

CSCI 284/162 – Cryptography – Spring 2009
George Washington University

Homework 2: 20 points

due 9 February, 6 pm

Policy on collaboration: All examinations, papers, and other graded work products and assignments are to be completed in conformance with The George Washington University Code of Academic Integrity. You may *not* discuss HWs among yourselves. Each student is expected to work on his or her own HW out independently. You may only refer to your class notes, the text book, and to class material such as slides, notes and links provided on the course website. You may not refer to any other material while working on the homework.

Any violations will be treated as violations of the Code of Academic Integrity.

Submit all HW in TA's mailbox by 6 pm on due date.

1. (5 points) Prove that $\gcd(a, m) = 1$ and $\gcd(b, m) = 1$ implies that $\gcd(ab, m) = 1$. Also provide a counter-example to show that $\gcd(a, m) = x$ and $\gcd(b, m) = y$ does not imply that $\gcd(ab, m) = xy$.

2. (15 points) Show that an element $a \in \mathbb{Z}_m$ does not have a multiplicative inverse if and only if $\exists x \in \mathbb{Z}_m, x \neq 0$ such that $ax = 0$. (As both a and x are in \mathbb{Z}_m , their product is understood to be a product *mod* m).