Homework Assignment 2 - Introduction To Cryptography

Ton That Tam Dinh

October 5, 2017

Problem 1.17.

Proof. □

Problem 1.18. Suppose that $g^a \equiv 1(modm)$ and that $g^b \equiv 1(modm)$. Prove that $g^{gcd(a,b)} \equiv 1(modm)$

Proof. By Euclide Algorithm we have: u, v such that au + bv = gcd(a,b). So, $g^{gcd(a,b)} \equiv g^{au+bv} \equiv (g^a)^u.(g^b)^v \equiv 1(modm)$. □

Problem 1.19.

Proof. □

Problem 1.23.d. Prove that if gcd(m,n) = 1, then the pair of congruences $x \equiv a(modm)$ and $x \equiv b(modm)$ has a solution for any choice of a and b. Also give an example to show that the condition gcd(m, n) = 1 is necessary.

Proof. □

Problem 1.24.

Proof. □