when Alice receives $(3, 12)$, she does the following:

She calculates $3^{29} \pmod{37}$. Since 3 is small, we can short-circuit this calculation a bit:

$$3^{29} = 3^{10 \cdot 3^9} = (59049)(59049)(19683) \equiv 34 \cdot 34 \cdot 36 \equiv (-3)(-3)(-1) \equiv -9 \equiv 28 \pmod{37}$$

Then, she finds $28^{-1} \pmod{37}$:

$$37 = 1 \times 28 + 9$$
$$28 = 3 \times 9 + 1$$

$$28 - 3 \times 9 = 1$$
$$28 - 3(37 - 28) = 1$$
$$28 - 3 \times 37 + 3 \times 28 = 1$$
$$4 \times 28 - 3 \times 37 = 1$$

Take this equation mod 37 to get

$$4 \times 28 \equiv 1 \pmod{37}$$

Thus, $28^{-1} \equiv 4 \pmod{37}$

To recover the message now, just calculate $K^{-1} \cdot C_2 \pmod{p}$ which is

$$4 \cdot 12 = 48 \equiv 11 \pmod{37}$$

**Grading:** 1 pt to state some choice for $k$ that is valid.

- 2 pts for calculating $K$,
- 2 pts for calculating $C_1$,
- 2 pts for calculating $C_2$.
- 6 pts for Alice's calculation of $\alpha^{X_A}$.
- 6 pts for Euclidean and Extended Euclidean
- 1 pt for extracting $M$ back.
8) (15 pts) The discrete log problem is as follows: Given a prime number $p$, a generator $g$, and a result $y$, determine the value of $x$ such that $g^x \equiv y \pmod{p}$. For large values of $p$, this problem is too difficult to solve quickly. However, for small values of $p$, and a given $g$, we can simply make a look up table such that table[$y$] = $x$, for all possible values of $y$ from 1 to $p$-1, inclusive. Complete the function below so that it returns an array storing these discrete log values. (For example, if $p = 11$ and $g = 6$, we see that $6^1 \equiv 6$, $6^2 \equiv 3 \pmod{11}$, $6^3 \equiv 7 \pmod{11}$, $6^4 \equiv 9 \pmod{11}$, $6^5 \equiv 10 \pmod{11}$, $6^6 \equiv 5 \pmod{11}$, $6^7 \equiv 8 \pmod{11}$, $6^8 \equiv 4 \pmod{11}$, $6^9 \equiv 2 \pmod{11}$, and $6^{10} \equiv 1 \pmod{11}$. Thus, for $p = 11$, $g = 6$, your code should return the array storing $[0, 10, 9, 2, 8, 6, 1, 3, 7, 4, 5]$. Note that we default a value of 0 in index 0, even though this isn’t a possible result of an exponentiation.)

```c
int* discLogTable(int p, int g) {
    int* result = calloc(p, sizeof(int));
    int cur = g;
    for (int i=1; i<=p-1; i++) {
        result[cur] = i;
        cur = (cur*g)%p;
    }
    return result;
}
```

Grading: init 1 pt, for loop 3 pts, Storing result 5 pts, Updating cur, 5 pts, return 1 pt

Automatic deductions:
-5 for using the pow function
-3 for overflow with multiplication
-3 for flipping the array (doing the inverse of what was asked)

9) (3 pts) What letter appears in the middle of the Circle K logo? K (give to all)