ECE 568: Assignment 2

Introduction

Please answer the following questions. Your answers should be written in full sentences, and any quantitative claims about security should be justified (i.e., more than just ”yes” or ”it’s much more secure”). The completed assignments should be submitted in **hard copy during class** on the week of March 14, 2016, and work must be done *individually*.

For questions covering cryptography, you may find it helpful to consult the Handbook of Applied Cryptography, available at http://www.cacr.math.uwaterloo.ca/hac/

Basic Ciphers

In class we discussed the properties of basic shift (Caesar) and substitution ciphers. Assume that a cryptographer wants to select one to encrypt strings of Cyrillic characters (47 possible letters):

1. How many possible keys can the shift cipher have? The substitution cipher? The poly-alphabetic cipher with period 3? Which would be considered more secure? *(2 marks)*
2. Is it generally true that one type of cipher (shift, substitution, or poly-alphabetic) is always more secure than one or more other ciphers? *(1 mark)*

Key Exchange

Alice and Bob are going to use Diffie-Hellman to establish a shared secret. Alice and Bob agree to use modulus n = 23 and generator g = 5. When establishing the secret, Alice selects a random number x and then sends 23, 5, and 4 to Bob. Bob then selects a random number y and sends 15 back to Alice.

Suppose an attacker Mallory intercepts the values send by Alice and Bob. Answer the following questions:

1. What would Mallory have to do in order to recover the secret? *(1 mark)*
2. What is the random value x selected by Alice? *(2 marks)*
3. What is the random value y selected by Bob? *(2 marks)*
4. What is the established secret? *(2 marks)*

ECE 568: Assignment 2

SSL

The transport phase of SSL performs the following operations to prepare data for transmission:

Step #	Description
1	Messages are broken into 4kB fragments
2	Each fragment is compressed
3	A sequence number is applied to each chunk
4	A MAC of each chunk is computed
5	Each chunk and MAC is encyrpted

Indicate what the consequences would be if each of the following changes is made to the SSL transport phase protocol:

1. Omitting step #1 *(1 mark)*
2. Omitting step #2 *(1 mark)*
3. Omitting step #3 *(1 mark)*
4. Omitting step #4 *(1 mark)*

Trust

Read the paper "*Do You Believe in Tinker Bell? The Social Externalities of Trust",* available from the course website. It presents some hypothetical key exchanges that could be used to help build networks of trust based on social networks.

1. Explain the purpose of "$\{k\}_{K_{AS}}$" in the exchange described in section 3.2. Specifically, what problem is it trying to solve (versus the simpler key exchange proposed on page 4), why does "k" need to be a unique value every time, and why is it encrypted with K_{AS}? *(3 marks)*
2. What role do "k" and "N_{AS}" play in the exchange described in section 3.3? *(3 marks)*

Total: 20 marks.