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 XXX 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 XXX 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

Additional