Name: Solutions

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

1. [**3 points**] Solve for x in $x^{19} \equiv 21 \pmod{79}$.

79: prime

$N' = p-1 = 78$

Find $(19)^{-1} \bmod 78$:

$78 = (4)(19) + 2$

$\underline{\underline{19}} = (9)(2) + 1$

$1 = 19 - (9)(2)$

$= 19 - (9)[78 - (4)(19)]$

$= (37)(19) - (9)(78)$

So $(19)^{-1} \equiv 37 \pmod{78}$.

$x^{19} \equiv 21 \pmod{79}$

$(x^{19})^{37} \equiv (21)^{37} \pmod{79}$

$x^{kN'+1} \equiv (21)^{37} \pmod{79}$

$x \equiv (21)^{37} \pmod{79}$

Fast Power:

$(21)^2 = 46$

$(21)^4 = (46)^2 = 62$

$(21)^8 = (62)^2 = 52$

$(21)^{16} = (52)^2 = 18$

$(21)^{32} = (18)^2 = 8$

$37 = 32 + 4 + 1$

$(21)^{37} = (21)^{32} \cdot (21)^4 \cdot (21) \pmod{79}$

$= 8 \cdot 62 \cdot 21 \pmod{79}$

$= 10416 \pmod{79}$

$= \boxed{67} \pmod{79}$

2. [**2 points**] Suppose that $N = pq$ for distinct primes p and q. Given $N = 167653$ and $N' = (p-1)(q-1) = 166828$, find p and q using the efficient method from class.

$N' = pq - (p+q) + 1$

$p + q = pq - N' + 1$

$= N - N' + 1$

$= 167653 - 166828 + 1$

$= 826$

$p = 826 - q$

$N = 167653 = pq = (826 - q)q$

$q^2 - 826q + 167653 = 0$

$q = \dfrac{826 \pm \sqrt{(826)^2 - 4(167653)}}{2}$

$= \dfrac{826 \pm \sqrt{11664}}{2}$

$= \dfrac{826 \pm 108}{2} = 413 \pm 54$

$p = 413 - 54 = \boxed{359}$

$q = 413 + 54 = \boxed{467}$

3. Alice generates an RSA key with $p = 13$, $q = 19$, and she picks public exponent $e = 5$.

(a) [**2 points**] What is Alice's public key? What is her private key?

$N = pq = 247$

$N' = (p-1)(q-1) = 12 \cdot 18 = 216$

Find 5^{-1} mod N':

$216 = (43)(5) + 1$

$1 = (216) - (43)(5)$

So $5^{-1} \equiv -43 \equiv 173$ mod 216

Alice's public key: $(N, e) = \boxed{(247, 5)}$

Alice's private key: $(N, d) = \boxed{(247, 173)}$

(b) [**2 points**] Bob wishes to encrypt and send the message $m = 189$ to Alice. What should he send?

$C = m^e \pmod N$

$= (189)^5 \pmod{247}$

$(189)^2 = 153$

$(189)^4 = (153)^2 = 191$

$c = (189)^5 = (189)^4 \cdot (189) \pmod{247}$

$= 191 \cdot 189$

$= 36099$

$= \boxed{37}$

(c) [**1 point**] After many years of using $e = 5$, Alice wishes to change her public exponent. What would you recommend to Alice?

Recommend that Alice generate fresh primes p and q and a new modulus $N = pq$ along with a new exponent. Then choose an exponent e such that $\gcd(e, N') = 1$, where $N' = (p-1)(q-1)$. If an adversary has the same message m encrypted with $e = 5$ and e' using the same modulus, it is usually easy to decrypt m.