ITIS 6200/8200 Principles of Information Security and Privacy

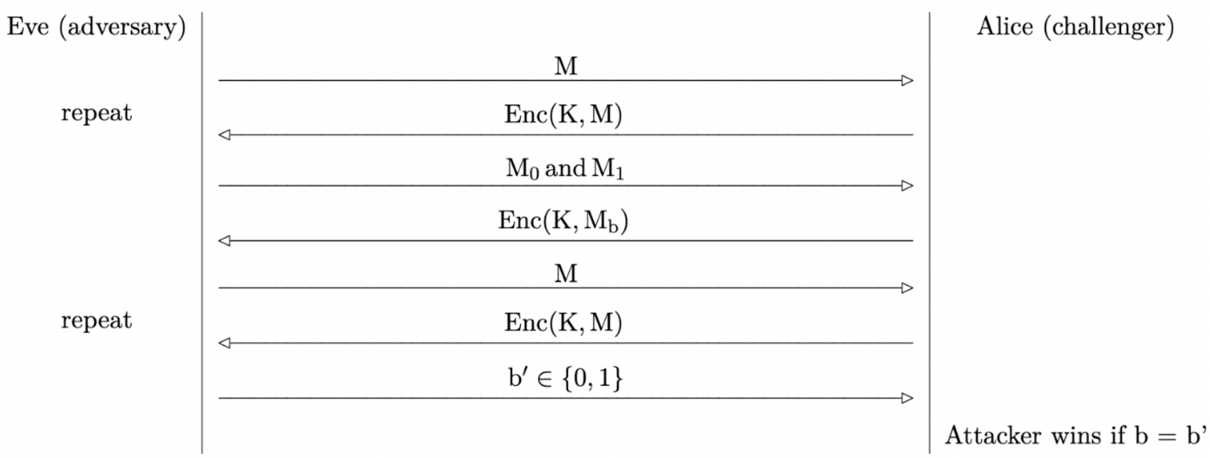
Homework 2

Question 1. Break block cipher DES (10 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 Eve wants 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. And one year is approximately 3×10^7 seconds.

Question 2. IND-CPA (20 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 here.



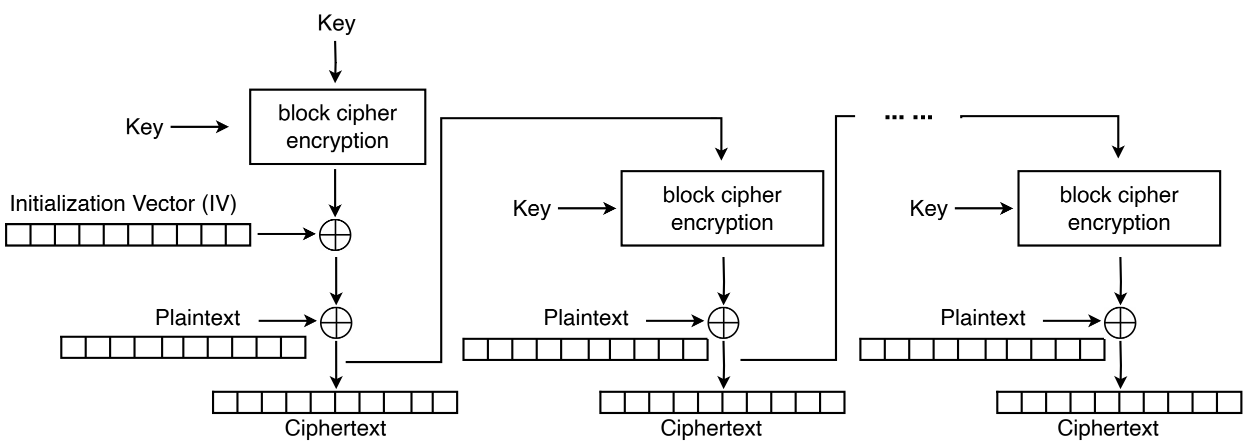
Q 2.1: Eve sends two messages M_0 and M_1 to Alice. Alice will flip a random bit $b \in \{0,1\}$, encrypt M_b, and send back $C = Enc(k, M_b) = M_b \oplus k$ to Eve. How does Eve determine b with probability > 1/2?

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. Block Cipher Design (25 points)

Alice has developed a new block cipher as below:



The message M is split into j plaintext blocks $M_1 \ldots M_j$ each of size n. The encryption mode outputs (IV, C_1, …, C_j) as the overall ciphertext. Assume that IV is randomly generated per encryption.

Q 3.1: Write down the encryption formula. That is, what is the formula for C_1 and C_i ($0 < i <= j$) given (1) plaintext $M_1 \ldots M_j$ (2) encryption algorithm Enc(K, M) which takes a key K and message M as inputs, and (3) a randomly generated IV.

Q 3.2: Write the decryption formula for M_i ($0 < i <= j$) using this mode. That is, how to get M_1 and M_i ($0 < i <= j$) given (1) ciphertext (IV, C_1, …, C_j) and (2) encryption algorithm Enc(K, M).

Q 3.3: Is this mode IND-CPA secure? If yes, explain why; if not, describe how an attacker can break IND-CPA.

Question 4. Hash (20 points)

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

$$\text{Ciphertext } c = c_1 \,||\, c_2 \text{ where } c_1 = \text{Enc}(K, m) \text{ and } c_2 = \text{Hash}(c_1)$$

Here, Enc(K,m) is the 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 an eavesdropper 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 5. PRNGs and Diffie-Hellman Key Exchange (25 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 can learn the internal state of a PRNG at step 5. And Eve wants to learn the Diffie-Hellman shared secret g^{ab} 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 g^{ab} mod p? If yes, how? If no, why?

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 g^{ab} mod p? If yes, how? If no, why?

Q 4.3: Assume that at step 2, Alice generates a secret value a = 3, and Bob generates a secret value b = 2. For step 3, the values of g and p are 5 and 7 respectively. Then, the shared secret should be g^{ab} mod p = 5^6 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 Bob. Can you find a positive value m from Mallory, such that the shared secret Alice computes is the same as the shared secret Bob computes? (Hint: consider writing a short loop program in whatever programming languages you prefer to try different m)