ITIS 6200/8200 Principles of Information Security and Privacy

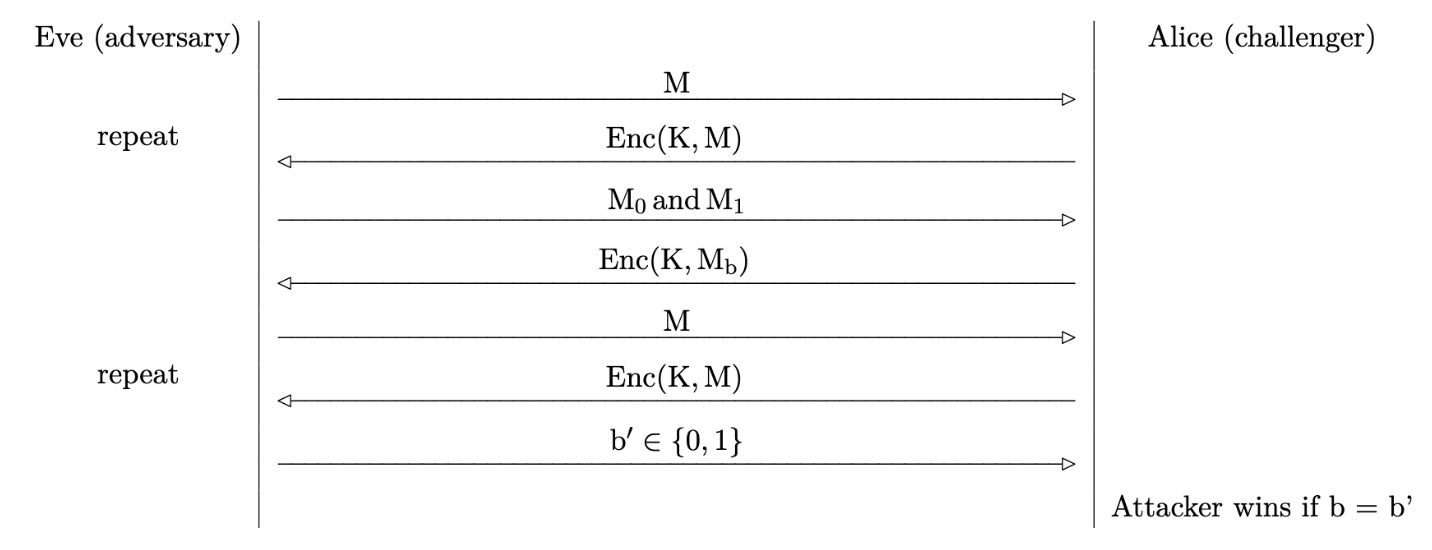
Homework 2

**Question 1**. Break DES.

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

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:



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: Putting it all together, 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: Assume that an adversary chooses an algorithm and runs the IND-CPA game a large number of times, winning with probability 0.6. Is the encryption scheme IND-CPA secure? Why or why not?

Question 3. MAC

Question 4. Confidentiality and Integrity

Alice and Bob want to communicate with confidentiality and integrity. They have:

• Symmetric encryption.  
– Encryption:Enc(K,m). – Decryption:Dec(K,c).

• Cryptographic hash function: Hash(m).

• MAC:MAC(K,m).  
They share a symmetric key K and know each other’s public key.

We assume these cryptographic tools do not interfere with each other when used in combination; i.e., we can safely use the same key for encryption and MAC.

Alice sends to Bob  
1. c = Hash(Enc(K, m))  
2. c = c1,c2 : where c1 = Enc(K,m) and c2 = Hash(c1)  
3. c = c1,c2 : where c1 = Enc(K,m) and c2 = MAC(K,m) 4. c = c1,c2 : where c1 = Enc(K,m) and c2 = MAC(K,c1)

Q2.1 Which ones of them can Bob decrypt?

Q2.2 Consider an eavesdropper Eve, who can see the communication between Alice and Bob. Which schemes, of those decryptable in (a), also provide confidentiality against Eve?

Question 5. Diffie-Hellman Key Exchange