M343L: HOMEWORK SET 6 PROOFS

ANDREW TSENG: ART2589

Problem 4.8

Part A
At a glance, Eve can check if $S_1 = S_1'$ to check if Samantha used the same k to sign D, D'.
This is because within both of the processes of signing the two documents all have the same g, p, a in the Elgamal Signature.

Part B You can first solve for a with the given S_2, S_2'.

$$k(S_2 + S_2') = (D + D') - a(S_1 + S_1')$$

Part C Solve the DLP for the k. $k = 1$. Plugging in the values we find $a = 348145$.

Problem 5.30

Problem 5.38

Part A
Taking the second deriviative of $f(x) = e^{-x} - (1 - x)$.
Finding the zeroes of $f'(x) = -e^{-x} + 1$, we get that $x = 0$. Meaning that $f(0)$ is the minimum of $f(x)$ which we find to be 0. Thus for all x,

$$e^{-x} \geq 1 - x$$

Part B
We use the same technique from part A with the second derivative with $f(x) = -e^{-ax} + (1 - x)^a + \frac{1}{2}ax^2$
We find that the min is again 0 and is at the end point. Thus it is clear that for all x, $f(x) \geq 0$.

Part C
Let $a = m, x = \frac{n}{N}$.
The probability to get at least one red:

$$\Pr(E) = 1 - (1 - \frac{n}{N})^m$$

From part b:

$$1 - e^{\frac{nm}{N}} \geq 1 - (1 - \frac{n}{N})^m - \frac{-mn^2}{2N^2}$$

Moving and isolating the sides:

$$1 - (1 - \frac{n}{N}^m) \leq 1 - e^{\frac{nm}{N}} + \frac{-mn^2}{2N^2}$$

We conclude:

$$\Pr(E) \leq 1 - e^{\frac{nm}{N}} + \frac{-mn^2}{2N^2}$$

Given that N and n is small relative to N, then we know that $\frac{mn^2}{2N^2}$ converges to zero as N grows larger and n stays small. While $\frac{-mn}{N}$ also converges to 0 but not as fast as the previous expression. Thus at some range where N is large,

$$\Pr(E)/leqq - e^{\frac{-mn}{N}}$$

Problem 5.43

$I = 2\sqrt{\pi}$