

Directions: Solve the following problems. All written work must be your own. See the course syllabus for detailed rules.

1. Alice's public key uses modulus

$$N = 22476\ 96411\ 17831.$$

Of course, $N = pq$ for some secret primes p and q . Somehow, Eve is able to compute

$$(p - 2)(q - 3) = 22476\ 95651\ 24622.$$

Help Eve use this information to factor N . *Hint:* try to adapt the technique for factoring N given $(p - 1)(q - 1)$ to this new case.

2. In RSA, Alice picks two large random primes p and q and computes $N = pq = 36\ 07160\ 97653$. Unfortunately, she generates two private/public exponents, where $e_1 = 3245$ and $e_2 = 2^{16} + 1 = 65537$. What's worse, Bob sends Alice the same message m encrypted with both e_1 and e_2 , sending both $c_1 = m^{e_1} = 21\ 71952\ 87254$ and $c_2 = m^{e_2} = 9\ 65647\ 24994$. Help Eve find m efficiently (so, no factoring N or solving a discrete root problem).
3. Bob uses the RSA Signature Scheme. He picks $p = 29101$ and $q = 12713$, and computes $N = pq = 369961013$ and $N' = 369919200$. He picks $e = 328253$ as his public exponent and publishes (N, e) as his public key.
 - (a) Find Bob's private exponent d .
 - (b) Bob wishes to sign the message $m = 95342$. What is the signature s ?
 - (c) Alice publishes her RSA public key $(N_A, e_A) = (598680829, 55213)$. Bob receives three message/signature pairs (m_i, s_i) claiming to be from Alice: $(12, 456268725)$, $(100, 581415411)$, and $(25326, 200402993)$. Which of these messages (if any) are actually from Alice?
4. [JJJ 3.13(a)] Here, we prove that 561 is a Carmichael number. That is, 561 is composite and yet it has no Fermat witnesses. Note that $561 = 3 \cdot 11 \cdot 17$.
 - (a) Prove that if $a \in \mathbb{Z}_{561}^*$, then a satisfies the system

$$a^{560} \equiv 1 \pmod{3}$$

$$a^{560} \equiv 1 \pmod{11}$$

$$a^{560} \equiv 1 \pmod{17}$$

- (b) Prove that 561 has no Fermat witnesses.
5. For each pair (n, a) below, determine whether a is (i) a Fermat witness for n ; and (ii) a Miller–Rabin witness for n .
 - (a) $n = 21$ and $a = 8$
 - (b) $n = 1279$ and $a = 1091$
 - (c) $n = 1722971$ and $a = 1711330$
 - (d) $n = 1722971$ and $a = 2$
 - (e) $n = 8533633$ and $a = 3862185$
 - (f) $n = 8533633$ and $a = 5393220$