UNIVERSITY OF MARYLAND
DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

ENEE 457
Computer Systems Security
Instructor: Charalampos Papamanthou

Homework 1

Out: 09/05/18 Due: 09/12/18 11:59pm

Instructions

1. Strictly adhere to the University of Maryland Code of Academic Integrity.
2. Submit your solutions as a pdf document at Canvas. Include your full name in the solutions document. Name the solutions document as x-hw1.pdf, where x is your last name.

Problem 1 (20 points) Write down the definition of perfect secrecy. Prove that one-time pad satisfies this definition. Consider an one-time pad that maps messages of two bits to ciphertexts of two bits using the keys $\{00, 01, 11\}$ (instead of $\{00, 01, 10, 11\}$). Argue why this is not a good one-time pad (i.e., it does not satisfy perfect secrecy).

Problem 2 (20 points) In class we talked about two different techniques for ensuring the *recoverability* of n blocks $b_1, b_2, \ldots, b_n$. One that does simple replication and one that uses error-correcting codes. Both techniques store $2n$ blocks, instead of n. In the first technique (simple replication), what is the minimum number of blocks that the adversary can delete in order to make some b_i irretrievable? How about in the second technique? Explain.

Problem 3 (40 points) As studied in class, a one-time pad can be used to encrypt one message only. Encrypting more than one message with the same key will start to leak information. In this problem, your goal will be to decrypt multiple messages encrypted with the same one-time pad, but without the key.

The following are hexadecimal representations of the encrypted messages. The length of all messages and the key is 52 bytes each. All the original plaintext messages are valid English text.

Cipher Text of Message 1:
737f68797e691a10020c1d6e75100c7009651d1d6561060c6d0b
6f046116650c031e1c001c09130a001b0163016569637a626f72

Cipher Text of Message 2:
6e6f7c6f78001d0018017270140016770e720b1d656f06690e17
7900150b671f0e020d6917680a0b791c6e0a0b006f676b636673

Cipher Text of Message 3:

6378737a7e6f091717151a691673116502680107147511 1a6d17
651c18646f036f1f04741c0d0c0f74060d10656d65797e66730e

You are given that the following four words are expected to be in the plain text of some of the messages (note that all plaintext messages are already in UPPER CASE):

CRYPTOGRAPHIC - PASSWORDS - DECIPHER - MATHEMATICS

1. Argue with an example (that you devise yourself) why using one-time pad multiple times can leak information, and how this can generally be useful for an attacker.

2. Describe how knowing certain words in the plaintext may even enable an attacker to recover some other portions that could be important. Think about small examples. Imagine two simple expressions in some war context:

   LOSS: 50 SOLDIERS
   WITHDRAW TOMORROW

   If these two messages are encrypted with the same one-time pad, and an adversary knows that the words "SOLDIERS" and "WITHDRAW" may appear in the actual plaintext, how can this be useful for the adversary to infer the rest of the plaintext?

3. Given your thoughts about point 2, decrypt as much as possible from the encrypted messages listed earlier. You will need to write some code in a programming language of your choice to help you decrypt the messages. The code is not required to automatically decrypt the messages directly (this is possible, but it can be challenging). It can be used as an intermediate stage to help you get to the right solution.

Your submission should include the code you used, its output, and a complete description in the report for how it was used to decrypt the messages. Providing the decrypted messages directly will result in no points for this item. It is required to illustrate your approach and effort.

Problem 4 (20 points) Alice and Bob shared an n-bit secret key some time ago. Now they are no longer sure they still have the same key. Thus, they use the following method to communicate with each other over an insecure channel to verify that the key k_a held by Alice is the same as the key k_b held by Bob. Their goal is to prevent an attacker from learning the secret key.

1. Alice generates a random n-bit value r.
2. Alice computes $x = k_a \oplus r$, and sends x to Bob.
3. Bob computes $y = k_b \oplus x$ and sends y to Alice.
4. Alice compares r and y. If $r = y$, she concludes that $k_a = k_b$, that is, she and Bob have indeed the same secret key.

Show how an attacker eavesdropping on the channel can gain possession of the shared secret key. Also show how an attacker who can do more than eavesdropping can make Alice and Bob believe they do not share the same key.