Problem 1 [10pts]

What are the fundamental goals in information security? Give a practical scenario each where each of these goals are desired? Explain how cryptography can be used to achieve these goals?

Problem 2 [10pts]

We studied various notions of security of a symmetric encryption scheme (against a passive attacker), namely, key recovery (KR), one-wayness (OW), indistinguishability (IND) and semantic security (SEM). State each of these notions (informally). What are the relations among these security notions (we studied some of these in the class)? Just state the relations. Is one-wayness a stronger security notion than key recovery? Show why/why not. Give an example to illustrate where OW security might not be sufficient, but IND is.

Problem 3 [15pts]

We discussed various active attacks on a symmetric encryption schemes, namely, chosen-plaintext attack (CPA), chosen-ciphertext attacks (CCA-1 and CCA-2). Describe each one of these attacks. Give a practical scenario where each such attack might be feasible to perform. Show IND-CCA2 \( \Rightarrow \) IND-CCA1 \( \Rightarrow \) IND-CPA.

Problem 4 [15pts]

We studied two different adversarial games to model the indistinguishability notion, namely IND and IND-G. Show that \( \text{Adv}^{\text{IND}}(A) = 2 \text{Adv}^{\text{IND-G}}(A) - 1. \)

Problem 5 [10+10pts]

1. Show that DES encryption satisfies the complementation property, i.e. if \( C = \text{Enc}(K, P) \) then \( C' = \text{Enc}(K', P') \) \((X' \text{ denotes the bitwise complement of } X)\). You have to explain each and every step to prove this.
2. Show how the above complementation property can be used to speed-up a brute force chosen-plaintext attack on DES by a factor of two, i.e. show a chosen-plaintext brute-force attack that requires only \( 2^{55} \) encryption/decryption operations in the worst-case, instead of \( 2^{56} \).
Problem 6 [10pts]

We studied perfect cipher one-time pad (OTP). Is OTP a deterministic or a probabilistic encryption scheme, and why?
Is OTP secure under IND-CPA attack? Why or why not?

Problem 7 [20pts]

We studied two definitions for perfect secrecy of a symmetric encryption scheme. Show that the two definitions are equivalent. In other words, you have to show that if an SE is secure w.r.t. the first definition then it is also secure w.r.t. to the second definition, and vice versa.