Cryptology Exercise Week 7

Zijun Yu 202203581

Octobor 2023

RSA is hard to break almost everywhere

If $z \notin \mathbb{Z}_n^*$, it means $gcd(z, n) \neq 1$. Since n is the product of two prime numbers p and q, we immediately know that $gcd(z, n)$ is either p or q. In either case, we can compute both p and q and then compute the secret key d.

If $z \in \mathbb{Z}_n^*$, we randomly pick an a in $\mathbb{Z}_n^*$, and compute $z \cdot a^e \mod n$. We know that $z \cdot a^e \equiv x^e \cdot a^e \equiv (x \cdot a \text{ mod } n)^e \mod n$. From theorems in group theory, we konw that modular mulplication is a bijection and so because $Pr[a \in S] = \epsilon$, we have $Pr[a \cdot x \mod n \in S] = \epsilon$. Therefore, we use $a \cdot x \mod n$ as the input to A and we have ϵ probility that we will get the plaintext of $a \cdot x \mod n$ and we can compute x by multiplying the inverse of a.