Week 2 Exercises (ECE 598 DA)

Exercise: Breaking a Toy Cipher with CPA. Suppose you have an encryption scheme where $E_k(m) = (m + k) \mod 26$ (an additive cipher on letters, like Caesar shift with key k). You are allowed to query an encryption oracle for this cipher. Devise a chosen-plaintext strategy to find the secret key k.

Exercise: Why Deterministic Encryption Fails CPA. Consider an encryption scheme that is deterministic (no randomization) and suppose an attacker suspects that two secret messages m_1 and m_2 are either equal or different. Explain how the attacker can use a chosen-plaintext query to distinguish these cases (thus breaking semantic security).

Exercise: CPA vs. Known-Plaintext. Briefly compare a *chosen-plaintext attack* with a *known-plaintext attack*. Which is a stronger adversarial model, and why do we require security against the stronger model in modern cryptography?

Exercise: Suppose a curator tries to protect a binary database of size n by adding noise σ (standard deviation) to each query answer. According to the Dinur–Nissim result, what should σ scale with (as a function of n) in order to prevent an attacker from reconstructing almost all secret bits, if the attacker can ask on the order of n queries?

Exercise: Show a simplified version of the Dinur–Nissim attack for a database of n bits with *no noise*: describe how an attacker can reconstruct all n bits with n carefully chosen queries.

Exercise: Timing Attack on Password Check. Consider a system that checks a password byte-by-byte and stops at the first wrong byte, returning "failure" immediately. Explain how an attacker could use timing measurements to gradually discover the correct password. What countermeasure would you suggest?

Exercise: RSA Square-and-Multiply Leak. Suppose an RSA decryption implementation uses square-and-multiply exponentiation and does not take constant time for each bit. Specifically, it takes T_0 time to process a '0' bit (square only) and T_1 time to process a '1' bit (square-and-multiply), with $T_1 > T_0$. The total decryption time is observable. How could an attacker recover a 1024-bit private exponent d from just the total time measurements of many decryptions?

Exercise: Mitigation Strategies. List two generic countermeasures against side-channel attacks and briefly explain how they help.

Exercise: Differential Cryptanalysis Example. Setup a tox example to show the efficacy of a differential cryptanalysis attack.