CS 4501-Cryptography, Homework 2

Response by: Your Name, (computing id)

Total points: 30. Points are noted after each problem.

Directions. For each problem, typeset your solution in the `answer` environment, and if there are sub-problems, mark them clearly. Feel free to use as much space as you want to. Before you submit the PDF, update 1) "Your Name" and id on the above, and 2) the "Acknowledgement" box at the last page properly.

Policies. We re-iterate our policy. It is encouraged to think and discuss the problems before looking for ready-made solutions. You shall acknowledge and/or reference any discussion and published material except for lecture notes and resources of LaTeX. In any case, it is a violation if any of the following cases happens:

- You copied text directly (from any source).
- You used any material or discussion without acknowledgement or citation.
- You are unable to explain your work orally.

This homework reviews some concepts, including negligible, computational indistinguishability, and PRG. Problems 2 and 3 are facts in probability that will be used later in the course.

Problem 1 (Negligible functions, 1pt each)**.** True or False. Please provide a one-sentence explanation. All the functions below are defined over $n \in \mathbb{N}$.

(a) $2^{-n/4}$ is a negligible function.

(b) $2^{-100 \log n}$ is a negligible function.

(c) For any polynomial $a(n) \geq n$, $\left(1 - \frac{1}{a(n)}\right)^{a(n) \cdot n}$ is a negligible function.

(d) For any polynomial $a(n) \geq n$ and for any negligible function $\epsilon(n)$, $a(n) \cdot \epsilon(n)$ is a negligible function.

Answer.

(a)

(b)

(c)

(d)

□

Problem 2 (Majority of random variables, 5pt each)**.** Let $\alpha > 0$ be a constant. Consider fixed strings x, y and a probabilistic polynomial-time algorithm A such that

$$\Pr_r[A(y; r) = x] \geq 1/2 + \alpha.$$

That is, $A(y)$ outputs x with probability at least $1/2 + \alpha$, where the probability is taken over the uniform random tape r used by A. Assume without loss of generality, the length of random tape $|r| = \ell(n)$ for some polynomial ℓ and $n := |y|$ is the input length. We want to amplify the probability of obtaining x by repeatedly running A using different random tapes. Consider the following procedure:

1. Let $r_1, r_2, ..., r_t$ be t random tapes for some fixed t; see below for the distribution of the random tapes.
2. Compute $z_i \leftarrow A(y; r_i)$ for all $i = 1, ..., t$ (thus z_i is a random variable depends on r_i).
3. Let z be the majority in the sequence $(z_1, ..., z_t)$ (that is, z is the string that appeared the maximal number of times in the sequence, and we break tie arbitrarily).

We sample the random tapes $(r_1, r_2, ..., r_t)$ from different distributions below, and then you are asked to provide an upper bound on the failure probability.

(a) Sample the random tapes independently and uniformly, i.e., $r_i \leftarrow \{0,1\}^\ell$ for all $i \in [t]$. Find an upper bound on $\Pr[z \neq x]$ using Chernoff's inequality (as a function of α, t).

(b) Sample the t random tapes $(r_1, r_2, ..., r_t)$ uniformly but only *pairwise independent*. Find an upper bound on $\Pr[z \neq x]$ using Chebyshev's inequality (as a function of α, t).

Remark: Notice that we can sample the pairwise independent random tapes using only $\ell \cdot \log t$ uniformly random bits, but the fully independent tapes take $\ell \cdot t$ uniformly random bits. The pairwise independence approach can be more efficient in utilizing randomness.

Answer.

(a)

(b)

□

Problem 3 (Statistically close distributions, 4pt)**.** For random variables X and Y taking values in U, their statistical difference (also known as variation distance) is

$$\Delta(X, Y) := \max_{T \subset U} |\Pr[X \in T] - \Pr[Y \in T]|.$$

Let $\mathcal{X} = \{X_1, X_2, ...\}$ and $\mathcal{Y} = \{Y_1, Y_2, ...\}$ be two ensembles of distributions. Suppose that there exists a function $\epsilon(n)$ such that for all $n \in \mathbb{N}$, $\Delta(X_n, Y_n) \leq \epsilon(n)$. Prove that for any deterministic algorithm D, for all $n \in \mathbb{N}$,

$$\left| \Pr_{t \leftarrow X_n}[D(t) = 1] - \Pr_{t \leftarrow Y_n}[D(t) = 1] \right| \leq \epsilon(n).$$

Remark: we say $\mathcal{X}$ and $\mathcal{Y}$ are *statistically close* iff ϵ is negligible. This proves that statistically close ensembles are always indistinguishable for even (non-uniform probabilistic) unbounded-time D.

Answer.

□

Problem 4 (Encrypting two messages, 4pt)**.** Suppose $g : \{0,1\}^n \to \{0,1\}^{2\ell(n)}$ for all $n \in \mathbb{N}$ is a PRG, where $\ell(\cdot)$ is a polynomial in n (e.g., think $\ell(n) := 100n$). We construct an encryption that encrypts two messages as below.

- $\mathsf{Gen}(1^n)$: outputs $s \leftarrow \{0,1\}^n$.
- $\mathsf{Enc}_{s,t}(m)$: given $m \in \{0,1\}^\ell$, output $c := m \oplus g(s)[1, ..., \ell]$ if $t = 1$, or output $c := m \oplus g(s)[\ell + 1, ..., 2\ell]$ if $t = 2$, where t denotes the first or the second message, and $g(s)[i, ..., j]$ denotes the string from the i-th to the j-th bit of $g(s)$.
- $\mathsf{Dec}_{s,t}(c)$: given $c \in \{0,1\}^\ell$, output $m := c \oplus g(s)[1 + (t-1)\ell, ..., t\ell]$ for $t = 1, 2$.

Is this a secure encryption? We require that even when the adversary knows the first message $(m', \mathsf{Enc}_{s,1}(m'))$, the second message m remains secure given the ciphertext $\mathsf{Enc}_{s,2}(m)$. Formally, we define the two-message security as follows: for all $m', m_0, m_1 \in \{0,1\}^\ell$, the following two ensembles are computationally indistinguishable,

$$\{m', \mathsf{Enc}_{s,1}(m'), \mathsf{Enc}_{s,2}(m_0)\}_{n\in\mathbb{N}} \approx \{m', \mathsf{Enc}_{s,1}(m'), \mathsf{Enc}_{s,2}(m_1)\}_{n\in\mathbb{N}},$$

where s is the random variable sampled by $s \leftarrow \mathsf{Gen}(1^n)$. Prove that the scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ satisfies the two-message security by a reduction from g is PRG.

Answer.

□

Problem 5 (PRG, 2pt each)**.** Let g be a pseudorandom generator. In each of the following cases, prove that g' is also a pseudorandom generator.

(a) Define $g'(s) := g(\bar{s})$, where $\bar{s}$ is the (bitwise) complement of s.

(b) Define $g'(s) := \overline{g(s)}$.

(c) Define $g'(s_1 \| s_2) := g(s_1) \| s_2$, where $|s_2| = 2$ is the 2-bit suffix of the input to g'.

Answer.

(a)

(b)

(c)

□

Problem 6 (PRG expansion, 2pt)**.** Suppose $g : \{0,1\}^n \to \{0,1\}^{n+1}$ for all $n \in \mathbb{N}$ is a PRG. Define $h : \{0,1\}^n \to \{0,1\}^{2n+4}$ to be the following:

$$h(s) := g(s\|0)\|g(s\|1).$$

Clearly, h is expanding much faster than g (since $\frac{2n+4}{n} > \frac{n+1}{n}$). Is h a PRG? Provide a counterexample such that g is PRG but the resulting h is not.

Answer. □

Acknowledgement

Replace this with your collaborators and resources like below (if you did not have any, replace this with *None*).

Problem 1 is inspired by a discussion with Jonathan, who explained Extended Euclidean Algorithm to me.

Problem 5: I used ChatGPT with the prompt "teach me DMT2" and obtained XXX.