

1 RSA Practice

Consider the following RSA schemes and solve for asked variables.

- (a) Assume for an RSA scheme we pick 2 primes $p = 5$ and $q = 11$ with encryption key $e = 9$, what is the decryption key d ? Calculate the exact value.
- (b) If the receiver gets 4, what was the original message?
- (c) Encode your answer from part (b) to check its correctness.

2 RSA Practice

Bob would like to receive encrypted messages from Alice via RSA.

- (a) Bob chooses $p = 7$ and $q = 11$. His public key is (N, e) . What is N ?
- (b) What number is e relatively prime to?
- (c) e need not be prime itself, but what is the smallest prime number e can be? Use this value for e in all subsequent computations.
- (d) What is $\gcd(e, (p-1)(q-1))$?
- (e) What is the decryption exponent d ?

- (f) Now imagine that Alice wants to send Bob the message 30. She applies her encryption function E to 30. What is her encrypted message?
- (g) Bob receives the encrypted message, and applies his decryption function D to it. What is D applied to the received message?

3 RSA Lite

Woody misunderstood how to use RSA. So he selected prime $P = 101$ and encryption exponent $e = 67$, and encrypted his message m to get $35 = m^e \pmod{P}$. Unfortunately he forgot his original message m and only stored the encrypted value 35. But Carla thinks she can figure out how to recover m from $35 = m^e \pmod{P}$, with knowledge only of P and e . Is she right? Can you help her figure out the message m ? Show all your work.

4 RSA with Three Primes

Show how you can modify the RSA encryption method to work with three primes instead of two primes (i.e. $N = pqr$ where p, q, r are all prime), and prove the scheme you come up with works in the sense that $D(E(x)) \equiv x \pmod{N}$.