

APR 10.

CS/ECE/MATH 435, HOMEWORK 7, DUE ~~APR 10~~.

1. Suppose Alice's RSA public key is $N = 91, e = 7$.
 - (a) Compute her decryption exponent.
 - (b) Alice wants to sign the message $x = 21$. Calculate her signature.
 - (c) Bob receives the message-signature pair $(x, s) = (54, 89)$. Is the signature authentic?

2. (a) Show that if $p = 11, q = 5, x = 3$, and $k = 3$, then $(x^k \pmod{p}) \pmod{q}$ and $(x^k \pmod{q}) \pmod{p}$ are different.
 - (b) Alice and Bob want to exchange encrypted signed messages. Alice's public key is (N, e) and private decryption exponent d , whereas Bob's public key is (N', e') and private decryption exponent d' . Alice wants to send x to Bob. She signs a message encrypted by Bob's public key so sends $y = (x^{e'} \pmod{N'})^d \pmod{N}$ to Bob. To read the message and verify the signature, Bob computes $z = y^e \pmod{N} = x^{e'} \pmod{N'}$ and then computes $z^{d'} \pmod{N'} = x^{e'd'} \pmod{N'} = x$. Will this work? Explain why or why not.