Day 19 – RSA

RSA

- The RSA system was invented in 1977 by Ron Rivest, Adi Shamir, and Leon Adleman.
- It is based on the assumption that it is easy to multiply two prime numbers but difficult to factor a product of two primes into its prime components.

The steps of RSA:

1. (key creation, private) Bob chooses secret primes $p$ and $q$. Computes the modulus $N = pq$.

2. Bob also chooses the encryption exponent $e$ that is a positive integer coprime to $\varphi(N) = (p-1)(q-1)$.

3. (public) Bob publishes $N$ and $e$.

4. (private, encryption) Alice chooses the plaintext $m$ and uses Bob’s public key to encrypt it. That is, she computes the ciphertext
   \[ c \equiv m^e \pmod{N}. \]

5. (public) Alice sends ciphertext $c$ to Bob. (Eve can see this.)

6. (private, decryption) Bob decrypts Alice’s message by computing first
   \[ d \equiv e^{-1} \pmod{\varphi(N)} \equiv e^{-1} \pmod{(p-1)(q-1)} \]
   and then
   \[ m \equiv c^d \pmod{N}. \]
RSA steps

Sender

Public

Enemy

Receiver

N → N, e

2 primes p, q

N = p · q (mod)

\( \varphi(N) = (p-1) \cdot (q-1) \)

pick an encryption factor e

\( e > 0, \text{ integer, } e \text{ coprime to } \varphi(N) \)

calculate decryption factor d.

\( d = e^{-1} \mod \varphi(N) \)

plaintext: m

\( c = m^e \mod N \)

encrypt

\( c \)

To decrypt:

\( m = c^d \mod N \)

decrypt func.
**Why does it work? - What can Eve do?**

Even if she knows \(N, c\) and \(e\) and tries to get \(d\), she needs to solve the equation

\[
d \cdot e \equiv 1 \pmod{\varphi(N)}.
\]

But getting \(\varphi(N)\) from \(N\) alone is equivalent to factoring \(N\).

**Can enemy find \(\varphi(N)\) based on \(N\)?**

\[
\varphi(N) = (p - 1)(q - 1) = p + q - p - q + 1 = N - (p + q) + 1
\]

To get \(\varphi(N)\), you need to know either one of the following:

1. **How to factor** \(N = p \cdot q\). → **Hard to solve** (for now)
2. **Sum** \(p + q\). → **Never published by receiver.**

What do we need to know in order to use RSA?

1. How to convert messages into numbers and vice versa
2. How to compute \(\varphi(N) = (p - 1)(q - 1)\) → **easy. ✓**
3. For encryption: how to compute high powers \((\mod N)\)
4. For decryption: how to compute inverses \((\mod \varphi(N))\) and high powers \((\mod N)\) (Berlekamp's)

3
Converting messages into numbers and vice versa

The following is one of many possible methods for converting text into numbers. The basic idea is to use letters as the digits of a number written in base 26 using the conversion table to the left.

Since any resulting $k$ digit number (base 26) must be less than $N$ we must have

$$N > 26^k - 1 \implies k = \lfloor \log_{26} N \rfloor$$

For instance, if $N = 13 \cdot 1873 = 245363 \implies k = 3$.

It becomes the message

$$m = T \cdot 26^0 + H \cdot 26^1 + E \cdot 26^2 = 19 + 7 \cdot 26 + 4 \cdot 26^2 = 2905$$

We encrypt using $e = 323$ and get $2905^{323} \equiv 13,388 \pmod{N}$. Then we convert the new number into text.

$$13,388 = 24 + 514 \cdot 26$$

$$= 24 + (20 + 19 \cdot 26)26 = 24 + 20 \cdot 26 + 19 \cdot 26^2$$

$$= Y \cdot 26^0 + U \cdot 26^1 + T \cdot 26^2$$

So the plaintext THE is encrypted into the ciphertext YUT.
Power in modulo arithmetic

**Theorem 1.** Let $a, n, x, y$ be non-negative integers with gcd$(a, n) = 1$. Then

$$x \equiv y \pmod{\varphi(n)} \implies a^x \equiv a^y \pmod{n}.$$ 

$$a^x = a^{y + k\varphi(n)} = a^y \cdot a^{k\varphi(n)} = a^y \cdot (a^{\varphi(n)})^k = a^y \pmod{n}$$

**Example:**

$$7^{42} \pmod{11} \quad \varphi(11) = 10.$$ 

$$42 \equiv 2 \pmod{\varphi(11)} = 2 \pmod{10}$$

$$7^{42} \equiv 7^2 \pmod{11} = 49 \pmod{11} = 5.$$

**Example:** Find the last three digits of $7^{803}$

($$,$$ equiv. to finding $7^{803} \pmod{1000} = 10^3$)

($$you try$$)

In Wolfram Alpha: $\gg$ PowerMod[$7, 803, 1000$]

$$7^{803} \pmod{1000}$$
How do we compute $a^k \pmod{n}$ without ever having to deal with number bigger than $n^2$?

**Example.** Compute $1915793^{2641} \pmod{5678923}$.

**Step 1.** Compute the binary expansion of $k = 2641$.

$$2641 = 1 + 2^4 + 2^6 + 2^9 + 2^{11} = 1 + 16 + 64 + 512 + 2048$$

\[ \gg \text{Binary } [2641] \quad \gg \text{subtract from } 2641 \text{ the biggest power of } 2 \text{ I can.} \]

**Step 2.** Use repeated squaring to get the powers above \((\mod n)\).

\[
\begin{align*}
a^{16} &\equiv 3278564 \pmod{n} \\
a^{128} &\equiv 1529537 \pmod{n} \\
a^{1024} &\equiv 2627277 \pmod{n} \\
a^{2} &\equiv 3278564 \pmod{n} \\
a^{4} &\equiv 1631541 \pmod{n} \\
a^{8} &\equiv 3532287 \pmod{n} \\
a^{64} &\equiv 1631541 \pmod{n} \\
a^{128} &\equiv 3532287 \pmod{n} \\
a^{256} &\equiv 5673135 \pmod{n} \\
a^{512} &\equiv 5106329 \pmod{n} \\
a^{1024} &\equiv 2627277 \pmod{n} \\
a^{2048} &\equiv 1180227 \pmod{n} \\
\end{align*}
\]

Therefore,

\[
a^k = a \cdot a^{16} \cdot a^{64} \cdot a^{128} \cdot a^{2048}
\]

\[
\equiv 1915793 \cdot 1424066 \cdot 3305529 \cdot 5106329 \cdot 1180227 \pmod{n}
\]

\[
\equiv 1162684 \pmod{n}
\]
Example. Use RSA with modulus \( N = 53 \cdot 89 \), encryption exponent \( e = 119 \) and decryption exponent \( d = 423 \).

(a) Encrypt the message 75.

(b) Decrypt the message 2.

(a) To encrypt 75, compute \( c = m^e \pmod{n} = 75^{119} \pmod{4717} = 3500 \)

W/o Wolfram Alpha, use repeated squaring:

\[
119 = 64 + 32 + 16 + 4 + 2 + 1 = 2^6 + 2^5 + 2^4 + 2^2 + 2^1 + 2^0
\]

<table>
<thead>
<tr>
<th>( k )</th>
<th>1</th>
<th>2</th>
<th>4</th>
<th>8</th>
<th>16</th>
<th>32</th>
<th>64</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 75 \pmod{n} )</td>
<td>75</td>
<td>908</td>
<td>3706</td>
<td>3249</td>
<td>4072</td>
<td>929</td>
<td>9547</td>
</tr>
</tbody>
</table>

\[
75^2 \pmod{4717} = 5625 \pmod{4717} = 908
\]

\[
908^2 \pmod{4717} = 3706
\]

\[
3706^2 \pmod{4717} = 3249
\]

\[
75^{119} = 75 \cdot 908 \cdot 3706 \cdot 4072 \cdot 929 \cdot 4547 \pmod{4717}
\]

(b) To decrypt: \( m = c^d \pmod{n} = 2^{423} \pmod{4717} = \ldots = 3419 \)
Issue with RSA

In order to create an RSA key pair, Bob needs to choose two very large primes $p$ and $q$. More precisely, he needs a way of distinguishing between prime numbers and composite numbers, since if he knows how to do this, then he can choose large random numbers until he hits one that is prime.

**Definition 1.** Fix an integer $n$. We say that an integer $a$ is a **witness** for (the compositeness of) $n$ if

$$a^n \neq a \pmod{n}.$$  

**Remark:** A single witness for $n$ is enough to prove that $n$ is composite.

**Idea for prime testing:** Try a lot of numbers $a_1, a_2, a_3, \ldots$. If any one of them is a witness for $n$, then $n$ is composite; and if none of them is a witness for $n$, then Bob suspects, but does not know for certain, that $n$ is prime.

Unfortunately, there is no way to tell for sure!

- The number $561 = 3 \cdot 11 \cdot 17$ is composite, yet 561 has no witnesses. In other words,

  $$a^{561} \equiv a \pmod{561}$$ for every integer $a$.

- Composite numbers having no witnesses are called Carmichael numbers, after R.D. Carmichael, who in 1910 published a paper listing 15 such numbers.

- Worse, there are infinitely many Carmichael numbers (proved by Alford, Granville, and Pomerance in 1984)
Definition 2. An integer $a$ is a quadratic residue $\mod p$ if the equation
\[ x^2 - a \equiv 0 \pmod{p} \]
has a solution.

We will denote the set of quadratic residues $\mod p$ by the symbol $QR[p]$.

\[
\begin{array}{c|cccc}
\text{mod 5} : & x & 1 & 2 & 3 & 4 \\
\hline
x^2 & 1 & 4 & 4 & 1 \\
\end{array}
\]

\[
\begin{array}{c|cccc}
\text{mod 7} : & x & 1 & 2 & 3 & 4 & 5 & 6 \\
\hline
x^2 & 1 & 4 & 2 & 2 & 4 & 1 \\
\end{array}
\]

\[
\begin{array}{c|ccccccccc}
\text{mod 11} : & x & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\
\hline
x^2 & 1 & 4 & 9 & 5 & 3 & 3 & 5 & 9 & 4 & 1 \\
\end{array}
\]

Theorem 2. Precisely half the integers in $\{1, 2, \ldots, p-1\}$ are quadratic residues $\mod p$. That is, $\#QR[p] = (p - 1)/2$.

Theorem 3. For any prime $p > 2$ and any $a \not\equiv 0 \pmod{p}$ we have
\[ a_{\frac{p-1}{2}} \pmod{p} = \begin{cases} 
1 & \text{if } a \in QR[p] \\
-1 & \text{if } a \not\in QR[p] 
\end{cases} \]