Fundamentals of Information Science: Homework 10

May 14, 2025

Problem 1. Ciphertext expansion vs. security
Let $\mathcal{E} = (E, D)$ be an encryption scheme messages and ciphertexts are bit strings.

(a) Suppose that for all keys and all messages m, the encryption of m is the exact same length as m. Show that (E, D) cannot be semantically secure under a chosen plaintext attack.

(b) Suppose that for all keys and all messages m, the encryption of m is exactly ℓ bits longer than the length of m. Show an attacker that can win the CPA security game using $\approx 2^\ell/2$ queries and advantage $\approx 1/2$. You may assume the message space contains more than $\approx 2^\ell/2$ messages.

Problem 2. Understand public-key encryption

Given two random primers $(p, q) = (31, 43)$, you are asked to construct an RSA encryption based on the two primes (p, q) (although the primes are two small to guarantee security).

(a) Construct a pair of public key and secret key.

(b) Demonstrate the process of encrypting a message $m = 100$ with a random number $x = 13$ using the generated key pair, and then decrypt the resulting ciphertext.