# Fundamentals of Cryptography: Midterm

Wednesday Nov 6, 3-6PM

**Problem 1 (1pt)** Complete the definition of polynomial growth. For a functions $f : \mathbb{N} \to \mathbb{R}^+$. We say $f(n) = \text{poly}(n)$ if ____fill the blank____.

**Problem 2 (1pt)** Complete the definition of negligible functions. A function $f : \mathbb{N} \to \mathbb{R}^+$ is *negligible*, if ____fill the blank____.

**Problem 3 (2pt)** Complete the definition of CCA (i.e. CCA2) security. An encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is CCA2 secure if for any p.p.t. adversary $\mathcal{A}$, the adversary wins the following game with at most $1/2 + \text{negl}(\lambda)$ probability:

- The challenger samples key $k \leftarrow \mathsf{Gen}(1^\lambda)$.
- During the game, the adversary is always allowed to query the challenger for up to $\text{poly}(\lambda)$ times ____fill the blank (Describe the interaction.)____.
- $\mathcal{A}$ chooses two message $m_0, m_1$ of the same length, and sends them to the challenger.
- The challenger samples $b \in \{0,1\}$ and sends $c \leftarrow \mathsf{Enc}(k, m_b)$ to $\mathcal{A}$.
- The adversary outputs $b'$. It wins if $b' = b$.

**Problem 4 (2pt)** The assumption that PRGs exist is known to be equivalent to the assumption that _choose all correct answers_

(a) OWFs exist; (b) CRHFs exist; (c) PRFs and PRPs exist; (d) $P \neq NP$.

**Problem 5 (2pt)** Sort the following security definitions, from weakest to strongest.

(a) Authenticated Encryption; (b) CPA-security; (c) CCA-security;
(d) indistinguishable encryptions in the presence of an eavesdropper.

**Problem 6 (3pt)** Let $g : \{0,1\}^\lambda \to \{0,1\}^{\lambda+1}$ be a PRG. We can construct a length-doubling PRG $g' : \{0,1\}^\lambda \to \{0,1\}^{2\lambda}$ as

$g'(x^0)$ takes $x^0 \in \{0,1\}^\lambda$ as input;
For $i = 1, \ldots, \lambda$, computes $y_i \| x^i = g(x^{i-1})$, where $y_i \in \{0,1\}$ and $x^i \in \{0,1\}^\lambda$;
Outputs $y_1 \| y_2 \| \ldots \| y_\lambda \| x^\lambda$.

No p.p.t. distinguisher can distinguish between $g'(s)$ (when $s \leftarrow \{0,1\}^\lambda$) and a random $2\lambda$-bit string with non-negligible probability. We proved $g'$ is a PRG using hybrid argument.

State the hybrid worlds or hybrid distributions that are used in the proof.

Choose any 4 of the following problems (problem 7,8,9,10,11) to solve.

**Problem 7 (5pt)** Let $F : \{0,1\}^\lambda \times \{0,1\}^\lambda \to \{0,1\}^\lambda$ be a PRF. Define $F'$ as

$$F'(k, x) = F(1 \| k_{2:\lambda}, x).$$

In other words, $F'$ enforces the first bit of the key to be 1. Is $F'$ a PRF?

If the answer is negative, explicitly present a counter-example. If the answer is affirmative, explicitly state the reduction. In either case, you don't need to prove in detail why the counter-example or the reduction works.

**Problem 8 (5pt)** Design a PRF $F : \{0,1\}^\lambda \times \{0,1\}^{n(\lambda)} \to \{0,1\}$ such that there is a polynomial-time algorithm $\mathsf{psum}$ for computing

$$\mathrm{psum}(k, t) = \bigoplus_{i=0}^{t} F(k, i).$$

(The input $x \in \{0,1\}^{n(\lambda)}$ can be interpreted as a number in $\{0, 1, \ldots, 2^n - 1\}$.)

You can use any tool that is implied by OWF/OWP/CRHF in your construction.

**Problem 9 (5pt)** Let $\mathrm{Fstl}((k_1, k_2, k_3), (x_0, x_1)) = (x_3, x_4)$ be the 3-round Feistel network (illustrated in Figure 1). Prove that Fstl is a PRP if $H$ is difference unpredictable function (DUF) and $F$ is a PRF.

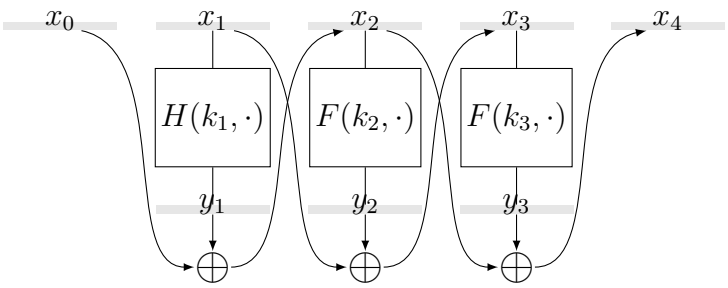


Figure 1: 3-round Feistel Network

We say $H$ is a DUF, if for any distinct $m_0, m_1$ and for any $\delta$

$$\Pr_{k \leftarrow \mathcal{K}}[H(k, m_0) \oplus H(k, m_1) = \delta] \leq \mathrm{negl}(\lambda).$$

**Problem 10 (5pt)** There are two encryption schemes $\Pi_A = (\mathsf{Gen}_A, \mathsf{Enc}_A, \mathsf{Dec}_A)$ and $\Pi_B = (\mathsf{Gen}_B, \mathsf{Enc}_B, \mathsf{Dec}_B)$. Both of them satisfies correctness, at least one of them is CPA-secure. Construct a CPA-secure encryption scheme $\Pi$ by making black-box use of $\Pi_A, \Pi_B$ without knowing which one is CPA-secure.

The construction and the reduction must be explicitly stated. If you use the hybrid argument, the hybrid distributions or the hybrid worlds must be explicitly stated. You may get partial credits by writing down informal proofs or providing proof intuitions.

**Problem 11 (5pt)** In this problem, we construct *constrained PRFs*, which is a generalization of puncturable PRFs.

A constrain is a predicate $c : \{0,1\}^n \to \{0,1\}$. In this problem, we only consider bit-fixing constrains. Each bit-fixing constrain $c$ can be viewed as a vector $c \in \{0,1,?\}^n$. Say say $x$ satisfies constrain $c$, denoted by $c(x) = 1$, if and only if for all $1 \le i \le n$, $c_i \in \{?, x_i\}$. In other words, there is no constrain on $x_i$ if $c_i = ?$.

We say a PRF $f$ is a constrained PRF for bit-fixing constrains, if given the key $k$ and a bit-fixing constrain $c$ one can compute a constrained key $k_c$. Say the constrained key $k_c$ is given to the adversary, then the adversary can compute $f(k,x)$ if $c(x) = 1$, but $f(k,x)$ is hidden from the adversary if $c(x) = 0$.

Formally, a PRF $F : \{0,1\}^\lambda \times \{0,1\}^{n(\lambda)} \to \{0,1\}$ is called a *constrained PRF* for for bit-fixing constrains, if

- There is an efficient algorithm $\mathsf{constrain}$, which takes a key, a bit-fixing *constrain* $c$, and outputs a constrained key $k_c$.
- There is an efficient algorithm $\mathsf{eval}$, which takes a constrained key, an input, and evaluate the PRF on that input. For any constrain $c$ and for any input $x$ that $c(x) = 1$, we have $\mathsf{eval}(k_c, x) = f(k,x)$ as long as $k_c \leftarrow \mathsf{constrain}(k,c)$.
- No PPT adversary $\mathcal{A}$ can distinguish the real world from the ideal world in the following game with better than negligible advantage.
  1. The adversary $\mathcal{D}$ is given input $1^n$, and outputs a bit-fixing constrain $c$.
  2. Sample a random key $k \leftarrow \{0,1\}^\lambda$, compute the constrained key $k_c \leftarrow \mathsf{constrain}(k,c)$, give $k_c$ to the adversary.
  3. The adversary can make oracle query to
     - in the real world: $f(k,\cdot)$, or
     - in the ideal world: $F(\cdot)$, where $F : \{0,1\}^n \to \{0,1\}$ is a random function

     on any input $x$ not satisfying the constrain $c$.
  4. Eventually, the adversary should guess which world it is in.

Your task is to construct a constrained PRF. You can use any tool that is implied by OWF/OWP/CRHF in your construction. Explicitly state the construction. The proof can be informal unless it is highly non-trivial.