Name: Solutions

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

1. **[3 points]** Solve for x in $x^{53} \equiv 48 \pmod{67}$.

We seek $(53)^{-1}$ in the exponent modulus $\phi(67)$. Since 67 is prime, $\phi(67) = 67-1 = 66$.

So: EEA(53, 66):

$66 = (1)(53) + 13$

$53 = (4)(13) + 1$

$1 = 53 + (-4)(13)$

$= 53 + (-4)[66 + (-1)(53)]$

$= (5)(53) + (-4)(66)$.

So $(53)^{-1} = 5$ in $\mathbb{Z}_{66}$. So $x^{53} \equiv 48 \pmod{67}$

$x^{53 \cdot 5} \equiv (48)^5 \pmod{67}$

$x \equiv (48)^5 \pmod{67}$.

Fast Power in $\mathbb{Z}_{67}$

$(48)^2 = 26$

$(48)^4 = (26)^2 = 6$

$(48)^5 = (48)^{4+1} = (48)^4 \cdot 48$

$= 6 \cdot 48 = 288 = 20$.

So $\boxed{x \equiv 20} \pmod{67}$.

Check:

$(20)^2 = 65 = -2$

$(20)^4 = (-2)^2 = 4$

$(20)^8 = 4^2 = 16$

$(20)^{16} = 55$

$(20)^{32} = 10$

$(20)^{53} = 20^{32+16+4+1} = 10 \cdot 55 \cdot 4 \cdot 20 = 48$ ✓.

2. **[2 points]** Suppose that $N = pq$ for distinct primes p and q. Given $N = 560401$ and $N' = (p-1)(q-1) = 558900$, find p and q using the efficient method from class.

$p + q = N - N' + 1 = 1502$.

$(x-p)(x-q) = x^2 - (p+q)x + pq = x^2 - 1502x + 560401$.

$$x = \frac{1502 \pm \sqrt{(1502)^2 - 4(560401)}}{2} = \frac{1502 \pm \sqrt{14400}}{2} = \frac{1502 \pm 120}{2} = 751 \pm 60$$

So $x = 811$ or $x = 691$. Check $N \stackrel{?}{=} \boxed{691 \cdot 811} = 560401$ ✓.

3. Alice generates an RSA key with $p = 37$, $q = 23$, and she picks public exponent $e = 7$.

   (a) **[3 points]** What is Alice's public key? What is her private key?

$N = pq = (37)(23) = 851$, $\quad N' = (p-1)(q-1) = 36 \cdot 22 = 792$.

$ed \equiv 1 \pmod{N'}$:

EEA(N', e):

$792 = (113)(7) + 1$

$1 = (792) + (-113)(7)$

So $d \equiv -113 \equiv 679 \pmod{N'}$.

So public key: $(N, e) = (851, 7)$

private key: $(N, d) = (851, 679)$.

   (b) **[2 points]** Bob wishes to encrypt and send the message $m = 80$ to Alice. What should he send?

$C \equiv m^e \pmod{N}$

$\equiv (80)^7 \pmod{851}$

Fast Power:

$(80)^2 = 443$

$(80)^4 = (443)^2 = 519$

$C = (80)^7 = (80)^{4+2+1} = (80)^4 \cdot (80)^2 \cdot (80)^1$

$= (519) \cdot (443) \cdot 80$

$= 18,393,360$

$= \boxed{697}$