CS 4351 Computer Security, Fall 2026
University of Texas at El Paso
Homework 1
Due on 09/10/2026, at 11:59pm
Total: 60 points
You need to submit a pdf generated from LaTeX. If you do not have a local LaTeXsetup, I suggest https://www.overleaf.com/. You need to write the math formulas correctly using LaTeX.
This homework should be finished independently. AI violations are taken seriously.

1. [10 points] Consider an automated teller machine (ATM) to which users provide a personal identification number (PIN) and a card for account access. Give examples of confidentiality, integrity, and availability requirements associated with the system and, in each case, indicate the degree of importance of the requirement. Include as much resources (data, meta data, equipment, etc.) as you can think of which are worth protecting in the context of this problem.

2. [20 points] Read article "Computer security in the real world" by B. W. Lampson (Computer, 2004), available at `https://tomal-kuet.github.io/armanuzzaman/courses/Fall26/docs/comp-sec-lampson.pdf`. Answer the questions below in your own words (write a few sentences for each question, one line is not sufficient).

(a) [10 points] What was the most important message that you learned from the article?

(b) [10 points] Describe the parallel to physical security that the author draws in the article and differences that arise in the computer world.

3. [15 points] Suppose there is a simple (symmetric key) block cipher that takes a 128-bit key and a 64-bit block. Encryption of a block m with key $k = k_1||k_2$ in this block cipher is specified as $c = ((m+k_1)\ mod\ 2^{64}) \oplus k_2$, where k_1 and k_2 are both 64-bit long, $||$ denotes concatenation, and $\oplus$ denotes bitwise XOR. Note that $(m + k_1)\ mod\ 2^{64}$ corresponds to conventional 64-bit addition (where the overflow during the addition is simply discarded).

(a) [5 points] Provide a formula for decrypting block c using key k.

(b) [5 points] Suppose an attacker is capable of mounting a known plaintext attack on the cipher and uses that information to try to learn information about the key. This means that the attacker gets access to a sufficient number of pairs (m_1, c_1), (m_2, c_2), etc. Is it possible for the attacker to use the plaintext-ciphertext pairs to determine the key in less than 2^{128} time needed for a conventional brute force search? Show your attack. Note that your attack doesn't need to be efficient as long as it is better than brute forcing the entire key in 2^{128} time.

(c) [5 points] Suppose that an attacker is now capable of carrying out an (adaptive) chosen plaintext attack. What is now the amount of work that the attacker needs to do to recover the key? Show your attack.

4. [15 points] Assume an encryption algorithm in which performance for the legitimate parties, i.e., those with access to the key, grows linearly with the length of the key. In other words, for an n-bit key, encryption and decryption cost $O(n)$. At the same time, the only way to break the algorithm is to a perform a brute-force attack trying all possible keys. As discussed in class, security parameters and consequently key sizes are determined by the best known way to break an algorithm and current computing capabilities.

Now suppose that at some point in time the key size is k bits, but soon after advances in computer technology make computers twice as fast. Because computing capabilities have changed, the key size will need to be revisited to guarantee that the brute-force search cost is as time consuming as before (and you need to determine the new size). Given that both the legitimate users and attackers get faster computers, does this advance in computer speed work to the advantage of the legitimate users, the attackers, or does it not make any difference? In other words, the question asks how computing costs of the parties may be affected by the change in the computing speed (and consequently the key length). Explain your answer.