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 $y' = z \cdot r^{-1} \bmod N$.

5. Repeat step 1 to 4 for XXX times. Denote the y' in the i-th round as y'_i. If any two outputs(y'_i and y'_j) in these XXX rounds are the same, output y'_i. Otherwise output 0.

Let me explain it in detail.

Step1 and Step2 is trival. In Step3, $z = y^{1/e}$

2

Additional