MATH 295A/395A: CRYPTOGRAPHY
HOMEWORK #10

Problems for all

Problem 1. Bob chooses the RSA modulus

$$n = 106952478872918644452128409915498921623837587061712268002137333458806512673436 87$$

and

$$e = 185730878059908293557942613452699667102216138436831817754987098752055482543977 9$$

and because he is short for time chooses a small decryption exponent. Alice sends the secret message

$$b = 587690344299547613971164024486198201454760869407647377722691345230694980729 4092$$

to Bob by converting her codeword of seven letters into ASCII bytes, interpreting this as the binary expansion of an integer, and encrypting it using RSA. Decrypt the message and recover the plaintext codeword.

Problem 2. In the RSA public-key encryption scheme, each user has a public key e and a private key d. Suppose Bob leaks his private key. Rather than generating a new modulus, he decides to generate a new public and a new private key. Is this safe?

Problem 3. A *Carmichael number* is a composite integer $n > 1$ such that $a^n \equiv a \pmod{n}$ for all $a \in \mathbb{Z}$. Show that in practice Carmichael numbers are easy to factor into primes. Illustrate the method on the Carmichael number $n = 1729$.

Problem 4. Let n be an RSA modulus, e_1 an encryption exponent, d_1 the corresponding decryption exponent, and e_2 a second encryption exponent. Given the data n, e_1, d_1, e_2, exhibit a fast and certain algorithm that determines the corresponding decryption exponent d_2 which does *not* using random choices, the factorization of n, or exponentiation modulo n. Illustrate your algorithm on $n = 119$, $e_1 = 23$, $d_1 = 23$, $e_2 = 7$ and $n = 119$, $e_1 = 23$, $d_1 = 23$, $e_2 = 11$.

Problem 5. For the following integers either provide a witness for the compositeness of n or conclude that n is probably prime by providing 5 numbers that are not witnesses.

(a) $n = 1009$.
(b) $n = 2009$.

Problem 6. Using big-O notation, estimate the number of bit operations required to perform the witness test on a number n enough times so that, if n passes all of the tests, it has less than a 10^{-m} chance of being composite.

Date: Due Friday, November 5, 2010.