Instructions and Rules

- Your solution must be stapled, and please do not forget to indicate on every single sheet (1) Your name and (2) The discussion section you are enrolled in (either Thu 4pm or Thu 5pm). Your graded solution will be returned during your section.

- 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 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 (7 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 social-security numbers from the Equifax breach.

b) A thief steals Josh’s house key.

c) The FBI wiretaps the cell phone of a suspect in a criminal investigation.

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

e) The NSA finds an efficient method to break AES.
f) Anna registers the domain name “JohnSmith.com” and refuses to let John Smith buy or use the domain name.

g) Jonah sends Peter an e-mail with a 2MB attachment, knowing that Peter’s remaining quota for his e-mail account is 2.1MB.

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

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

**Task 2 – Cryptanalysis**

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 \( \text{http://www.cs.ucsb.edu/˜tessaro/cs177/hw/cipher1.txt} \) has been encrypted using the Shift Cipher – find the corresponding plaintext!

b) The ciphertext at \( \text{http://www.cs.ucsb.edu/˜tessaro/cs177/hw/cipher2.txt} \) 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**

A block cipher is an algorithm implementing a function \( E : \{0, 1\}^k \times \{0, 1\}^n \rightarrow \{0, 1\}^n \), such that for all values of \( K \in \{0, 1\}^k \), the function \( E_K : \{0, 1\}^n \rightarrow \{0, 1\}^n \) 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) Which of the following function tables describe a block cipher for \( k = n = 2 \) and which ones do not? (Rows and columns correspond to keys and plaintexts, respectively, and the table entry for row \( K \) and column \( X \) is the ciphertext \( E(K, X) \).)

<table>
<thead>
<tr>
<th>( K ) ( X )</th>
<th>00</th>
<th>01</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>10</td>
<td>01</td>
<td>11</td>
<td>00</td>
</tr>
<tr>
<td>01</td>
<td>00</td>
<td>01</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>10</td>
<td>01</td>
<td>00</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>11</td>
<td>10</td>
<td>11</td>
<td>01</td>
<td>00</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>( K ) ( X )</th>
<th>00</th>
<th>01</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>00</td>
<td>01</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>01</td>
<td>01</td>
<td>10</td>
<td>11</td>
<td>00</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>11</td>
<td>01</td>
<td>01</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>00</td>
<td>00</td>
<td>10</td>
</tr>
</tbody>
</table>

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

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

e) Alice claims she has developed a new block cipher, with key and block length both equal to 16 bytes. Bob obtains an implementation of this cipher, and runs some tests. In particular, he picks a random key $K$, which ends up being

$$K = \text{AF 13 2A CC F1 9D C2 58 F3 6A BE B2 4C 26 4E 32}$$

and then evaluates the cipher on this key, and plaintexts

$$M_1 = 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01,$$
$$M_2 = 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02,$$
$$M_3 = 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03,$$
$$M_4 = 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04.$$

He then obtains the ciphertext blocks

$$C_1 = \text{AF 13 2A CC F1 9D C2 58 F3 6A BE B2 4C 26 4E 32},$$
$$C_2 = \text{AE 13 2A CC F1 9D C2 58 F3 6A BE B2 4C 26 4E 33},$$
$$C_3 = \text{AD 13 2A CC F1 9D C2 58 F3 6A BE B2 4C 26 4E 34},$$
$$C_4 = \text{AC 13 2A CC F1 9D C2 58 F3 6A BE B2 4C 26 4E 35}.$$

Bob believes the cipher is insecure. Is Bob’s belief justified? Explain!

**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. Throughout this task, let $X$ be the 16-byte string consisting of your 6-digit perm number, followed by 10 0’s. For example,

$$X = \text{01 02 03 04 05 06 00 00 00 00 00 00 00 00 00 00}$$

in hex-format, if your perm number is 123456.

a) What is the value of $\text{AES}_X(X)$? Write the result in hex-format. Here, $\text{AES}_K(M)$ 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 first byte of $C = \text{AES}_X(M)$ is equal 00. Explain how you have found it!

c) Find a 16-byte key $K$ with the property that the first byte of $C = \text{AES}_K(X)$ 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.