ITIS 6200/8200 Principles of Information Security and Privacy

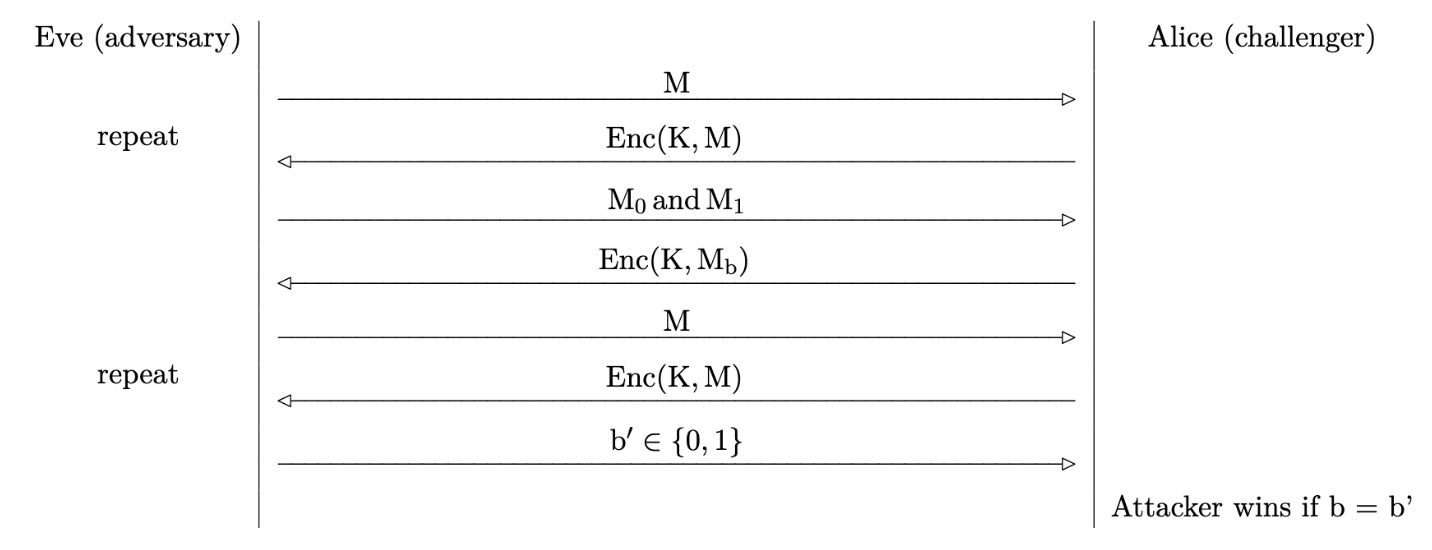
Homework 2

**Question 1. Break block cipher DES (20 points)**

The DES (Data Encryption Standard) was a symmetric encryption algorithm designed in 1976. It was the government standard until 2001. It has a block size of 64 bits, and key size of 56 bits. If an attack Eve want to brute-force attack DES, i.e., try all possible keys, how much time does Eve need? Assume that she can try 10^10 keys per second with her personal computer.

**Question 2. IND-CPA (25 points)**

When formalizing the notion of confidentiality, as provided by a proposed encryption scheme, we introduce the concept of indistinguishability under a chosen plaintext attack, or IND-CPA security. A scheme is considered IND-CPA secure if an attacker cannot gain additional information about a message given its ciphertext. This definition can be defined as an experiment between a challenger and adversary, detailed in the diagram below. Note that the same key K is used for encrypting different messages.



Q 2.1: The challenger will now flip a random bit b ∈ {0,1}, encrypt Mb, and send back C = Enc(k,Mb) = Mb ⊕ k to the adversary. How does the adversary determine b with probability > 1/2?

Q 2.2: Explain how an adversary can always win the IND-CPA game with probability 1 against a deterministic encryption algorithm. Note: Given an identical plaintext, a deterministic encryption algorithm will produce identical ciphertext.

Q 2.3: Explain why reusing keys in one-time pads is dangerous.

**Question 3. Hash (25 points)**

Alice is sending message M to Bob in the following way:

Ciphertext c = c1 || c2 , where c1 = Enc(K, m) and c2 = Hash(c1)

Here, Enc(K,m) is a secure encryption scheme AES-CBC, and Hash(m) is the cryptographic hash function SHA-256.

Q 3.1: Does this scheme provide confidentiality? E.g., can Eve learn about the contents of the message?

Q 3.2: Does this scheme provide integrity? E.g., can Mallory tamper with message without being detected?

Q 3.3: Can you design an approach for sending the message so it provides both integrity and confidentiality?

**Question 4. PRNGs and Diffie-Hellman Key Exchange (30 points)**

Eve is an eavesdropper between Alice and Bob.

1. Alice and Bob each seed a PRNG with different random inputs.
2. Alice uses her PRNG from the previous step to generate a, and Bob uses his PRNG from the previous step to generate b.
3. Alice and Bob perform a Diffie-Hellman key exchange using their generated secrets (a and b). Recall that, in Diffie-Hellman, neither a nor b are directly sent over the channel.
4. Alice and Bob, without reseeding, each use their PRNG to generate some pseudorandom output.
5. Eve learns both Alice’s and Bob’s pseudorandom outputs.

Assume that Eve always learns the internal state of a PRNG between steps 3 and 4. And Eve wants to learn the Diffie-Hellman shared secret gab mod p.

Q 4.1: If Alice and Bob both use a PRNG that are not rollback-resistant. Can Eve learn about the shared secret gab mod p? If yes, how?

Q 4.2: If Alice uses a PRNG that is not rollback-resistant. Bob uses a PRNG that is rollback-resistant. Can Eve learn about the shared secret gab mod p? If yes, how?

Q 4.3: Assume Alice generates a secret value a = 3, and Bob generates a secret value b = 2. The values of g and p are 5 and 7 respectively. Then, the shared secret should be gab mod p = 56 mod 7 = 1. However, Diffie-Hellman Key Exchange is vulnerable to Man-in-the Middle attack. Assume that Mallory is successfully launching Man-in-the Middle attack against the key exchange between Alice and Eve. Can you find a positive value m, such that the shared secret Alice computes is the same as the shared secret Bob computes? (Hint: consider writing a short loop in whatever programming languages you like to try different m)