Name: _____

Directions: Show all work. No credit for answers without work.

1. [**5 points**] Two security companies offer encryption products. Both companies have been in business for 10 years and charge similar fees. Company A uses proprietary cryptosystem developed internally by their most senior engineers, and the details are a closely guarded secret. Company B publishes the full details of its cryptosystem, with security depending on a secret key randomly generated by each customer. Both companies act in good faith and consider maintaining their customer's security their highest priority. As the IT professional at your company, which security company would you recommend, and why?

2. [**10 points**] Let $a = -78$ and $b = 10$. Find integers q and r such that $a = qb + r$ and $0 \leq r \leq b - 1$.

3. [**2 parts, 5 points each**] Compute $89 \cdot (-51) \pmod{46}$ in **two different ways**. Your answer should be an integer in the set $\{0, \ldots, 45\}$.

   (a) Way 1:

   (b) Way 2:

4. [**10 points**] Let $a = 2911$, let $b = 2419$, and let $d = \gcd(a, b)$. Use the Extended Euclidean Algorithm to compute d and find integers u and v such that $d = ua + vb$.

5. [**5 points**] List all numbers in $\mathbb{Z}_{15}$ that have multiplicative inverses.

6. [**10 points**] Find the multiplicative inverse of 217 modulo 673.

7. [**10 points**] Using the fast power algorithm, compute $(83)^{85}$ (mod 10000).

8. Computation modulo 18.

    (a) [**10 points**] Give the multiplication table for the unit group $\mathbb{Z}_{18}^*$.

    (b) [**5 points**] Use the table to solve for x in $5x \equiv 11$ (mod 18).

9. [**10 points**] Let a, b, and c be integers. Prove that if $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

10. [**5 points**] What special property does $\mathbb{Z}_m$ have when m is prime that it otherwise lacks?

11. [**2 parts, 5 points each**] Orders.

    (a) Compute $\mathrm{ord}_2(167872)$.

    (b) Either prove the following or find a counter-example: $\mathrm{ord}_2(n) = 8$ if and only if $256 \mid n$.