Name: Key

**Show your work. Answers without work earn reduced credit.**

1. [**3 points**] Write $\gcd(4959, 273)$ as a linear combination of 4959 and 273.

$(4959, 273)$: $4959 = 18 \cdot 273 + 45$

$(273, 45)$: $273 = 6 \cdot 45 + 3$

$(45, 3)$: $45 = 15 \cdot 3 + 0$

$(3, 0)$: $\gcd = 3$.

$3 = 273 - 6 \cdot 45$

$45 = 4959 - 18 \cdot 273$

$3 = 273 - 6 \cdot (4959 - 18 \cdot 273)$

$\boxed{3 = 109 \cdot 273 - 6 \cdot 4959}$

2. [**2 points**] How many of the integers in $\{1, 2, 3, \ldots, 99\}$ are relatively prime to 100?

$100 = 2^2 \cdot 5^2$

$\varphi(100) = 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5}$

$= \boxed{40}$

3. [**2 points**] The prime factorization of $32,830$ is given by $32,830 = 2 \cdot 5 \cdot 7^2 \cdot 67$. Find $\varphi(32,830)$.

$\varphi(32830) = 2 \cdot 5 \cdot 7^2 \cdot 67 \cdot \frac{1}{2} \cdot \frac{4}{5} \cdot \frac{6}{7} \cdot \frac{66}{67}$

after canceling $= 7 \cdot 4 \cdot 6 \cdot 66 = \boxed{11,088}$

4. [**3 parts, 1 point each**] In the RSA algorithm, let $p = 5$ and $q = 17$. Then $n = 85$ and $\varphi(n) = 4 \cdot 16 = 64$. For the encryption key, pick $e = 5$.

(a) Use the Euclidean algorithm to find the decryption key $d$.

$(64,5)$: $64 = 12 \cdot 5 + 4$ | $1 = 5 - 1 \cdot 4$

$(5,4)$: $5 = 1 \cdot 4 + 1$ | $4 = 64 - 12 \cdot 5$

$(4,1)$: $4 = 4 \cdot 1 + 0$ | $1 = 5 - 1(64 - 12 \cdot 5)$

$(1,0)$: gcd = 1. | $1 = 13 \cdot 5 - 1 \cdot 64$

$\boxed{d = 13}$

(b) Encode $T = 42$ using the public key $(n, e)$.

$U = (42)^5 \bmod 85$. Modulo 85:

$(42)^2 \equiv 1764 \equiv 64$

$(42)^4 \equiv 64 \cdot 64 \equiv 4096 \equiv 16$

$(42)^5 \equiv 16 \cdot 42 \equiv 672 \equiv \boxed{77}$

(c) Decode your answer to part (b) to retrieve the plain-text message 42.

Need: $(77)^{13} \bmod 85$.

$(77)^2 \equiv 5929 \equiv 64$

$(77)^4 \equiv 4096 \equiv 16$

$(77)^8 \equiv 256 \equiv 1$

$(77)^{12} \equiv (77)^8 \cdot (77)^4 \equiv 1 \cdot 16 \equiv 16$

$(77)^{13} \equiv 77 \cdot 16$

$\equiv 1232$

$\equiv \boxed{42}$ ✓