CSE 5852: Problem Set 2

Due: September 28, 2016

1 Defining integrity

a) **15 pts** In class we considered message unforgeability against chosen message attack. Formalize an alternative definition that provides security against messages drawn from a message distribution.

b) **15 pts** Our definition in class is secure for a single message. Present a modified experiment that provides security for k-messages. Think carefully about the order of events.

2 Number Theory

In this section we will prove some items that were asserted in class. Be careful about what manipulations you make and why you're allowed to make them.

a) **7 pts** Prove that if $a_1 = a_2 \mod n$ then $n|(a_1 - a_2)$.

b) **12 pts** Prove that for any a_1, a_2,

$$a_1 \mod b + a_2 \mod b \equiv a_1 + a_2 \mod b$$

and

$$(a_1 \mod b)(a_2 \mod b) \equiv a_1 a_2 \mod b.$$

c) **5 pts** Compute $248^{15} \mod 252$ without using numbers with more than three decimal digits. Show your work.

d) **5 pts** Compute $7^{128} \mod 9$. Show your work.

e) **12 pts** Let n be an integer, show that for any a such that $\gcd(a, n) = 1$ there exists an inverse $\mod n$. That is, $\exists a^{-1} \in \mathbb{Z}_n$ such that $a \cdot a^{-1} = 1$.

f) **12 pts** Let p be a prime. For an integer $a \in \{1, ..., p-1\}$ show the values $a \mod p, 2 \cdot a \mod p, 3 \cdot a, ..., (p-1)a \mod p$ are unique. What value is $\mathbb{Z}_p$ is not included in this set of values?

g) **7 pts** *Fermat's Little Theorem* Show that for any $a \in \{1, ..., p-1\}$, $a^{p-1} = 1 \mod p$.

3 Message Authentication Codes/Message Integrity

We will consider extensions to the integrity protections we built using a universal hash function. In this question we consider extensions to this construction.

a) **10pts** Show that the MAC we presented in class is insecure if used to protect two (distinct) messages. Show how to completely recover the key.