CS 355: Topics in Cryptography **Spring 2026**

Problem Set 1

Due: Friday, 10 April 2026 (submit via Gradescope)

Instructions: You **must** typeset your solution in LaTeX using the provided template:

https://cs355.stanford.edu/homework.tex

Submission Instructions: You must submit your problem set via Gradescope. Please use course code **X85KN6** to sign up. Note that Gradescope requires that the solution to each problem starts on a **new page**.

Bugs: We make mistakes! If it looks like there might be a mistake in the statement of a problem, please ask a clarifying question on Ed.

Problem 1: A Special PRF [10 points]. One can show that $F(k,x) = H(x)^k$ is a PRF, if H is modeled as a random oracle to a group where the discrete logarithm problem is hard (We will discuss the random oracle model in Lecture 4, but you do not need to know what they are for this problem). This PRF has many special properties. In this problem, we will explore two applications of this PRF.

(a) Let $F : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$ be a PRF defined over groups $(\mathcal{K}, +)$ and $(\mathcal{Y}, \otimes)$, where $+$ and $\otimes$ are the respective group operations in those groups. We say F is *key-homomorphic* if it holds that

$$F(k_1 + k_2, x) = F(k_1, x) \otimes F(k_2, x).$$

Let us consider a PRF defined over $(\mathcal{K} = \mathbb{Z}_p, +)$ with group operation addition and $(\mathcal{Y} = G, \otimes)$ where G is a group of prime order p. Is the PRF $F(k,x) = H(x)^k$ defined with a random oracle $H : \mathcal{X} \to G$ a key-homomorphic PRF? Please prove your answer one way or the other (you only need to prove key-homomorphism, and do not need to prove whether it is a secure PRF).

(b) *Key rotation* is a common problem encountered in cloud storage: how to change the key under which data is encrypted without sending the keys to the storage provider? A naive solution is to download the encrypted data, decrypt it, re-encrypt it under a new key, and re-upload the new ciphertext. We will now see how this process can be made more efficient with a key-homomorphic PRF.

Suppose you have a ciphertext c made up of blocks $c_1, ..., c_N$ that corresponds to a message $m = (m_1, ..., m_N)$ encrypted under a key k_1 using a key-homomorphic PRF F in counter mode, i.e., $c_i = m_i \otimes F(k_1, i)$. Now you want to rotate to a key k_2. It turns out you can send the storage provider a single element $k_{\mathsf{update}} \in \mathcal{K}$ which it can then use to generate c', an encryption of m under k_2. Please tell us how you can compute k_{update} and how the storage provider can use k_{update} and c to compute c'. Prove that your protocol is correct (you need not prove security).

(c) An *oblivious PRF* is an interactive protocol between a client who holds a message x and a server who holds a key k. The protocol allows the client to learn the PRF evaluation $F(k,x)$ without the server learning anything about x. Oblivious PRFs are used in many advanced crypto protocols.

It turns out that there is an oblivious PRF protocol for the PRF $F(k,x) = H(x)^k$. Please show us how a client holding x and a server holding k can interact so that the client learns $H(x)^k$ while the server learns nothing about x. Prove that your protocol is correct (you need not prove security).

Problem 2: True/False [7 points]. Note: Please give a short explanation with your answers.

(a) Which of the following are true in a world where P = NP.

i Secure PRFs exist in the standard model.

ii Secure PRFs exist in the random oracle model.

iii The one-time-pad cipher is secure.

(b) If there exists a PRG with 1-bit stretch, there exists a PRG with n^{800}-bit stretch (where n is the length of the PRG seed).

(c) Let $F\colon \mathcal{K} \times \mathcal{X} \to \mathcal{X}$ be a pseudorandom permutation. Then:

i $f_{k=0}(x) := F(0,x)$ is (always) a one way function.

ii $f_{k=0}(x) := F(0,x)$ is (always) a one way permutation.

iii $f_{x=0}(k) := F(k,0)$ is (always) a one way permutation.

Problem 3: Key Leakage in PRFs [5 points]. Let F be a secure PRF defined over $(\mathcal{K},\mathcal{X},\mathcal{Y})$, where $\mathcal{K} = \mathcal{X} = \mathcal{Y} = \{0,1\}^n$. Let $\mathcal{K}_1 = \{0,1\}^{n+1}$. Construct a new PRF F_1, defined over $(\mathcal{K}_1,\mathcal{X},\mathcal{Y})$, with the following property: the PRF F_1 is secure; however, if the adversary learns the last bit of the key then the PRF is no longer secure. Prove that F_1 indeed has both of these properties. This shows that leaking even a *single* bit of the secret key can completely destroy the PRF security property.
[**Hint:** Try changing the value of F at a single point.]

Problem 4: Composition [10 points]. Determine whether each of the following statements is TRUE or FALSE. For the first two statements, prove that your answer is correct. That is, give a security proof or describe an adversary and prove it has high advantage.

Let $F(k,x) \to y$ be a PRF, and $f(x) \to y$ be a OWF, and let $G(s) \to r$ be a PRG. Assume that the PRF outputs fixed-length bit-strings.

1. The function $F_1(k,(x_1,x_2)) = F(k,x_1) \oplus F(k,x_2)$ is a PRF
2. The function $F_2((k_1,k_2),x) = F(k_1,x) \oplus F(k_2,x)$ is a PRF
3. The function $G_3(s) = (G(s),G(s))$ is a PRG
4. The function $G_4((s_1,s_2)) = (s_1,G(s_2))$ is a PRG (where $s_1,s_2 \in \mathcal{S}$: the seed space for G)
5. The function $f_5((x_1,x_2)) = (f(x_1),f(x_2))$ is a OWF

Problem 5: Time Spent [1 point for answering]. How long did you spend on this problem set? This is for calibration purposes, and the response you provide will not affect your score.

Optional Feedback [0 points]. Please answer the following questions to help us design future problem sets. You do not need to answer these questions, and if you would prefer to answer anonymously, please use this form. However, we do encourage you to provide us feedback on how to improve the course experience.

(a) What was your favorite problem on this problem set? Why?

(b) What was your least favorite problem on this problem set? Why?

(c) Do you have any other feedback for this problem set?

(d) Do you have any other feedback on the course so far?