Dartmouth College Department of Mathematics
Math 75 Cryptography
Spring 2020

Problem Set # 6 (upload to Canvas by Friday, May 15, 11:30 am EDT)

Problems:

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.

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

3. 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, and showing her the resulting plaintext. Show how Eve can recover a.

4. 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.

5. 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!]*