CS 161 – Computer Security
Instructor: Tygar
15 September 2015

Homework 2

Notes

- Homework 2 is due on 22 September 2015 at 3PM.
- Please work on this homework individually – no collaboration allowed.
- Please submit this homework in PDF format.
- It is possible to answer all questions relatively briefly. Please limit your answer to each question to a page at most.
- Submit this homework using Gradescope.

Please start the answer to each question and subquestion on a new page

1.

a. Compute $500^{-1} \bmod 10007$ using EGCD. Show your work. Note 10007 is prime.
b. Compute $500^{-1} \bmod 10007$ using the Euler-Fermat theorem. Show your work. Note 10007 is prime. You may use at most 30 multiplication operations; you may not use a computer to compute exponentials.

2. Consider the following protocol. Alice and Bob choose a common prime p. Alice picks a random $r \in \mathbb{Z}_p$ and sets s such that $rs = 1 \pmod{p-1}$. Bob similarly picks a random $t \in \mathbb{Z}_p$ and sets u such that $tu = 1 \pmod{p-1}$. They then exchange messages as follows:

$A \rightarrow B$: $m^r \bmod p \ (= m')$

$B \rightarrow A$: $(m')^t \bmod p \ (= m'')$

$A \rightarrow B$: $(m'')^s \bmod p \ (= m''')$

B computes $(m''')^u \bmod p$ and recovers m

a. Why does this protocol work?
b. Show the protocol is vulnerable to a man in the middle attack
c. Show that if an eavesdropper can compute discrete logarithms, it can break this protocol.

3. Let $h()$ be a collision-resistant, pre-image resistant, and second pre-image resistant hash function that outputs n bits. Let $expand(x)$ output the n-bit binary string representing x left-padded by zeros when $0 \leq x < 2^n$ and otherwise be undefined. Let $\|$ be the string concatenation operator. We construct a new function $h'()$:

$$h'(x) = \begin{cases} 0 \parallel expand(x) & 0 \leq x < 2^n \\ 1 \parallel h(x) & 2^n \leq x \end{cases}$$

a. Is $h'()$ pre-image resistant?
b. Is $h'()$ second pre-image resistant?
c. Is $h'()$ collision resistant?
d. Does second pre-image resistance imply pre-image resistance? Why or why not?
e. Does collision resistance imply pre-image resistance?