CptS 327 - Fundamentals of Cyber Security and Cryptography
Assignment 6

Washington State University
School of Electrical Engineering and Computer Science

Spring 2025
Due: TBD

Problem 1

In this problem, you are going to show that the following encryption scheme is NOT secure against chosen plaintext attacks (CPA), even though the building block is a secure pseudorandom function.

Let $H(\cdot,\cdot) : \{0,1\}^{256} \times \{0,1\}^{256} \to \{0,1\}^{256}$ be SHA256, with key length and point length being 256 bits. We define the encryption scheme as follow:

- KeyGen: select a random secret key $k \leftarrow \{0,1\}^{256}$.
- Encrypt: to encrypt a message $m \in \{0,1\}^{256}$ with a secret key k, the algorithm samples a random $r \in \{0,1\}^{5}$ and output as ciphertext $c = (r, H(k,r) \oplus m)$.
- Decrypt: to decrypt a ciphertext $c = (c_1, c_2)$ with secret key k, the algorithm outputs $m = H(k, c_1) \oplus c_2$.

Your Task. (1) reason why the encryption is NOT secure against CPA. This encryption is very similar to the construction in the class (Feb 24 and Feb 26). Discuss the subtlety why the above scheme is insecure whereas the one in the class is secure.

(2) Write a program that launch a CPA attack against the above scheme in AWS. The details are as follow:

- Your Lambda function can make multiple (up to 1000) encryption queries (perhaps of the same message) to the challenger, i.e., the TA's AWS.
- Then the challenger will return ciphertexts of these queries.
- You then submit two messages m_0, m_1 to the challenger.

- The challenger will pick a random bit b and send encryption of m_b to you.
- You are going to send b' and you win if $b' = b$.

You need to win the game 100 times.