MATH 75: Cryptography **Spring 2022**

PSET 6 — May 13, 2022

Prof. Asher Auel ***Student: Amittai Siavava***

Credit Statement

I worked on these problems alone, with reference to class notes and the following books:

(a) ***The Code Book*** by **Simon Singh**.
(b) ***Cryptography*** by **Simon Rubinsen-Salzedo**

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?

Bob sends:

$$\begin{aligned} m^e \pmod{n} &= 892383^{103} \pmod{2038667} \\ &= 455638 \end{aligned}$$

(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.

We know that $d \cdot e \equiv 1 \pmod{\textbf{lcm}\,(p-1,\ q-1)}$ Alice finds d by solving the equation:

$$\begin{aligned} n &= 2038667 \\ p &= 1301 \\ q = \frac{n}{p} &= 1567 \\ \textbf{lcm}\,(1300,\ 1566) &= 1017900 \\ &\Downarrow \\ d \cdot e &\equiv 1 \pmod{1017900} \\ 103 \cdot e &\equiv 1 \pmod{1017900} \end{aligned}$$

We can use the extended euclidean algorithm to find $103^{-1} \pmod{1017900}$

$$\begin{aligned} 1017900 &\equiv 9882 \cdot 103 + 54 \\ 103 &\equiv 1 \cdot 54 + 49 \\ 54 &\equiv 1 \cdot 49 + 5 \\ 49 &\equiv 9 \cdot 5 + 4 \\ 5 &\equiv 1 \cdot 4 + 1 \end{aligned}$$

$$\begin{aligned} 1 &\equiv 5 - 4 \\ 1 &\equiv 5 - (49 - 9 \cdot 5) \\ 1 &\equiv 10 \cdot 5 - 49 \\ 1 &\equiv 10(54 - 49) - 49 \\ 1 &\equiv 10 \cdot 54 - 11 \cdot 49 \\ 1 &\equiv 10 \cdot 54 - 11(103 - 54) \\ 1 &\equiv 21 \cdot 54 - 11 \cdot 103 \\ 1 &\equiv 21(1017900 - 9882 \cdot 103) - 11 \cdot 103 \\ 1 &\equiv -(21 \cdot 9882 + 11) \cdot 103 \\ 1 &\equiv -207533 \cdot 103 \\ 1 &\equiv 810367 \cdot 103 \\ 103^{-1} &\equiv 810367 \pmod{1017900} \\ &\Downarrow \\ d &= 810367 \end{aligned}$$

(c) Alice receives the ciphertext $c = 317730$ from Bob. Decrypt the message.

Alice decrypts as follows:

$$\begin{aligned} p &= c^d \pmod{n} \\ &= 317730^{810367} \pmod{2038667} \\ &= 514407 \end{aligned}$$

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

$$\begin{aligned} (p-1)(q-1) &= 172204660344 \\ p(q-1) - 1(q-1) &= 172204660344 \\ p \cdot q - p - q + 1 &= 172204660344 \\ \because\ p \cdot q &= 172205490419 \\ \therefore\ p + q - 1 &= 172205490419 - 172204660344 \\ p + q &= 830076 \\ q &= 830076 - p \\ p \cdot q = p\,(830076 - p) &= 830076p - p^2 \\ p^2 - 830076p + 172205490419 &= 0 \\ p &= 422183 \\ q &= 407893 \end{aligned}$$

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.

Eve can trick Bob into decrypting the ciphertext $c = 2^e b$.
Let x be the decryption of this ciphertext, $2^e b$.
Then:

$$\begin{aligned} 2^e b &= x^e \pmod{n} \\ b &\equiv (x \cdot 2^{-1})^e \pmod{n} \\ \because\ b &\equiv a^e \pmod{n} \\ \therefore\ a^e &\equiv (x \cdot 2^{-1})^e \pmod{n} \\ a &\equiv x \cdot 2^{-1} \pmod{n} \end{aligned}$$

To recover a, Eve can simply find $2^{-1} \pmod{n}$ and multiply that by the decryption she got from Bob.

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.

Since e and f are relatively prime, Eve can find x, y such that $e \cdot x + f \cdot y \equiv 1 \pmod{n}$.
Then:

$$b^x + c^y = a^{e \cdot x + f \cdot y} \equiv a^1 \pmod{n}$$

Thus, if Eve Eve intercepts both b and c, and finds the corresponding values for x and y such that $e \cdot x + f \cdot y \equiv 1 \pmod{n}$, she can recover a as the equivalent of $b^x + c^y \pmod{n}$.

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!]*

Any *Carmichael numbers* n must have the properties:

(a) n is a square-free composite.
(b) For every prime divisor $p \mid n$, $p - 1 \mid n - 1$.

```
ghci> primeFactors 561
[3,11,17]

ghci> primeFactors 1105
[5,13,17]

ghci> primeFactors 1729
[7,13,19]
```

Checking the divisors, we can see that:

(1) $(2|560) \wedge (10|560) \wedge (16|560)$
(2) $(4|1104) \wedge (12|1104) \wedge (16|1104)$
(3) $(6|1728) \wedge (12|1728) \wedge (18|1728)$

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.

I wrote a simple implementation of this algorithm.

```
pollard' :: Integer -> IO (Integer, Integer)
pollard' n = iter n 2 1
  where
    iter n a i = do
      let g = gcd (a - 1) n
      printf "n = %5d   a_%d = %5d   gcd = %5d" n i a g

      if g /= 1 && g /= n then
        return (g, n div g)
      else if g == n then
        iter n (randomInt 2 n) 1
      else
        iter n ((a ^ i) mod n) (i + 1)
```

Results:

```
ghci> pollard' 47371
n = 47371       a_1 =     2     gcd =     1
n = 47371       a_2 =     4     gcd =     1
n = 47371       a_3 =    64     gcd =     1
n = 47371       a_4 =  7882     gcd =     1
n = 47371       a_5 = 34800     gcd =     1
n = 47371       a_6 = 31941     gcd =     1
n = 47371       a_7 = 15368     gcd =   127
(127,373)
```

Thus, we can see that 127 and 373 are non-trivial factors of 47371.

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

We can prove this by induction on i:
For the base case, we have the definition of a_1:

$$a_1 \equiv a \equiv a^{1!} \bmod n$$

In the inductive step, we have the definition that, for all $1 < i < n$, $a_i \equiv a_{i-1}^i \bmod n$.
Thus, we have the base-case that $a_1 = a^{1!} \pmod n$, and, for every next i,
$a_i \equiv a_{i-1}^i \pmod n = a^{i\cdot(i-1)!} \equiv a^{i!} \pmod n$.

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

$$p-1|N \Rightarrow \exists k \in Z_+ \ni N = k \cdot (p-1)$$
$$a^N = a^{k\cdot(p-1)} \equiv \left(a^{p-1}\right)^k \pmod{p}$$
$$\therefore\ a^N = a^{p-1} \equiv 1 \pmod{p} \text{ per Fermat's Little Theorem}$$
$$\therefore\ a^N = \left(a^{p-1}\right)^k \equiv 1^k \equiv 1 \pmod{p}$$
$$\therefore\ a^N - 1 \equiv 0 \pmod{p}$$
$$\therefore\ p \mid (a^N - 1)$$

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

The algorithm works because of Fermat's Little Theorem and the property it induces—that if $(p-1)|i!$ then $p|(a^{i!}-1)$ for any a.

(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.