Dartmouth College Department of Mathematics
**Math 75 Cryptography**
Spring 2022

Problem Set # 6 (upload to Canvas by Friday, May 13, 10:10 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 back at the proof of $a^{ed} \equiv a \pmod{n}$, $n = pq$, in RSA. You may factor these numbers!]*

**6.** Pollard's $p-1$ factorizing algorithm uses the following idea. Let $p$ be a prime divisor of an integer $n$ and let $d$ be a divisor of $p-1$. Suppose that an integer $a$ has multiplicative order $d$ in $\mathbb{Z}/p\mathbb{Z}$, i.e., that $a^d \equiv 1 \bmod p$. If $a^d \not\equiv 1 \bmod n$ then $\gcd(a^d - 1, n)$ is a proper divisor of $n$. This can be turned into an algorithm: choose a random $1 < a < n$ and inductively set $a_1 = a$ and $a_i \equiv a_{i-1}^i \bmod n$ for $i > 1$, and check whether $\gcd(a_i - 1, n) \neq 1, n$. If you ever get $\gcd(a_i - 1, n) = n$, then halt, choose a different $a$, and start over.

(a) Find a nontrivial factor of $n = 47371$ using this algorithm, starting with $a = 2$. Show what happens at each step.

(b) Show that $a_i \equiv a^{i!} \bmod n$ for all $i \geq 1$.

(c) If $p - 1 | N$ for some integer $N$, show that $p | a^N - 1$ for any integer $a$ relatively prime to $n$.

(d) Explain why this algorithm runs quickly if there is a reasonably small $i \leq 1$ such that $p - 1 | i!$, and deduce that in this case, $p - 1$ must be quite smooth.

(e) A prime number $p$ is called a **safe prime** if $p-1 = 2p'$ for a prime number $p'$. Explain why the existence of Pollard's $p-1$ algorithm implies that for the modulus $n = pq$ in RSA, both $p$ and $q$ should be chosen to be safe primes.

A prime number $p'$ such that $2p'+1$ is also prime is called a **Sophie Germain prime**. So $p$ is safe if and only if $(p-1)/2$ is a Sophie Germain prime. Sophie Germain was a late 18th/early 19th century French mathematician who, due to prejudices of the time, was not allowed to attend lectures at the École Polytechnique in Paris. So she obtained the lecture notes and started corresponding with famous mathematicians Lagrance and Gauss about her ideas under a male pseudonym. She did fantastic research work in number theory, most famously, she presented a strategy to prove Fermat's Last Theorem for prime exponents related to Sophie Germain primes, which is how her primes were named. She also did important work in philosophy and in the theory of elasticity, for which she was the first woman to win a prize from the Paris Academy of Sciences, in 1816. You can read more about her history and mathematics in Wikipedia.