Homework 1

Due date: Friday, September 13, 2024

Throughout this homework assignment, we assume that $b \in \{0,1\}$ is a plaintext bit. To encrypt it, we generate a uniform random bit $r \in_R \{0,1\}$, and the ciphertext bit $c = b \oplus r$. We assume r is uniform random independent of b, so $\Pr[r = 1] = \Pr[r = 0] = 1/2$. Let p_b be the probability that the plaintext bit is chosen to be b, for $b = 0, 1$, so in particular $p_0 + p_1 = 1$.

Formally we have a sample space $\Omega_B = \{0,1\}$ for the plaintext bit b with probability distribution $p_0 = \Pr[b = 0]$ and $p_1 = \Pr[b = 1]$, a sample space $\Omega_R = \{0,1\}$ for r with probability distribution $\Pr[r = 0] = \Pr[r = 1] = 1/2$. As discussed in lectures, we may regard b, r and c as random variables over the sample space $\Omega_B \times \Omega_R$, with b and r being independent.

1. Show that no matter what p_b is for $b = 0, 1$, c is always a fair bit. That is, $\Pr[c = 0] = \Pr[c = 1] = 1/2$.

2. In class we proved that b and c are independent. Identify the properties of r and c from which that the independence of b and c follows. Point out in what steps of the proof these properties are used.

3. Suppose a secret plaintext bit b is encrypted and the ciphertext bit c is revealed to us. We would like to guess what b is. As mentioned before, we know the probability distribution of b and the key r is uniform random. Let $q_i(j)$ denote the probability that we guess that the plaintext bit b is j when the ciphertext bit $c = i$. More formally let z be the random variable representing our guess. Then $q_i(j) = \Pr[z = j | c = i]$, and $q_i(0) + q_i(1) = 1$ for $i = 0, 1$.

   (a) Argue that z and b are independent.

   (b) What is the probability of success with the guessing strategy?

   (c) Show that if b is uniform random then the success probability is always $\frac{1}{2}$ regardless of the guessing strategy, that is, regardless of how we set $q_i(j)$, for $i, j \in \{0,1\}$.

4. Following up on Question 3, suppose we know the plaintext probability distribution p_0 and p_1. What guessing strategy should we adopt to maximize winning probability?