

Problem Set 2

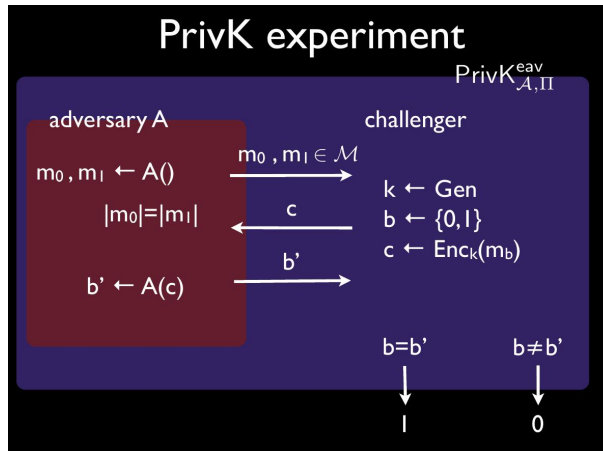


Figure 1: The $\text{PrivK}_{\mathcal{A}, \Pi}^{\text{eav}}$ experiment

Problem 1: The $\text{PrivK}_{\mathcal{A}, \Pi}^{\text{eav}}$ experiment (see Figure 1)

For each of the following scenarios, give the maximal value of $\Pr[\text{PrivK}_{\mathcal{A}, \Pi}^{\text{eav}} = 1]$ and explain how it can be achieved.

- (a) Let Π be the shift cipher, and let us consider an adversary \mathcal{A} that submits $m_0 = \mathbf{a}$ and $m_1 = \mathbf{a}$.
- (b) Let Π be the shift cipher, and let us consider an adversary \mathcal{A} that submits $m_0 = \mathbf{a}$ and $m_1 = \mathbf{b}$.
- (c) Let Π be the shift cipher, and let us consider an adversary \mathcal{A} that submits $m_0 = \mathbf{aa}$ and $m_1 = \mathbf{bb}$.

- (d) Let Π be the shift cipher, and let us consider an adversary \mathcal{A} that submits $m_0 = \mathbf{aa}$ and $m_1 = \mathbf{ab}$.
- (e) Let Π be the one-time-pad encryption of three-letter messages, and let us consider an adversary \mathcal{A} that submits $m_0 = \mathbf{aaa}$ and $m_1 = \mathbf{abc}$.
- (f) Let Π be the monoalphabetic substitution cipher. Give an adversary \mathcal{A} that manages to win the $\text{PrivK}_{\mathcal{A}, \Pi}^{\text{eav}}$ experiment all the time, i.e. such that $\Pr[\text{PrivK}_{\mathcal{A}, \Pi}^{\text{eav}} = 1] = 1$.

Problem 2: Negligible functions

Recall Definition 3.4: A function $f : \mathbb{Z}^+ \rightarrow \mathbb{R}^+$ is called *negligible* if for every positive polynomial $p(n)$ there exists $N \in \mathbb{Z}^+$ such that for all integers $n > N$, it holds that $f(n) < \frac{1}{p(n)}$.

- (a) Example 3.5 states that $f(n) = 2^{-\sqrt{n}}$ is negligible. For the polynomial $p(n) = 16n^4$, give a possible N as in the definition above, i.e. such that for all integers $n > N$, it holds that $f(n) < \frac{1}{p(n)}$.
- (b) Example 3.5 states that $f(n) = n^{-\log n}$ is negligible. For the polynomial $p(n) = 16n^4$, give a possible N as in the definition above, i.e. such that for all integers $n > N$, it holds that $f(n) < \frac{1}{p(n)}$.
- ★ Let negl_1 and negl_2 be negligible functions. Prove that the function negl_3 defined by $\text{negl}_3(n) = \text{negl}_1(n) + \text{negl}_2(n)$ is negligible.
- ★ For any positive polynomial p , the function negl_4 defined by $\text{negl}_4(n) = p(n) \cdot \text{negl}_1(n)$ is negligible.

Problem 3: not PRGs

For all of the following constructions, explain why they are not PRGs. Can you give an explicit description of an efficient distinguisher in each case?

- (a) Let $G(s)$ output s .
- (b) Let $G(s)$ output $s||s$
- (c) Let $G(s)$ output $s||\bigoplus_{i=1}^n s_i$.

See https://colab.research.google.com/drive/1s3ZOM35nJKWv_PGnYGH87rtVP2-QA0qa for programming versions of this exercise which might help your understanding.

Problem 4: Basic properties of PRGs

Recall that the *image of a function* $f : A \rightarrow B$ is the subset $f(A)$ of B . Formally,

$$\text{im}(f) := f(A) = \{b \in B \mid \exists a \in A \text{ such that } b = f(a)\}.$$

Let $G : \{0, 1\}^n \rightarrow \{0, 1\}^{2n}$ be a PRG.

- (a) Let us assume that G is *injective*. How many different $2n$ -bit strings y are there in the image of G ?
- (b) What is the fraction of images of G among all $2n$ -bit strings?
- (c) For a given $y \in \{0, 1\}^{2n}$, what is $\Pr_{s \leftarrow \{0, 1\}^n}[G(s) = y]$? Express this probability in terms of $|\{s \in \{0, 1\}^n \mid G(s) = y\}|$ and n .

Problem 5: Exercise 3.5 from [KL]

Let $|G(s)| = \ell(|s|)$ for some ℓ . Consider the following experiment:

The PRG indistinguishability experiment $\text{PRG}_{A,G}(n)$, see also Figure 2:

- (a) A uniform bit $b \in \{0, 1\}$ is chosen. If $b = 0$ then choose a uniform $r \leftarrow \{0, 1\}^{\ell(n)}$ and set $w := r$; if $b = 1$ then choose a uniform $s \leftarrow \{0, 1\}^n$ and set $w := G(s)$.
- (b) The adversary \mathcal{A} is given w , and outputs a bit b' .

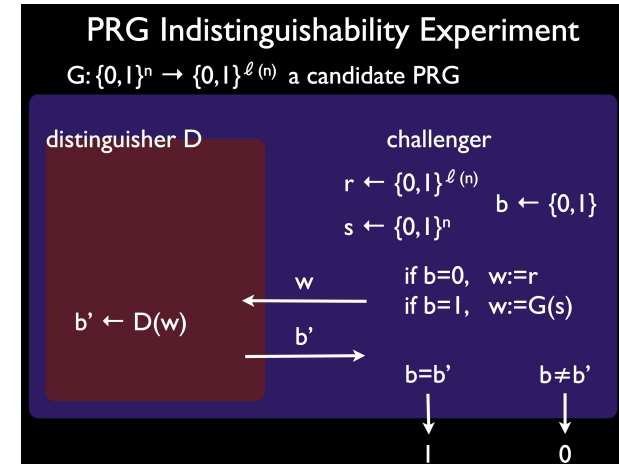


Figure 2: The $\text{PRG}_{D,G}$ experiment

- (c) The output of the experiment is defined to be 1 if $b' = b$, and 0 otherwise.

Provide a definition of a pseudorandom generator based on this experiment, and prove that your definition is equivalent to Definition 3.14. (That is, show that G satisfies your definition if and only if it satisfies Definition 3.14.)

Hint: For proving the equivalence of the two definitions, argue why the following equalities hold

$$\begin{aligned} \Pr[\text{PRG}_{A,G}(n) = 1] &= \Pr[b = 0] \cdot \Pr[D(w) = 0 | b = 0] + \Pr[b = 1] \cdot \Pr[D(w) = 1 | b = 1] \\ &= \Pr[b = 0] \cdot \Pr[D(r) = 0] + \Pr[b = 1] \cdot \Pr[D(G(s)) = 1] \\ &= \frac{1}{2} \Pr[D(r) = 0] + \frac{1}{2} \Pr[D(G(s)) = 1] \\ &= \frac{1}{2} (1 - \Pr[D(r) = 1]) + \frac{1}{2} \Pr[D(G(s)) = 1] \\ &= \frac{1}{2} + \frac{1}{2} (\Pr[D(G(s)) = 1] - \Pr[D(r) = 1]) \end{aligned}$$

and use them in your proof.

Problem 6: Exercise 3.2 from [KL]

Prove that Definition 3.8 cannot be satisfied if Π can encrypt arbitrary-length messages and the adversary is not restricted to output equal-length messages in experiment $\text{PrivK}_{\mathcal{A}, \Pi}^{\text{eav}}$.

Hint: Let $q(n)$ be a polynomial upper-bound on the length of the cipher-text when Π is used to encrypt a single bit. Then consider an adversary who outputs $m_0 \in \{0, 1\}$ and a uniform $m_1 \in \{0, 1\}^{q(n)+2}$. How many possible m_1 's can have ciphertexts of length at most $q(n)$ if the encryption scheme is perfectly correct (i.e. it never fails to decrypt)?

★ Problem 7: Exercise 3.4 from [KL]

Prove the equivalence of Definition 3.8 and Definition 3.9 from the book [KL].

★ Problem 8: Exercise 3.7 from [KL]

Prove the converse of Theorem 3.18. Namely, show that if G is not a pseudorandom generator then Construction 3.17 does not have indistinguishable encryptions in the presence of an eavesdropper.