Day 21 – Discrete Log Problem and Applications

Solovay-Strassen Prime Testing

• Pick at random $a_1, a_2, \ldots, a_k \in \{1, 2, \ldots, n - 1\}$.

• For each $a = a_i$ check the two equalities
  
  \[ J(a, n) = a^{\frac{n-1}{2}} \pmod{n} \]
  
  \[ \gcd(a, n) = 1. \]

• If any of the two equalities fails, then $n$ is not a prime.

• If both equalities check out for all $a_i$, we accept $n$ as a prime.

The bigger $k$ is, the higher the probability of reaching the correct conclusion.
An attack on RSA - quadratic factoring

To factor $n$, Eve wants to find pairs $x > y$ such that

$$x^2 - y^2 \equiv 0 \pmod{n}.$$ 

If neither $x + y$, nor $x - y$ are divisible by $n$, then the $\gcd(x + y, n)$ and $\gcd(x - y, n)$ give nontrivial factors of $n$.

This will definitely happen if $0 \leq y < x \leq (n - 1)/2$, as in this case

$$0 < x - y \leq x < n - 1 \quad \text{and} \quad 0 < x + y \leq n - 1.$$ 

The idea above allows one simple attack on RSA:

1. Randomly select distinct integers $x_1, x_2, \ldots, x_k \in [0, (n - 1)/2]$.
2. Compute $x_i^2 \pmod{n}$ for all $i$.
3. If we find a pair $i \neq j$ with

$$x_i^2 \equiv x_j^2 \pmod{n}$$

then $\gcd(x_i + x_j, n)$ and $\gcd(x_i - x_j, n)$ are nontrivial factors of $n$. 


Discrete Log Problem

Fix a prime $p$ and a number $\alpha$ not divisible by $p$. For a given integer $\beta$, we want to find $x$ such that

$$\alpha^x \equiv \beta \pmod{p}.$$ 

Definition 1. We say that $a$ is a primitive root mod $p$ if

$$a^i \not\equiv 1 \pmod{p} \text{ for all } i < p - 1.$$ 

Theorem 1. If $g$ is a primitive root mod $p$, then

$$g^1, g^2, \ldots, g^{p-1} \pmod{p}$$

give a permutation of the integers

$$1, 2, \ldots, p - 1.$$
Recall the Möbius function:

\[ \mu(d) = \begin{cases} (-1)^k & \text{if } d \text{ is the product of } k \text{ distinct primes} \\ 0 & \text{otherwise} \end{cases} \]

**Definition 2.** The \( n \)-th **cyclotomic polynomial** is given by

\[ C_n(x) = \prod_{m|n} (1 - x^m)^{\mu\left(\frac{n}{m}\right)} \]

**Theorem 2.** Each prime \( p \) has exactly \( \varphi(p - 1) \) primitive roots. In fact, \( a \) is a primitive root modulo \( p \) if and only if

\[ C_{p-1}(a) \equiv 0 \pmod{p}. \]
Question: How to find all primitive roots if you know one of them?

Theorem 3. If $a$ is a primitive root modulo the prime $p$, then the set of primitive roots mod $p$ is

$$\{a^r : 1 \leq r \leq p - 1, \gcd(r, p - 1) = 1\}.$$
Solving equations using primitive roots
Under modulo $p = 11$ 2 is a primitive root and the powers of 2 are

<table>
<thead>
<tr>
<th>$k$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^k$</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>6</td>
<td>1</td>
</tr>
</tbody>
</table>

Solve the equation $9x \equiv 5 \pmod{11}$.

Solve the equation $7^x \equiv 5 \pmod{11}$. 
Definition 3. Fix a prime $p$ and a \textbf{primitive root} $\alpha$ modulo $p$. For a given integer $\beta$, we want to find $x$ such that

\[ \alpha^x \equiv \beta \pmod{p}. \]

In this case, we write $x = \log_\alpha (\beta) \pmod{p}$.

- We take $\alpha$ to be a primitive root so that the discrete log problem can have a solution for any RHS value $\beta$.
- Given a prime $p$, it is fairly easy to find a primitive root.
- For small $p$, we can compute discrete logs by exhaustive search.
- In general, computing discrete logs is hard (no known polynomial time algorithm)
- In other words, exponentiation mod $p$ is believed to be a trapdoor function.
**El Gamal Cryptosystem**

1. Alice and Bob agree on a prime $p$ and a primitive root $r$ modulo $p$.

2. Alice comes up with her secret component $a$ and compute her public key $\alpha = r^a \mod p$.

3. Bob comes up with his secret component $b$ and compute his public key $\beta = r^b \mod p$.

4. Suppose Bob wants to send the message $X$ to Alice. He then picks a session key $k$, which is a random number in the interval $[2, p - 2]$.

5. Bob then computes $U = r^k \mod p$ and $V = \alpha^k X = r^{ak}X \mod p$. He then sends $(U, V)$ to Alice.

6. To decrypt Bob’s message, Alice computes

$$U^{-a}V = r^{-ka}\alpha^k X = r^{-ak}r^{ak}X = X.$$
What can the enemy do?

Suppose that Eve intercepts the pair \((U, V)\), but to recover the message, Eve would need to know Alice’s secret component \(a\). Eve then has two choices, either

- solve for \(a\) from \(\alpha = r^a \mod p\), or
- solve for \(k\) from \(U = r^k \mod p\) then compute \(\alpha^{-k}V = \alpha^{-k}\alpha^kX = X\).

One of the major downsides of public key cryptosystems (e.g. RSA, El Gamal) is that they are relatively slow compared to modern ciphers (DES, AES). If you want to encrypt a good bit of data,

1. Use a public key cryptosystem to establish a secret key.
2. Encrypt the actual data using a fast cipher with the established secret key.