Note: Please cite any resources used, and mention any classmates that you worked with on this assignment. If you worked alone, please also say so. We will start taking points off if this is missing.

Problem 1. Authentication

Show a man in the middle attack on the following authentication protocol:

$A \to S : A,\ B,\ N_a$

$S \to A : A,\ B,\ \{A,\ N_a,\ K_{ab}\}_{K_a},\ \{B,\ N_a,\ K_{ab}\}_{K_b}$

$A \to B : A,\ B,\ \{B,\ N_a,\ K_{ab}\}_{K_b}$

Problem 2. CryptoLocker

CryptoLocker is a piece of malware that, once delivered and run, encrypts files on its victims' computers, deletes the original file, and demands a payment in exchange for the ability to decrypt to recover the file. The creator wants to achieve certain properties:

- The user shouldn't be able to decrypt without payment (even if they hire a forensics expert);
- Different victims should not be able to co-operate to avoid paying separately: if victim Alice pays, that should in no way help victim Bob decrypt his files; and
- The creator wants to minimize the cost of administering the malware as well as the probability of being compromised itself

(a) How can CryptoLocker achieve these properties (to the extent possible)? What key-related material, if any, should be part of the malware binary? How would encryption and decryption work?

(b) Name one advantage and one disadvantage of your design (from the malware author's point of view.)