MATH 295A/395A: CRYPTOGRAPHY
HOMEWORK #9

Problems for all

Problem 1. Alice publishes her RSA public key: modulus $n = 2038667$ and exponent $e = 103$.

(a) Bob wants to send Alice the message $m = 892383$. What ciphertext does Bob send to Alice?
(b) Alice knows that her modulus factors into a product of two primes, one of which is $p = 1301$. Find a decryption exponent d for Alice.
(c) Alice receives the ciphertext $c = 317730$ from Bob. Decrypt the message.

Problem 2. Alice uses the RSA public key modulus $n = pq = 172205490419$. Through espionage, Eve discovers that $(p-1)(q-1) = 172204660344$. Determine p, q.

Problem 3. Suppose Bob leaks his private decryption key d in RSA. Rather than generating a new modulus n, he decides to generate a new public encryption key e and a new private decryption key d. Is this safe?

Problem 4. Bob uses RSA to receive a single ciphertext b corresponding to the message a. Suppose that Eve can trick Bob into decrypting a single chosen ciphertext c which is not equal to b. Show how Eve can recover a.

Problem 5. Suppose that Alice and Bob have the same RSA modulus n and suppose that their encryption exponents e and f are relatively prime. Charles wants to send the message a to Alice and Bob, so he encrypts to get $b = a^e \pmod{n}$ and $c = a^f \pmod{n}$. Show how Eve can find a if she intercepts b and c.

Additional problems for 395A

Problem 6. A *Carmichael number* is an integer $n > 1$ that is *not* prime with the property that for all $a \in \mathbb{Z}$, $a^n \equiv a \pmod{n}$. Prove that $561, 1105, 1729$ are Carmichael numbers. *[Hint: Look at the proof of $a^{ed} \equiv a \pmod{n}$, $n = pq$, in RSA. You may factor these numbers!]*

Problem 7. In this exercise, we show why small encryption exponents should not be used in RSA. We take $e = 3$. Three users with pairwise relatively prime moduli n_1, n_2, n_3 all use the encryption exponent $e = 3$. Suppose that the same message $a \in \mathbb{Z}_{>0}$ with $a < \min(n_1, n_2, n_3)$ is sent to each of them and Eve intercepts the ciphertexts $b_i \equiv a^3 \pmod{n_i}$.

(a) Show that $0 \le a^3 < n_1 n_2 n_3$.
(b) Show how to use the Chinese remainder theorem to find $a^3 \in \mathbb{Z}$ and therefore $a \in \mathbb{Z}$ (without factoring).
(c) Suppose that

$$n_1 = 2469247531693, \quad n_2 = 11111502225583, \quad n_3 = 44444222221411$$

and

$$b_1 = 359335245251, \quad b_2 = 10436363975495, \quad b_3 = 5135984059593.$$

Compute a.

Date: Due Wednesday, 5 November 2008.