Lecture 23: RSA Assumption

Recall

- Earlier we have seen how to generate a random n-bit prime number
- We also saw how to efficiently test whether a number is a prime number or a composite number (basic Miller–Rabin Test)

Summary

- Today we will see a new computational hardness assumption: the RSA Assumption

RSA Assumption I

- Let N be the product of two n-bit primes numbers p, q chosen uniformly at random from the set P_n
- Let $\varphi(N) = (p-1)(q-1)$ be the number of elements in $\mathbb{Z}_N^*$ (the set of integers that are relatively prime to N)
- We shall state the following result without proof

Claim

Let $e \in \{1, 2, \ldots, \varphi(N) - 1\}$ be any integer that is relatively prime to $\varphi(N)$. Then, the function x^e from the domain $\mathbb{Z}_N^*$ to the range $\mathbb{Z}_N^*$ is a bijection.

RSA Assumption II

- The RSA Assumption states the following.

Honest Challenger		Adversary $\mathcal{A}$
$p, q \xleftarrow{\$} P_n$		
$N = p \cdot q$		
$e \xleftarrow{\$} \mathbb{Z}^*_{\varphi(N)}$		
$y \xleftarrow{\$} \mathbb{Z}^*_N$	$\xrightarrow{N, n, e, y}$	
	$\xleftarrow{x}$	
$z = (y == x^e)$		

- **RSA Assumption.** For any computationally bounded adversary $\mathcal{A}$, the probability that $z = 1$ is exponentially small

Working Example

- We shall use $p = 3$ and $q = 11$
- So, we have $N = p \cdot q = 33$
- Moreover, we have

$$\mathbb{Z}_N^* = \{1, 2, 4, 5, 7, 8, 10, 13, 14, 16, 17, 19, 20, 23, 25, 26, 28, 29, 31, 32\}$$

- Now, $\varphi(N) = (p-1)(q-1) = 2 \cdot 10 = 20$. Verify that this is the size of $\mathbb{Z}_N^*$
- For this example, we shall choose $e = 3$ (note that 3 is relatively prime to $\varphi(N) = 20$, that is $e \in \mathbb{Z}_{\varphi(N)}^*$)

Working Example

Let us start the repeated squaring procedure. The first row represents each element of $\mathbb{Z}_N^*$ and the second row is the square of the corresponding element in the first row.

x	1	2	4	5	7	8	10	13	14	16	17	19	20	23	25	26	28	29	31	32
x^2	1	4	16	25	16	31	1	4	31	25	25	31	4	1	31	16	25	16	4	1

Working Example III

Using repeated squaring, we compute the third row that is the fourth-power of the element in the first row.

x	1	2	4	5	7	8	10	13	14	16	17	19	20	23	25	26	28	29	31	32
x^2	1	4	16	25	16	31	1	4	31	25	25	31	4	1	31	16	25	16	4	1
x^4	1	16	25	31	25	4	1	16	4	31	31	4	16	1	4	25	31	25	16	1

We add a row that computes $y = x^e$ (recall that $e = 3$ in our case). We can obtain x^3 by multiplying $x \times x^2$.

x	1	2	4	5	7	8	10	13	14	16	17	19	20	23	25	26	28	29	31	32
x^2	1	4	16	25	16	31	1	4	31	25	25	31	4	1	31	16	25	16	4	1
x^4	1	16	25	31	25	4	1	16	4	31	31	4	16	1	4	25	31	25	16	1
$y = x^e = x^3$	1	8	31	26	13	17	10	19	5	4	29	28	14	23	16	20	7	2	25	32

We can now verify from the table that x^3 is a bijection from $\mathbb{Z}_N^*$ to $\mathbb{Z}_N^*$ (because 3 is relatively prime to $\varphi(N)$)
We recall the following result (stated without proof) from the beginning of the lecture.

Theorem

For any $e \in \mathbb{N}$ such that $\gcd(e, \varphi(N)) = 1$ and $e < \varphi(N)$, the function $x^e : \mathbb{Z}_N^* \to \mathbb{Z}_N^*$ is a bijection.

Since x^e is a bijection, we can uniquely define $y^{1/e}$ for any $y \in \mathbb{Z}_N^*$.
For example, if $y = 19$ then $y^{1/e} = 13$, where $e = 3$.
The RSA assumption states that, for a random y, finding $y^{1/e}$ is a computationally difficult task!

Let d be an integer $< \varphi(N)$ such that $e \cdot d = 1 \mod N$. In our case, we have $d = 7$.

Let us calculate a row corresponding to x^7. We can calculate this by multiplying $x \times x^2 \times x^4$.

x	1	2	4	5	7	8	10	13	14	16	17	19	20	23	25	26	28	29	31	32
x^2	1	4	16	25	16	31	1	4	31	25	25	31	4	1	31	16	25	16	4	1
x^4	1	16	25	31	25	4	1	16	4	31	31	4	16	1	4	25	31	25	16	1
$y = x^e = x^3$	1	8	31	26	13	17	10	19	5	4	29	28	14	23	16	20	7	2	25	32
$x^d = x^7$	1	29	16	14	28	2	10	7	20	25	8	13	26	23	31	5	19	17	4	32

Note that d is also relatively prime to $\varphi(N)$, and, hence, the mapping x^d is also a bijection.

But note that, given d, we can easily compute the e-th root of y. Check that y^d is identical to $y^{1/e}$.

x	1	2	4	5	7	8	10	13	14	16	17	19	20	23	25	26	28	29	31	32
x^2	1	4	16	25	16	31	1	4	31	25	25	31	4	1	31	16	25	16	4	1
x^4	1	16	25	31	25	4	1	16	4	31	31	4	16	1	4	25	31	25	16	1
$y = x^e = x^3$	1	8	31	26	13	17	10	19	5	4	29	28	14	23	16	20	7	2	25	32
$x^d = x^7$	1	29	16	14	28	2	10	7	20	25	8	13	26	23	31	5	19	17	4	32
$y^d = y^7$	1	2	4	5	7	8	10	13	14	16	17	19	20	23	25	26	28	29	31	32

Quick Summary

- The function $x^e \colon \mathbb{Z}_N^* \to \mathbb{Z}_N^*$ is a bijection for all e such that $\gcd(e, \varphi(N)) = 1$
- Given (n, N, e, y), where $y \xleftarrow{\$} \mathbb{Z}_N^*$, it is difficult for any computationally bounded adversary to compute the e-th root of y, i.e., the element $y^{1/e}$
- But given d such that $e \cdot d = 1 \mod \varphi(N)$, it is easy to compute $y^{1/e}$, because $y^d = y^{1/e}$

Now, think how we can design a key-agreement scheme using these properties. Once the key-agreement protocol is ready, we can use a one-time pad to create a public-key encryption scheme.