CAS CS 538. Solutions to Problem Set 2

Due electronically via gradescope, Monday February 2, 2026 11:59pm

Useful Definitions

A function is negligible is if goes to zero very quickly. How quickly? Faster than $1/n$, $1/n^2$, $1/n^3$, etc. Formally, we have the following definition.

Definition 1 (Negligible function)**.** A function $f : \mathbb{Z}_{\geqslant 1} \to \mathbb{R}$ is **negligible** if for all integers $c > 0$, we have

$$\lim_{n\to\infty} f(n) \cdot n^c = 0.$$

We will need negligible functions to formalize security (basically, we will want to make sure that the probability of adversarial success is negligible). See Chapter 2.3.1 of Boneh & Shoup textbook.

Definition 2 (Semantic security advantage)**.** For a given cipher $\mathcal{E} = (E, D)$ defined over $(\mathcal{K}, \mathcal{MC})$ and for a given adversary $\mathcal{A}$, we define two experiments, Experiment 0 and Experiment 1. For $b \in \{0, 1\}$, we define Experiment b as follows:

- The adversary computes $m_0, m_1 \in \mathcal{M}$, of the same length, and sends them to the challenger.
- The challenger computs $k \xleftarrow{\text{R}} \mathcal{K}, c \xleftarrow{\text{R}} E(k, m_b)$, and sends c to the adversary.
- The adversary outputs a bit $\hat{b} \in \{0, 1\}$.

For $b \in \{0, 1\}$, let W_b be the event that $\mathcal{A}$ outputs 1 in Experiment b. We define $\mathcal{A}$'s **semantic security advantage** with respect to $\mathcal{E}$ as

$$\mathsf{SSadv}[\mathcal{A}, \mathcal{E}] := \left|\Pr[W_0] - \Pr[W_1]\right|.$$

Definition 3 (Semantic security)**.** A cipher $\mathcal{E}$ is **semantically secure** if for all efficient adversaries $\mathcal{A}$, the value $\mathsf{SSadv}[\mathcal{A}, \mathcal{E}]$ is negligible.

Problems

Problem 1. (15 points)

Show that each of the following functions are negligible:

a) $f(n) + g(n)$, where $f(n)$ and $g(n)$ are both negligible

b) $1000 \cdot f(n)$, where $f(n)$ is negligible

c) $\frac{1}{2^{\sqrt{n}}}$

Solution. For **a**, let $c > 0$ be any positive int. Since $f(n)$ is negligible, by its definition we have:

$$\lim_{n \to \inf} f(n) \cdot n^c = 0$$

The same can be said for $g(n)$ too:

$$\lim_{n \to \inf} g(n) \cdot n^c = 0$$

Using limit properties (property of sums), we can then get:

$$\begin{aligned} \lim_{n \to \infty} [f(n) + g(n)] \cdot n^c &= \lim_{n \to \infty} [f(n) \cdot n^c + g(n) \cdot n^c] \\ &= \lim_{n \to \infty} f(n) \cdot n^c + \lim_{n \to \infty} g(n) \cdot n^c \\ &= 0 + 0 = 0 \end{aligned}$$

Since this holds for any int $c > 0$, this proves that **a** is negligible.

For **b**, let $c > 0$ be any positive int. Like before, $f(n)$ is negligible, so:

$$\lim_{n \to \inf} f(n) \cdot n^c = 0$$

Using limit properties (that of multiples), we then get:

$$\begin{aligned} \lim_{n \to \infty} [1000 \cdot f(n)] \cdot n^c = \lim_{n \to \infty} 1000 \cdot [f(n) \cdot n^c] \\ &= 1000 \cdot \lim_{n \to \infty} f(n) \cdot n^c \\ &= 1000 \cdot 0 = 0 \end{aligned}$$

As it holds for all $c > 0$, this proves **b** is negligible.

For **c**, let $c > 0$ be any positive int. We now need to show that, as n grows, $\frac{1}{2^{\sqrt{n}}}$ will decay into something negligible (so to 0 essentially). Firstly, consider the expression:

$$\frac{1}{2^{\sqrt{n}}} \cdot n^c = \frac{n^c}{2^{\sqrt{n}}}$$

I'll show now how $\lim_{n \to \infty} \frac{n^c}{2^{\sqrt{n}}} = 0$ using limit properties.
Firstly, take the natural log:

$$\ln(\frac{n^c}{2^{\sqrt{n}}}) = \ln(n^c) - \ln(2^{\sqrt{n}}) = c \ln n - \sqrt{n} \ln 2$$

Taking this equation, we can now consider it as a limit as $n \to \infty$:

$$\lim_{n \to \infty} [c \ln n - \sqrt{n} \ln 2] = ???$$

Now looking at this expression, consider *which* term would grow faster consider the circumstances. $c \ln n$, or $\sqrt{n} \ln 2$? Well, the first term is essentially being multipled by a constant, c. The latter term, however, **is the multiple**. Therefore we can assume that the 2nd term will dominate this growth.

$$\lim_{n \to \infty} [c \ln n - \sqrt{n} \ln 2] = -\infty$$

Now we can take this result and plug it back into our original negligible function that we're considering:

$$\begin{aligned} \lim_{n \to \infty} \frac{n^c}{2^{\sqrt{n}}} = \lim_{n \to \infty} e^{\ln(\frac{n^c}{2^{\sqrt{n}}})} \\ &= e^{-\infty} \\ &= 0 \end{aligned}$$

And since this applies for all $c > 0$, this proves **c**.

Problem 2. (30 points)

You're a rising spy working your way up the ranks of national intelligence. One day you are sent a top-secret mission via a mysterious encrypted message. It's a single clue: a three-character airport code for one of the following airports in five possible countries:

USA	**Germany**	**China**	**Brazil**	**India**
BOS	MUC	PEK	GIG	DEL
JFK	FRA	SZX	BSB	BOM
LAX	DUS	PVG	GRU	MAA
DCA	HAM	CAN	CGH	BLR

Unbeknownst to you, a copy of the ciphertext was intercepted by a rival attempting to learn which country you are going to.

Consider the following security game between a challenger and an adversary. Let $\Sigma = (\mathsf{Enc}, \mathsf{Dec})$ be a computational cipher with message space $\mathcal{M}$ equal to the set of 20 airport codes above. The challenger chooses a random plaintext $m \xleftarrow{R} \mathcal{M}$ and key $k \xleftarrow{R} \mathcal{K}$, computes $c \xleftarrow{R} \mathsf{Enc}(k, m)$ and sends c to the adversary. The adversary $\mathcal{A}$ outputs a string s from the following set:

$$\{\texttt{"USA"}, \texttt{"Germany"}, \texttt{"China"}, \texttt{"Brazil"}, \texttt{"India"}\}.$$

Let $\mathsf{Country}(m)$ be a function that outputs the country string in which a given airport code is located. Let W be the event that $s = \mathsf{Country}(m)$, let $p = \Pr[W]$, and define $\mathsf{CountryGuessAdv}[\mathcal{A}, \Sigma] = |p - \frac{1}{5}|$.

Prove that if Σ is a semantically secure cipher (per Section 2.2.2 of the textbook), then for any efficient adversary $\mathcal{A}$, $\mathsf{CountryGuessAdv}[\mathcal{A}, \Sigma]$ is negligible. Notice what this implies: your rival's attempt to learn which country you're travelling to is at most negligibly better than random guessing.

To prove this, use a reduction: supposing there exists an efficient adversary with non-negligible advantage in the country-guessing game, construct an efficient adversary with non-negligible advantage in the semantic security game.

Solution. I'll prove the **contrapositive** here, so: If there exists some efficent adversary $\mathcal{A}$ with a non-negligible advantage, then we can make an efficent adversary $\mathcal{B}$ also with a non-negligible advantage in the semantic security game, contradiction that Σ is secure.

Given $\mathcal{A}$ for the country-guessing game with $\mathsf{CountryGuessAdv}[\mathcal{A}, \Sigma] = \epsilon$, we can make $\mathcal{B}$ for the semantic security game as follows:

- $\mathcal{B}$ will choose 2 distinct countries C_0, C_1 from USA, Germany, China, Brazil, India.
- For each country C_i, $\mathcal{B}$ choose some arbitary airport code m_i from that country.
- $\mathcal{B}$ will then submit m_0, m_1 to the semantic security challenger (*important to note how these codes will have the same length, all codes are 3-characters long.*)
- The challenger chooses $b \twoheadleftarrow 0, 1$, $k \twoheadleftarrow \mathcal{K}$, computs $c \twoheadleftarrow \mathsf{Enc}(k, m_b)$, and then sends c to $\mathcal{B}$.
- $\mathcal{B}$ then sends result c to $\mathcal{A}$ and recieves $\mathcal{A}$'s output $s \in$ "USA", "Germany", "China", "Brazil", "India".
- $\mathcal{B}$ outputs $\hat{b}$ in accordance to the following rule:
  - If $s = \mathsf{Country}(m_0)$, output $\hat{b} = 0$.
  - If $s = \mathsf{Country}(m_1)$, output $\hat{b} = 1$
  - Elser, output rnd $\hat{b} \twoheadleftarrow 0, 1$

Let W_b be the occurance that $\mathcal{B}$ outputs 1 in Experiement b of the semantic security game.

Case 1: $b = 0$ (challenger encrypts m_0)

- This case basically says that $\mathcal{A}$ recieves m_0 as encryption.
- Let $p_0 = \Pr[\mathcal{A}$ outputs $\mathsf{Country}(m_0) \mid$ encryption of $m_0]$.
- Let $p_1 = \Pr[\mathcal{A}$ outputs $\mathsf{Country}(m_1) \mid$ encryption of $m_0]$.
- Then, $\Pr[W_0] = \Pr[\mathcal{B}$ outputs $1 \mid b = 0] = p_1 + \frac{1}{2}(1 - p_0 - p_1)$

Case 2: $b = 1$ (challenger encrpyts m_1)

- In this case, $\mathcal{A}$ insteads gets m_1.
- Let $q_0 = \Pr[\mathcal{A}$ outputs $\mathsf{Country}(m_0) \mid$ encryption of $m_1]$.
- Let $q_1 = \Pr[\mathcal{A}$ outputs $\mathsf{Country}(m_1) \mid$ encryption of $m_1]$.
- Then, $\Pr[W_1] = \Pr[\mathcal{B}$ outputs $1 \mid b = 1] = q_1 + \frac{1}{2}(1 - q_0 - q_1)$.

By the definition of CountryGuessAdv, we know that, overall, $\mathcal{A}$ will guess the correct country with a probability of $\frac{1}{5} + \delta$ for some δ (where $|\delta| = \epsilon$, and we can then also assume that *,in general*, that $\delta > 0$ because otherwise we could just flip $\mathcal{A}$'s output).

When looking at the specific countries C_0, C_1, $\mathcal{A}$ NEEDS to have AT LEAST the avg. adv. Then *in general*, we then assume that $\mathcal{A}$ is AT LEAST as good at distinguishing between C_0, C_1 as between any other pair of countries. We then get:

$$\frac{p_0 + q_1}{2} \geqslant \frac{1}{5} + \frac{\epsilon}{2}$$

This is because, when encryption m_0, $\mathcal{A}$ should output Country(m_0), with a probability of AT LEAST $\frac{1}{5} + \frac{\epsilon}{2}$, and similarily of that for m_1.

Then, the semantic security advantage for $\mathcal{B}$ becomes:

$$\begin{aligned}
\mathsf{SSadv}[\mathcal{B}, \Sigma] &= |\Pr[W_0] - \Pr[W_1]| \\
&= \left| \left(p_1 + \frac{1}{2}(1 - p_0 - p_1) \right) - \left(q_1 + \frac{1}{2}(1 - q_0 - q_1) \right) \right| \\
&= \left| \frac{1}{2}(p_1 - p_0 - p_1 + q_0 + q_1 - q_1) \right| \\
&= \frac{1}{2}|q_0 - p_0|
\end{aligned}$$

Now, since $\mathcal{A}$ has that advantage ϵ overall, and we've chosen the counties where $\mathcal{A}$ performs best, we now have $|q_0 - p_0| \geqslant \frac{\epsilon}{5}$. *Note that the factor comes from the num. of possible counties. This means, worst case, $\mathcal{A}$'s adv. is spread evenly across all country pairs.*

Therefore:

$$\mathsf{SSadv}[\mathcal{B}, \Sigma] \geqslant \frac{\epsilon}{10}$$

Since ϵ is non-negligible by our assumption, $\frac{\epsilon}{10}$ will then also be non-negligible (this is proven from our answer from **1** as well, we can apply limit properties to preserve non-negligibility).

By proving this, we ultimately prove that $\mathcal{B}$ is an efficent adversary.

Problem 3. (30 points) Let Σ be a computational cipher with $|\mathcal{K}| < |\mathcal{M}|$. Construct an adversary $\mathcal{A}$ against Σ such that the running time of $\mathcal{A}$ is very reasonable (in fact, comparable to the running time of Enc and Dec) and $\mathsf{SSadv}[\mathcal{A}, \Sigma] > 0$. Note that it is okay if $\mathsf{SSadv}[\mathcal{A}, \Sigma]$ is very small, as long as it is positive.

You must demonstrate what the adversary does and prove that its SSadv is positive. The adversary should **not** depend on any knowledge about Σ that cannot be efficiently obtained (for example, the adversary doesn't know exact probabilities of different ciphertexts).

Hint: For the adversary design, use the idea from Discussion 2 Problem 2. You can't perform exhaustive search, of course, because you don't have the time; make a random guess instead. Then analyze the probability of outputting 1 in each of the two experiments. This analysis will be different from the one in discussion — go back to your first principles of probability. Conclude that it has non-zero advantage.

This problem justifies why any reasonable definition of semantic security must allow for at least a negligible advantage for $\mathcal{A}$ even when the running time of $\mathcal{A}$ is limited.

Solution. Your solution goes here

Problem 4. (25 points)[Boneh-Shoup Exercise 2.10 from Section 2.6] Let $\Sigma = (\mathsf{Enc}, \mathsf{Dec})$ be a semantically secure cipher defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$, where $\mathcal{M} = \mathcal{C} = \{0,1\}^L$. Which of the following encryption algorithms yields a semantically secure scheme? Either give an attack or provide a security proof via an explicit reduction.

(a) Let Σ_1 be a scheme s.t. $\mathsf{Enc}_1(k, m) := 0||\mathsf{Enc}(k, m)$

Solution. Your solution goes here

(b) Let Σ_2 be a scheme s.t. $\mathsf{Enc}_2(k, m) := \mathsf{Enc}(k, m)||\mathsf{parity}(m)$, where parity of a binary string refers to the number of 1 bits (equivalently, the exclusive-or of all the bits) in the string.

Solution. Your solution goes here