

1. The sampler S takes in three pure random bits r_1, r_2, r_3 and produces three output bits given by

$$y_1 = r_1 + r_2 r_3 \quad y_2 = r_2 + r_3 r_1 \quad y_3 = r_3 + r_1 r_2.$$

- (a) Every output bit is perfectly indistinguishable from random.

Solution: true. When r_2 and r_3 are fixed, r_1 flips between zero and one, so y_1 is unbiased. y_2 and y_3 are identically distributed to y_1 , so they are also unbiased.

- (b) Every two output bits are perfectly indistinguishable from independent random bits.

Solution: false. For example, $y_1 + y_2 = (r_1 + r_2)(1 + r_3)$ is one only when $r_1 + r_2 = 1$ and $r_3 = 0$, namely with probability $1/4$. In contrast a pair of random bits add to zero with probability $1/2$.

2. Eve observes the following four encryptions under the Pseudorandom Function Pad. Recall that encryptions of m have the form $(x, F(x) + m)$ for a random x . F is a PRF with 4 input bits and 4 output bits.

- (a) Assuming Eve knows the messages m_1, m_2, m_3, m_4 , circle the only pair of ciphertexts c_i, c_j that Eve can distinguish from 16 pure random bits.

$$c_1 = (0100, 0000)$$

$$c_2 = (0000, 0100)$$

$$c_3 = (1111, 0000)$$

$$c_4 = (0100, 1111)$$

Solution: c_1 and c_4 both use the same pad $F(0100)$. The encryptions 0000 and 1111 arise from the messages m_1 and m_4 being padded by this value. The sum of the last four bits of c_1 and c_4 will equal $m_1 + m_4$ with probability 1. In a random sequence this event has probability $1/16$ only.

- (b) Circle the only plausible hypothesis among these three alternatives:

$$m_i = 0000, m_j = 0100$$

$$m_i = 0011, m_j = 1100$$

$$m_i = 0100, m_j = 1100.$$

Solution: $m_i + m_j$ evaluate to 0100, 1111, 1000 under the three hypotheses. The only consistent one is the second one.