COSC412: Assignment 2

Due: 11:59pm Friday 25/09/2020

Instructions

- All work is to be submitted by email to dme@cs.otago.ac.nz.
- PDF format for documents is preferred—work can be done by hand and scanned into digital form.

Problems

1. A user U requires their client software C to authenticate on their behalf to a server S. The user's password is p. You are required to develop and present a protocol that allows C to authenticate U at S. Your protocol must not send p over the network at any time, in either plain-text or encrypted form.

   You may assume that C and S were able to establish securely a shared secret s at some time in the past, before your protocol is used.

   You should ensure that your protocol is resistant both (a) to replay attacks, and (b) to active attackers modifying data sent between C and S. Justify your protocol's resistance to each of these types of attack in your explanation of how your protocol works.

   [4 points]

2. In a similar manner to the worked example in the lecture notes, demonstrate and explain what happens at each of the following steps:

   (a) create some plaintext data that is different from that used in the lecture notes, and has a length of exactly three 128-bit blocks;

   (b) apply AES-128 encryption in the cipher block chaining mode (CBC) to that data;

   (c) choose and state your choice of a single bit within the first block of the ciphertext (you may need to explain how you number the bits);

   (d) flip your chosen bit within the ciphertext of the first block;

   (e) decrypt the data.

   The decrypted data will be damaged. Explain what effect (if any) your modification to the ciphertext has on each of the three decrypted blocks. (You may treat the inner workings of AES as a black box.) [3 points]

3. You receive two 128-bit ciphertext blocks that you know have been encrypted using AES. You know the encryption key. However, you also know that the plaintext message has a length between 134 and 254 bits, but you do not know the specific message length.

   Explain how the message can be encoded so that you are able to decode the correct length of plaintext.

   Now considering potential messages of any length, explain the difference in cost (e.g., space and/or time) between your method, and a method that does not encode the length of the message.

   [3 points]