Name: Solutions

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?

Recommend Company B. An open cryptosystem will be exposed to scrutiny by many independent experts and, if it withstands such attacks over time, then we gain more confidence in its security. A few people at Company A, even if experts, are no substitute for careful review by the larger crypto community.

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

$-78 = (-8)(10) + 2$

So $\boxed{q = -8}$ and $\boxed{r = 2}$.

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:

$(90-1)(50+1) = 4500 + 90 - 50 - 1$

$89 \cdot (-51) \equiv -4539$

$\equiv -4539 + 4600$

$\equiv 61$

$\equiv 61 - 46$

$\equiv \boxed{15} \pmod{46}$

(b) Way 2:

$89 \equiv 43 \equiv -3 \pmod{46}$

$-51 \equiv -5 \pmod{46}$

$89 \cdot (-51) \equiv (-3) \cdot (-5)$

$\equiv \boxed{15} \pmod{46}$

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 $d = ua + vb$.

$$\begin{array}{r} \overset{8\,0\,1}{2911} \\ 2419 \\ \hline 492 \end{array}$$

$4(500-8)$

$2000-32$

1968

$$\begin{array}{r} 2419 \\ -1968 \\ \hline 451 \end{array}$$

$$2911 = (1)(2419) + 492$$
$$2419 = (4)(492) + 451$$
$$492 = (1)(451) + 41$$
$$451 = (11)(41) + 0$$

So $d = 41$

$$\begin{aligned} 41 &= 492 - (1)(451) = 492 - (1)[2419 - (4)(492)] \\ &= (5)(492) - (1)(2419) \\ &= (5)[2911 - (1)(2419)] - (1)(2419) \\ &= (5)(2911) - (6)(2419) \end{aligned}$$

$$\boxed{d = 41 \quad u = 5 \quad v = -6}$$

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

All numbers in $\{0, \dots, 14\}$ relatively prime to 15:

$$\boxed{1, 2, 4, 7, 8, 11, 13, 14}$$

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

$$\begin{array}{r} 673 \\ 651 \\ \hline 22 \end{array}$$

$$673 = (3)(217) + 22$$
$$217 = (9)(22) + 19$$
$$22 = (1)(19) + 3$$
$$19 = (6)(3) + 1$$

$$\begin{aligned} 1 &= 19 - (6)(3) \\ &= 19 - (6)[22 - (1)(19)] \\ &= (7)(19) - (6)(22) \\ &= (7)[217 - (9)(22)] - (6)(22) \\ &= (7)(217) - (69)(22) \\ &= (7)(217) - (69)[673 - (3)(217)] \\ &= (214)(217) - (69)(673) \end{aligned}$$

So the inverse is $\boxed{214}$.

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

$83^1 \equiv 83$

$83^2 \equiv 6400 + 480 + 9 \equiv 6889$

$(83)^4 \equiv (83)^2 \cdot (83)^2 \equiv (6889)^2 \equiv 8321$

$(83)^8 \equiv (8321)^2 \equiv 9041$

$(83)^{16} \equiv (9041)^2 \equiv 9681$

$(83)^{32} \equiv (9681)^2 \equiv 1761$

$(83)^{64} \equiv (1761)^2 \equiv 1121$

$85 = 64 + 16 + 4 + 1$

$$(83)^{85} \equiv (83)^{64} \cdot (83)^{16} \cdot (83)^4 \cdot (83)$$

$$\equiv (1121) \cdot (9681) \cdot (8321) \cdot (83)$$

$$\equiv (2401) \cdot (8321) \cdot (83)$$

$$\equiv (8721)(83)$$

$$\equiv \boxed{3843}$$

8. Computation modulo 18.

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

$\mathbb{Z}_{18}^*$	1	5	7	$\equiv(-7)$ 11	$\equiv(-5)$ 13	$17 \equiv (-1)$
1	1	5	7	11	13	17
5	5	7	17	1	11	13
7	7	17	13	5	1	11
$(-7) \equiv 11$	11	1	5	13	17	7
$(-5) \equiv 13$	13	11	1	17	7	5
$(-1) \equiv 17$	17	13	11	7	5	1

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

From the table, we see $5 \cdot 13 \equiv 11 \pmod{18}$

so $x = \boxed{13}$.

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

Since $\gcd(a,b)=1$, by the Extended Euclidean Algorithm, we have

$$1 = ua + vb$$

for some $u, v \in \mathbb{Z}$. Multiplying both sides by c gives

$$c = uac + vbc$$

Since $a \mid bc$, we have $bc = ka$ for some $k \in \mathbb{Z}$. Therefore

$$c = uac + vbc = uac + vka = (uc + vk)a$$

and it follows that $a \mid c$. ∎

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

When m is prime, $\mathbb{Z}_m$ is a field, meaning that all non-zero elements have multiplicative inverses, and therefore division is generally possible.

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

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

$$167872 = 2^6 \cdot \underbrace{2623}_{\text{odd}}$$

So $\text{ord}_2(167872) = \boxed{6}$.

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

This is $\boxed{\text{false}}$. For example, let $n = 2^9 = 512$. We have

$\text{ord}_2(n) = 9$ but still $256 \mid n$ since $n = (2)(256)$.