CS 4501-Cryptography, Homework 3

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 the concepts of PRF and OWFs, but we also show an elementary proof on the number of primes. Notice that PRF is very different from OWF when they are evaluated more than once, as considered in Problems 3 and 4.

Problem 1 (6pt, 1pt each)**.** This problem will prove the Chebyshev's bound on $\pi(n)$, that is, for all $n > 1$,

$$\pi(n) \geq \frac{n}{2 \log n}, \tag{1}$$

where log is base 2.

(a) For any $n > 1, n \in \mathbb{N}$, let $N := \binom{2n}{n}$. Show that $N > 2^n$.

(b) For any $m \in \mathbb{N}$, consider the prime factorization of the factorial $m!$, which can be written as

$$m! = \prod_{p \text{ prime}} p^{\nu_p(m!)},$$

where $\nu_p(x) \in \mathbb{N}$ denotes the maximal power of p such that $p^{\nu_p(x)}$ divides x. Show that for any p, it holds that $\nu_p(m!) = \sum_{j=1,2,\ldots} \lfloor m/p^j \rfloor$.

(c) Take log on both sides of (a), and then show that

$$\sum_{p \text{ prime}} (\nu_p((2n)!) - 2\nu_p(n!)) \cdot \log p = \sum_{\text{prime } p<2n} (\nu_p((2n)!) - 2\nu_p(n!)) \cdot \log p > n \tag{2}$$

(d) Show that for any prime p, any $n > 1$,

$$\nu_p((2n)!) - 2\nu_p(n!) \leq \log_p(2n) = \frac{\log(2n)}{\log p}.$$

(e) Plug (d) into Equation (2) and then show that $\pi(2n) \cdot \log(2n) > n$, and thus Equation (1) holds for all even n.

(f) Show Equation (1) holds for all odd $n > 1$.

Answer.

(a)

(b)

(c)

(d)

(e)

(f)

□

Problem 2 (4pt)**.** Prove *unconditionally* the existence of a pseudorandom function

$$F = \left\{ f_s : \{0,1\}^{\log n} \to \{0,1\} \text{ such that } s \leftarrow \{0,1\}^n \right\}_{n \in \mathbb{N}}.$$

Notice that by unconditional, we mean the function is indistinguishable even for unbounded (including exponential time) algorithms, and it is sometimes called statistically secure. [KL, Exercise 3.10]

Answer. □

Problem 3 (3pt each)**.** Let $F = \{f_s : \{0,1\}^n \to \{0,1\}^n \mid s \in \{0,1\}^n\}_{n \in \mathbb{N}}$ be a length preserving pseudorandom function. For the following constructions of a keyed function f'_s, state whether $F' = \{f'_s : \{0,1\}^{n-1} \to \{0,1\}^{2n} \mid s \in \{0,1\}^n\}_{n \in \mathbb{N}}$ is a pseudorandom function. If yes, prove it; if not, show an attack. [KL, Exercise 3.11]

(a) $f'_s(x) := f_s(0\|x)\|f_s(0\|x)$.

(b) $f'_s(x) := f_s(0\|x)\|f_s(1\|x)$.

(c) $f'_s(x) := f_s(0\|x)\|f_s(x\|0)$.

(d) $f'_s(x) := f_s(0\|x)\|f_s(x\|1)$.

Answer.

(a)

(b)

(c)

(d)

□

Problem 4 (2pt each)**.** Suppose that $f : \{0,1\}^n \to \{0,1\}^{l(n)}$ for all $n \in \mathbb{N}$ is a OWF. This problem will step-by-step prove that $g : \{0,1\}^n \to \{0,1\}^{2l(n)}$ for all $n \in \mathbb{N}$ constructed below is also a OWF. The construction of g is:

$$g(x) := f(x) \| f(x),$$

where $\|$ is the concatenation of strings.

(a) Argue that g is an easy-to-compute function.

(b) Write the statement of "assume for contradiction, g is easy to invert" that is formally quantified by some probability $1/p(n)$ for some polynomial p; in this statement, denote A as the adversarial algorithm.

(c) Write an algorithm $B(1^n, z)$ such that (i) B takes as input z sampled by $x \leftarrow \{0,1\}^n, z \leftarrow f(x)$, and then (ii) B runs A as a subroutine. argue that B is NUPPT.

(d) Argue that B from the previous step inverts f with non-negligible probability, that is, there exists a polynomial q (as a function of n and $p(n)$) such that for infinitely many $n \in \mathbb{N}$,

$$\Pr[x \leftarrow \{0,1\}^n, z \leftarrow f(x) : f(B(1^n, z)) = z] \geq 1/q(n),$$

which contradicts that f is a OWF and completes this reduction.

Answer.

(a)

(b)

(c)

(d)

□

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.