HOMEWORK 7, DUE NOV 2.

Be sure to include explanations. You will not get full credit if you give only the final answer.

1. Suppose Alice's RSA public key is $N = 91, e = 7$.
(a) Compute her decryption exponent d.
(b) Alice wants to sign the message $x = 21$. Calculate the corresponding signature.
(c) Bob receives the message-signature pair $(x, s) = (54, 89)$. How does he check whether this is a valid signed message from Alice? Carry out this check. Is it a valid signed message?

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 a message x to Bob. She first 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. [Consider the correctness of the equalities claimed above.]

Typeset by $\mathcal{AMS}$-TEX