CS177: Computer Security
Prof. Stefano Tessaro

UC Santa Barbara
Fall 2018

Homework 1

Posted: Thursday, October 4, 2019 – 11:59pm
Due: Saturday, October 13, 2018 – 11:59pm (Gradescope submission)

Instructions and Rules

- Your submission must occur via Gradescope. Instructions will be posted on Piazza. Stay tuned.
- Write your solutions clearly. Justify *all claims* of your solution. Partially incorrect solutions can still be worth several points, but unjustified incorrect results will result in zero points for the corresponding question.
- You are not allowed to copy or transcribe answers to homework assignments from others or other sources.
- You are not allowed to look up solutions online, or use generic tools that may help you solve the task, unless otherwise instructed.
- You are not allowed to post (full or partial) solutions of your homework on the Piazza Q&A. Moreover, if you use facts from the online discussion, you should provide your own justification in your solution.
- You must write your answers *independently*. You should always be able to argue and explain your answers when asked for clarifications. You are allowed to discuss with other students about generic issues that arise in class (for instance, review the definition of a concept, or help with generic programming issues), but not the specifics of how you solved the task.
- When you will be unable to hand in the homework in time you must report this to the lecturer (ST) *as soon as possible*, but always before the deadline. No matter the reason, you will always be asked to present documentation.

Task 1 – Goals of Computer Security (5 points)

Classify each of the following acts (not necessarily related to computing infrastructures) as a violation of confidentiality, of data integrity, source integrity, or availability, or some combination thereof:

a) A hacker obtains millions of Yahoo passwords.

b) Anthony accidentally cuts the electricity from the server room.

c) The NSA finds an efficient method to break AES.

d) Anna registers the domain name "JohnSmith.com" and refuses to let John Smith buy or use the domain name.

e) Some malware encrypts the victim's hard drive with a secret key, and a criminal asks for a ransom to decrypt it.

f) The NSA wiretaps the cell phone of a suspect in a criminal investigation.

g) A foreign state actor finds a zero-day vulnerability for voting machines used in the US.

Hint: Answers may not be unique. Explain your answers as well as possible!

Task 2 – Cryptanalysis (10 + 5 points)

The goal of this task is to decrypt some ciphertexts generated with historical encryption methods which are only weakly secure.

a) The Shift Cipher (also known as Caesar's cipher) is a very simple symmetric encryption scheme. The secret key is a random integer k in the range $\{0, 1, \ldots, 25\}$. Then, to encrypt a certain text, we map each letter $x \in \{A, B, \ldots, Z\}$ to a new letter by moving k steps ahead in the alphabetical order, and possibly wrapping around if we reach the end of the alphabet. E.g., if $k = 2$, A is mapped to C, and Z is mapped to B, etc.

The ciphertext at `http://www.cs.ucsb.edu/~tessaro/cs177/hw/cipher1.txt` has been encrypted using the Shift Cipher – find the corresponding plaintext!

b) The ciphertext at `http://www.cs.ucsb.edu/~tessaro/cs177/hw/cipher2.txt` has been encrypted using a mono-alphabetic substitution cipher – find the corresponding plaintext!

c) (5 Bonus points) The ciphertext at `http://www.cs.ucsb.edu/~tessaro/cs177/hw/cipher3.txt` has been encrypted using a mono-alphabetic substitution cipher – find the corresponding plaintext!

Warning: You will get a positive number of points **only if** the decrypted plaintext comes with a detailed explanation of the procedure you used to obtain it. You are not allowed to use tools available on the Internet. If you write some code to help you out, please submit this code with the assignment. (Further instruction for code submission will follow.)

Task 3 – Block Ciphers (5 points)

A *block cipher* is an algorithm implementing a function $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$, such that for all values of $K \in \{0,1\}^k$, the function $E_K : \{0,1\}^n \to \{0,1\}^n$ mapping an n-bit string X to $E(K, X)$ is a *permutation*, i.e., it is one-to-one. The first k-bit argument is called the *key* and the second n-bit argument is the *plaintext*.

a) Does the following table describe a valid block cipher?[1] Justify your answer! (Rows and columns correspond to keys and plaintexts, respectively, and the table entry for row K and column X is the ciphertext $E(K, X)$.)

K / X	000	001	010	011	100	101	110	111
00	000	101	010	111	011	110	001	100
01	111	010	110	000	011	101	100	001
10	101	000	001	011	110	010	111	100
11	010	100	001	101	011	000	111	110

b) Consider the function $E' : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ such that $E'(K, X) = X$ for all $X, K \in \{0,1\}^n$. Show that E' is a block cipher.

c) Consider the function $E'' : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ defined as $E''(K, X) = \overline{X} \oplus K$ for all $X, K \in \{0,1\}^n$, where $\oplus$ denotes bit-wise xor, and where $\overline{X}$ is obtained by flipping all bits of X. Show that is E'' a block cipher.

d) Are E' and E'' secure block ciphers when $n = 128$? Justify your answer!

Task 4 – Playing with AES (5 points)

We want to develop a better sense of the pseudorandomness of the ciphertexts generated by the AES block cipher. In particular, we will focus on the most commonly used variant with 128-bit keys. Let X be the 16-byte string consisting of

$$X = 10\ 04\ 20\ 18\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00$$

in hex-format.

a) What is the value of $\mathsf{AES}_X(X)$? Write the result in hex-format. Here, $\mathsf{AES}_K(M)$ is the ciphertext generated by AES on input key $K$and plaintext M.

b) Find a 16-byte plaintext M with the property that the last byte of $C = \mathsf{AES}_X(M)$ is equal to 00.

Explain how you have found it!

c) Find a 16-byte key K with the property that the last byte of $C = \mathsf{AES}_K(X)$ is equal 00.

Explain how you have found it!

Hint: Instructions on how to evaluate AES using Python are available on Piazza. Solutions using other programming languages are possible, as AES would behave in the same way.

Task 5 – There is only so much one can do (5 points)

Mr. Cipher is a deep undercover agent from the Republic of Cryptonia. Every day, he sends one of two messages back to base:

- M_1 =“Nothing to report”,
- M_2 =“Meet me tomorrow at the rendez-vous point, I have information”.

[1] Note that we are not asking whether the block cipher is *secure!*

To send these messages, Mr. Cipher uses counter-mode encryption based on AES with a 128-bit key. In particular, it encrypts the current date (using 8 bytes), followed by the ASCII encoding of one of the above two messages. Mr. Cipher uses the same secret key every day.

You work for the counterintelligence – you *know* the messages M_1 and M_2, you know the exact location of the rendez-vous point, and you are intercepting Mr. Cipher's ciphertexts. Your task is to predict *when* Mr. Cipher will show up at the rendez-vous location.

a) Describe a strategy to obtain this information.

b) How could Mr. Cipher protect himself from your attack strategy?