

Name: _____

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

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

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.

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?

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