Cryptography: Homework 10

(Deadline: 11:59am, 2019/12/4)

1. (20 points) Show that the plain RSA encryption is correct for any $m \in \{0, 1, \ldots, N-1\}$. That is, we have that $\mathbf{Dec}(sk, \mathbf{Enc}(pk, m)) = m$ for any $m \in \{0, 1, \ldots, N-1\}$.

   (Hint: $\gcd(m, N) = 1$ or $\gcd(m, N) > 1$)

2. (30 points) In the Paillier's encryption, suppose that $c_1 = \left((1+N)^{m_1} r_1^N \bmod N^2\right)$ and $c_2 = \left((1+N)^{m_2} r_2^N \bmod N^2\right)$. Show that $c_1 = c_2$ is impossible unless $m_1 \equiv m_2 (\bmod\ N)$ and $r_1 \equiv r_2 (\bmod\ N)$.

   (Hint: $\gcd(N, \phi(N)) = 1$; $c_1 = c_2$ if and only if $c_1/c_2 \equiv 1 (\bmod\ N^2)$)