Cryptology Exercise Week 11

Zijun Yu 202203581

Octobor 2023

Hash functions from Factoring

We first prove that there exists an element in Z_n^* of order $2p'q'$.

Let α and β be a generator of Z_p^* and Z_q^* respectively, i.e. $2p'$ is the smallest i that satisfies $\alpha^i \mod p = 1$ and $2q'$ is the smallest i that satisfies $\beta^i \mod q = 1$.

By the Chinese remainder theorem, Z_n^* is isomorphic to $Z_p^* \times Z_q^*$, Z_p^*. Let f be the isomorphism from Z_n^* to $Z_p^* \times Z_q^*$, we prove that the order of $g = f^{-1}(\alpha, \beta)$ is $2p'q'$.

$$
\begin{array}{ccccccc}
(& \alpha & , & \beta &) & \leftrightarrow & g \\
(& \alpha^2 & , & \beta^2 &) & \leftrightarrow & g^2 \\
(& ... & , & ... &) & \leftrightarrow & ... \\
(& \alpha^{2p'q'} & , & \beta^{2p'q'} &) & \leftrightarrow & g^{2p'q'}
\end{array}
$$

We are going to prove that on the right side, $g^{2p'q'}$ is the first one that is equal to 1. By Chinese remainder theorem, it is equivalent to prove that on the left side, $(\alpha^{2p'q'}, \beta^{2p'q'})$ is the first pair that is equal to $(1, 1)$, which is true because $\alpha^{2p'} \equiv 1 \mod p$ and $\beta^{2q'} \equiv 1 \mod q$ and $2p'q'$ is the least common multiple of $2p'$ and $2q'$.

Then we show that given a collision for h defined by $h(m) = g^m \mod n$, one easily factor n.

Let m_1 and m_2 be two messages such that $h(m_1) = h(m_2)$, then $g^{m_1} \equiv g^{m_2} \mod n$, which is equivalent to $g^{m_1 - m_2} \equiv 1 \mod n$. This means that $m_1 - m_2$ is a multiple of $2p'q'$. Since $(p-1)(q-1) = 4p'q'$, by multiplying $m_1 - m_2$ by any even number, we get a multiple of $(p-1)(q-1)$. Then by Lemma 7.9, we can easily factor n.