Cryptography – Homework 4

冯诗伟 161220039

1

Assume that the adversary $\mathcal{A}$ can break 1% of $\mathbb{Z}_N^*$ (a specific subset) with probability of 1 and break the other 99% with probability of 0.

We can construct $\mathcal{A}'$ as follows:

1. Given $y = x^e \bmod N$.

2. Uniformly choose $r \in \mathbb{Z}_N^*$ and r^{-1} such that $r \cdot r^{-1} = 1 \bmod N$.

3. Feed $y \cdot r^e$ to $\mathcal{A}$ and get $z = \mathcal{A}(y \cdot r^e \bmod N)$.

4. Compute $x' = z \cdot r^{-1} \bmod N$. Check whether $(x')^e = y \bmod N$ holds.

5. Repeat step 1 to 4 for 459 times. Denote the x', y in the i-th round as x_i', y_i. If $(x_i')^e = y_i \bmod N$ for some i, output x_i' and stop. If this did not occur after 459 rounds, output x_1'.

Let me explain it in detail.

Step1 and Step2 are trival.

In Step3, the equation, $z = (y \cdot r^e)^{1/e} = y^{1/e} \cdot r \bmod N$, holds with probability of 0.01 since $\mathcal{A}$ succeeds with probability of 0.01.

In Step4, if $\mathcal{A}$ called by $\mathcal{A}'$ succeeds in Step3, we can get $x' = y^{1/e} \cdot r \cdot r^{-1} = y^{1/e} \bmod N$, which means $(x')^e = y \bmod N$.

In Step5, intuition is that the more times $\mathcal{A}'$ tries, the more likely $\mathcal{A}'$ will succeeds. So we want to know the least k that satisfy the following inequation:

$$1 - (1 - 0.01)^k \geq 0.99$$

which means after trying k times $\mathcal{A}'$ will succeeds with a probability not less than 0.99. So we have:

$$k \geq 459$$

As to the running time t', Step1 and Step4 is $\mathcal{O}(1)$. Step2 is $\mathcal{O}(log\ N)$ and Step3 is $\mathcal{O}(t)$. So running time t' of $\mathcal{A}'$ is polynomial in t and $\|N\|$.

2

First, because g is a generator($g^n = 1 \mod n$), $(g^r)^n = (g^n)^r = 1^r = 1 \mod n$.

Second, we can show that for all $0 \leq i \leq n-1$, $i \neq r$, there exists a $q(0 \leq q \leq n-1)$ such that $(g^r)^q = g^i \bmod n$.

Let $(g^r)^q = g^i \bmod n$. So $rq = i \mod n$. Because $gcd(r, n) = 1$, there exists a r^{-1} such that $r \cdot r^{-1} = 1 \mod n$. So we have

$$q = i \cdot r^{-1} \mod n$$

So far, we have proved that g^r is also a generator of $\mathbb{G}$.

Additional

Construct the following one-way function family $\Pi = (\mathsf{Gen}, \mathsf{Samp}, f)$:

Gen: Given 1^n, outputs parameters $I = (\mathbb{G},\ q,\ g)$ where the order $\|q\| = n$. g is the generator of $\mathbb{G}$. $\mathcal{D}_I = \mathcal{R}_I = \mathbb{G}$.

Samp: On input I, outputs a uniformly distributed $x \in \mathcal{D}_I$.

f : On input I and $x \in \mathcal{D}_I$, outputs $y = f_I(x) = g^x$.

We are going to show that Π is easy to compute and hard to invert.

1. Easy to compute. Given g and x, the complexity of compute g^x mod n is $\mathcal{O}(log\ x)$.

2. Hard to invert. Design the following experiment $\mathsf{Invert}_{\mathcal{A},\Pi}(n)$:

(1) Gen is run to obtain I, and then $\mathsf{Samp}(I)$ is run to obtain a uniform $x \in \mathcal{D}$. Finally $y := f_I(x) = g^x$ is computed.

(2) $\mathcal{A}$ is given I and $y = g^x$ as input, and outputs x'.

(3) The output if the experiment is 1 if $f_I(x') = x$.

We can see that the view of $\mathcal{A}$ in $\mathsf{Invert}_{\mathcal{A},\Pi}(n)$ is identical to that of $\mathsf{DLog}_{\mathcal{A},\mathsf{Gen}}(n)$. So $\mathcal{A}$ succeeds in $\mathsf{Invert}_{\mathcal{A},\Pi}(n)$ if and only if $\mathcal{A}$ succeeds in $\mathsf{DLog}_{\mathcal{A},\mathsf{Gen}}(n)$. We have:

$$\Pr[\mathsf{Invert}_{\mathcal{A},\Pi}(n) = 1] = \Pr[\mathsf{DLog}_{\mathcal{A},\mathsf{Gen}}(n) = 1] \leq negl(n)$$

So we have shown that Π is hard to invert.