

Lecture #2 Exercises

Distributed Lab

July 25, 2024



Exercise 1. Suppose that for the given cipher with a security parameter λ , the adversary \mathcal{A} can deduce the least significant bit of the plaintext from the ciphertext. Recall that the advantage of a bit-guessing game is defined as $\text{SSAdv}[\mathcal{A}] = \left| \Pr[b = \hat{b}] - \frac{1}{2} \right|$, where b is the randomly chosen bit of a challenger, while \hat{b} is the adversary's guess. What is the maximal advantage of \mathcal{A} in this case?

Hint: The adversary can choose which messages to send to challenger to further distinguish the plaintexts.

- a) 1
- b) $\frac{1}{2}$
- c) $\frac{1}{4}$
- d) 0
- e) Negligible value ($\text{negl}(\lambda)$).

Exercise 2. Consider the cipher $\mathcal{E} = (E, D)$ with encryption function $E : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{C}$ over the message space \mathcal{M} , ciphertext space \mathcal{C} , and key space \mathcal{K} . We want to define the security that, based on the cipher, the adversary \mathcal{A} cannot restore the message (*security against message recovery*). For that reason, we define the following game:

1. Challenger chooses random $m \xleftarrow{R} \mathcal{M}$, $k \xleftarrow{R} \mathcal{K}$.
2. Challenger computes the ciphertext $c \leftarrow E(k, m)$ and sends to \mathcal{A} .
3. Adversary outputs \hat{m} , and wins if $\hat{m} = m$.

We say that the cipher \mathcal{E} is secure against message recovery if the **message recovery advantage**, denoted as $\text{MRadv}[\mathcal{A}, \mathcal{E}]$ is negligible. Which of the following statements is a valid interpretation of the message recovery advantage?

- a) $\text{MRadv}[\mathcal{A}, \mathcal{E}] := \left| \Pr[m = \hat{m}] - \frac{1}{2} \right|$
- b) $\text{MRadv}[\mathcal{A}, \mathcal{E}] := |\Pr[m = \hat{m}] - 1|$.
- c) $\text{MRadv}[\mathcal{A}, \mathcal{E}] := \Pr[m = \hat{m}]$
- d) $\text{MRadv}[\mathcal{A}, \mathcal{E}] := \left| \Pr[m = \hat{m}] - \frac{1}{|\mathcal{M}|} \right|$

Exercise 3. Suppose that f and g are negligible functions. Which of the following functions is not necessarily negligible?

- a) $f + g$
- b) $f \times g$
- c) $f - g$
- d) f/g
- e) $h(\lambda) := \begin{cases} 1/f(\lambda) & \text{if } 0 < \lambda < 100000 \\ g(\lambda) & \text{if } \lambda \geq 100000 \end{cases}$

Exercise 4. Suppose that $f \in \mathbb{F}_p[x]$ is a d -degree polynomial with d **distinct** roots in \mathbb{F}_p . What is the probability that, when evaluating f at n random points, the polynomial will be zero at all of them?

- a) Exactly $(d/p)^n$.
- b) Strictly less than $(d/p)^n$.
- c) Exactly nd/p .
- d) Exactly d/np .

Exercise 5-6. To demonstrate the idea of Reed-Solomon codes, consider the toy construction. Suppose that our message is a tuple of two elements $a, b \in \mathbb{F}_{13}$. Consider function $f : \mathbb{F}_{13} \rightarrow \mathbb{F}_{13}$, defined as $f(x) = ax + b$, and define the encoding of the message (a, b) as $(a, b) \mapsto (f(0), f(1), f(2), f(3))$.

Question 5. Suppose that you received the encoded message $(3, 5, 6, 9)$. Which number from the encoded message is corrupted?

- a) First element (3).
- b) Second element (5).
- c) Third element (6).
- d) Fourth element (9).
- e) The message is not corrupted.

Question 6. Consider the previous question. Suppose that the original message was (a, b) . Find the value of $a \times b$ (in \mathbb{F}_{13}).

- a) 4
- b) 6
- c) 12
- d) 2
- e) 1