Dartmouth College Department of Mathematics
Math 148 Introduction to Public Key Cryptography and Elliptic Curves
Spring 2025

Problem Set # 3 (due by Canvas upload by the end of Friday 9 May)

Problems:

1. (HPS 2nd Edition 3.7) Alice publishes her RSA public key: modulus $N = 2038667$ and encryption 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. (HPS 2nd Edition 3.10.a) Suppose that Eve has a magic box that creates decryption exponents for (N, e) for a fixed modulus N and for a large number of different encryption exponents e. Explain how Eve can use her magic box to factor N.

3. (HPS 2nd Edition 3.11) Here is an example of a public key system that was proposed at a cryptography conference. It was designed to be more efficient than RSA. Alice chooses two large primes p and q and she publishes $N = pq$. It is assumed that N is hard to factor. Alice chooses three random numbers $g, r_1, r_2 \pmod N$ and computes

$$g_1 \equiv g^{r_1(p-1)} \pmod N \quad \text{and} \quad g_2 \equiv g^{r_2(q-1)} \pmod N.$$

Her public key is the triple (N, g_1, g_1) and her private key is the pair of primes (p, q). Now Bob wants to send the message m to Alice, where m is a number modulo N. He chooses two random integers s_1 and s_2 modulo N and computes

$$c_1 \equiv m g_1^{s_1} \pmod N \quad \text{and} \quad c_2 \equiv m g_2^{s_2} \pmod N.$$

Bob sends the ciphertext (c_1, c_2) to Alice. Decryption is extremely fast and easy. Alice uses the Chinese Remainder Theorem to solve the pair of congruences

$$x \equiv c_1 \pmod p \quad \text{and} \quad x \equiv c_2 \pmod q.$$

(a) Prove that Alice's solution x is equal to Bob's plaintext m.
(b) Explain why this cryptosystem is not secure.

4. (HPS 2nd Edition 3.14) We claimed in class that 561 is a Carmichael number, but we didn't check that $a^{561} \equiv a \pmod{561}$ for every value of a.

(a) The number 561 factors as $3 \cdot 11 \cdot 17$. First use Fermat's little theorem to prove that $a^{561} \equiv a \pmod 3$, $a^{561} \equiv a \pmod{11}$, and $a^{561} \equiv a \pmod{17}$ for every value of a. Then explain why these congruences imply that $a^{561} \equiv a \pmod{561}$ for every value of a.
(b) Prove that a Carmichael number must be odd.
(c) Prove that a Carmichael number must be a product of *distinct* primes.