CSCI-UA.0480-63: Intro to Security & Cryptography Fall 2025

Homework 1

due: Tueday 2025-09-30 22:00 EDT via brightspace.nyu.edu

1. **Threat modeling:** Imagine you've just been hired to produce a comprehensive threat model for CitiBike, New York's public bike share system. Describe three security *policies*, and for each of them describe a specific *mechanism* to enforce those policies. Choose one policy each that deals with a threat from thieves (financially motivated attackers), terrorists (attackers aiming to cause violent disruption) and trolls (attackers trying to cause inconvenience or annoyance).

2. **Hash functions and privacy**: Bob is launching a new secure messaging app, BobCrypt. When Alice installs the app, it uploads a hash of her phone number to the BobCrypt server. The app then queries the server by sending the hash of each phone number in Alice's address book to learn which of Alice's friends already have BobCrypt accounts. The goal is that users can discover their friends' accounts while preventing the server from learning every user's address book.

   Bob argues that the server only sees the hashes of users' contacts' phone numbers, and since hash-functions are one-way, this doesn't reveal any information about the actual phone numbers. Explain to Bob why he's wrong by describing how a malicious server could in fact learn users' contacts' phone numbers.

3. **MACs vs. PRFs:** We learned in class that a PRF is a "stronger" primitive than a MAC. That is, all PRFs are MACs, but not all MACs are PRFs. Show that this is true in two parts:

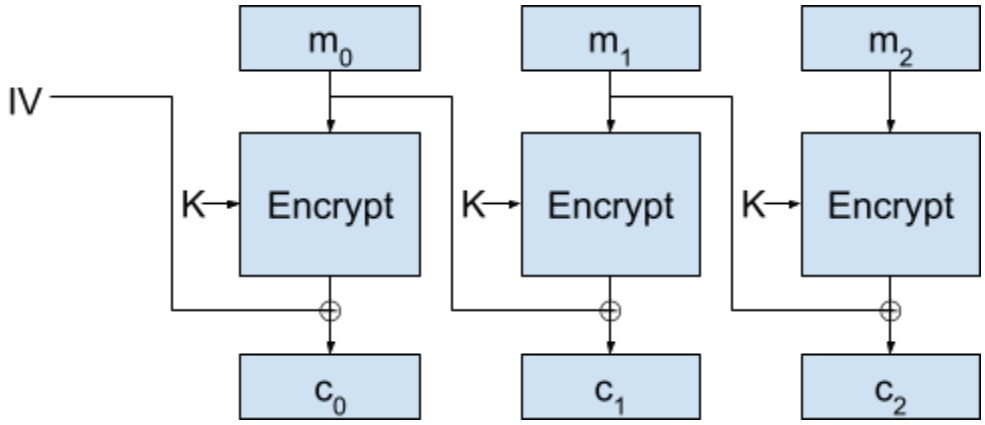
   a. Show that if a function F is a secure PRF, then F is also a MAC. To show this, show that any attacker who can win the MAC security game (existential unforgeability) against F can also win the PRF security. To do so, assume you have access to an algorithm A_1 which wins the MAC security game and describe an algorithm A_2 which uses A_1 as a subroutine and wins the PRF security game.

   b. Show a toy example of a MAC that isn't a PRF. One way to do this is to take a function F which *is* a PRF and define a tweaked version F' that is still a MAC but not a PRF.

4. **Semantic security for the Vigenère cipher:** The Vigenère cipher was a major advance in its day, but does not satisfy the modern definition of semantically secure encryption.

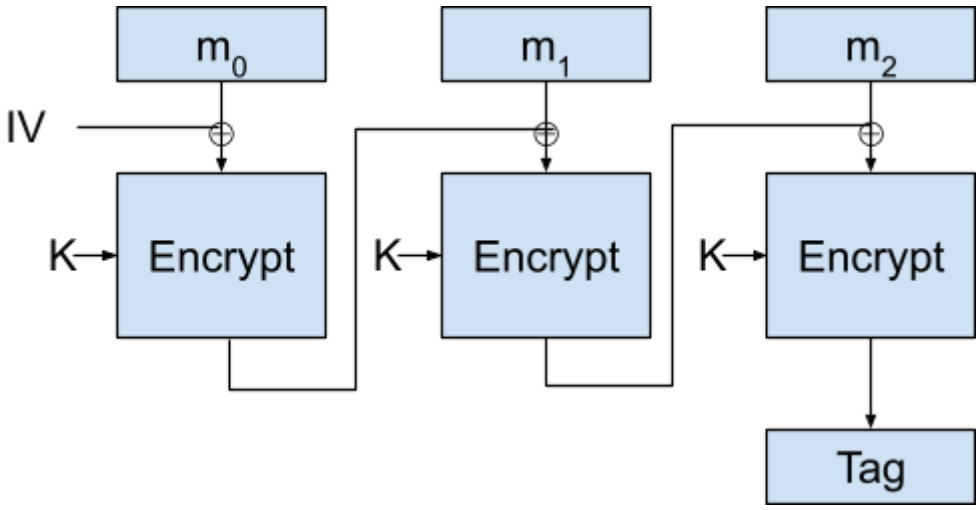
   To show this, describe an adversary algorithm that always wins the semantic security game, without making any chosen-plaintext or chosen-ciphertext queries. Your algorithm should submit two equal-length candidate plaintexts and then determine which one was encrypted to produce the ciphertext returned by the challenger. Assume the challenger chooses a random key of length 10 characters. **Hint:** your candidate plaintexts should be longer than 10 characters.

5. **Block cipher modes of operation:** In class we saw several modes such as ECB, CBC and CTR mode. Let's look at another possible mode of operation "plaintext block chaining" (PBC) which is similar to cipher block chaining (CBC) but allows for encryption in parallel:



Unfortunately, PBC mode is not secure. To see this, show how an attacker who knows IV, c_0, c_1, c_2 (which are public) and also knows that $m_1=m_2=x$ (for a known x) can easily compute m_0.

6. **CBC-MAC**: Alice is trying to design a MAC using a block cipher. She decides to use the following construction, which is essentially just CBC encryption, throwing away all but the final block:



Unfortunately, this construction is not secure. Describe how to produce an existential forgery against this MAC scheme. **Hint:** Start with two messages M_1 and M_2 (not to be confused with the individual blocks of a message in the diagram above) for which you know the outputs (IV_1, T_1) and (IV_2, T_2). Produce another message M_3 for which (IV_1, T_2) will be the MAC. M_3 will be close to the concatenation $M_1||M_2$, but with one block altered. **Hint 2:** There's also a way to produce a forgery with only one known block, if you look closely.

Caution: The blocks m_0, m_1,... in the diagram are distinct from the complete messages M_1, M_2...