EECS 70 Discrete Mathematics and Probability Theory
Fall 2014 Anant Sahai

Discussion 6M-S

1. RSA Practice

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

1. Bob chooses $p = 7$ and $q = 11$. His public key is (N, e).

2. What is N?

3. What number is e relatively prime to?

4. 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.

5. What is $gcd(e, (p-1)(q-1))$?

6. What is the decryption exponent d?

7. Now imagine that Alice wants to send Bob the message 30. She applies her encryption function E to 30. What is her encrypted message?

8. Bob receives the encrypted message, and applies his decryption function D to it. What is $D(x)$?

2. True or False

1. Bob has to publish his key (N, e) to receive encrypted messages from Alice.

2. Eve needs to know Bob's key d in order to send him encrypted messages.

3. The security of RSA relies on the computational intractability of determining x from $y = x^e \mod N$, even when y, e, and N are all known.

4. $E(x) = x^e \mod N$ is a bijection on numbers $\mod N$.