Cryptology Exercise Week 6

Zijun Yu 202203581

Octobor 2023

RSA decryption works on the entire domain

Because n is the product of two co-prime numbers p and q, the Chinese Remainder Theorem applies here. Because the f-function in the Chinese Remainder Theorem is injective, in order to show $x^{ed} \equiv x \mod n$, it suffices to show that $x^{ed} \equiv x \mod p$ and $x^{ed} \equiv x \mod q$, for all $x \in \mathbb{Z}_n$.

Here, we are showing the case where $x \notin \mathbb{Z}_n^*$. Since n is the product of the prime numbers p and q, we have that x is either the product of p and q, or a multiple of p or q.

In the case where $x = p \cdot q$, we have that $x \equiv x^{ed} \equiv 0 \mod p$ and $x \equiv x^{ed} \equiv 0 \mod q$.

We then discuss the case where x is a multiple of p or q. Without loss of generality, we assume that x is a multiple of p, but not of q. It is obvious that $x \equiv x^{ed} \equiv 0 \mod p$. Because q is a prime number and x is not a multiple of q, we have that x and q are co-prime and $(x \bmod q) \in \mathbb{Z}_q^*$. Notice that $|\mathbb{Z}_q^*| = q - 1$, hence we have

$$(x \bmod q)^{ed} \equiv x^{ed} \equiv x^{ed \bmod (q-1)} \mod q$$

Since $ed \equiv 1 \mod (p-1)(q-1)$, we have that $ed \equiv 1 \mod (q-1)$, hence

$$x^{ed} \equiv x \mod q$$