NYU COMPUTER SCIENCE FALL 2026

Introduction to Cryptography

CSCI-GA.3210-001 Instructor: Nir Bitansky

Problem Set 4

Due: November 11, 2026

Instructions:

- Turn in your solutions in LaTeX and submit a PDF through Gradescope.
  (You don't have to know latex, can use AI tools like Prism.)
- Solutions will be graded for both correctness and clarity. If you do not know how to solve a question, you may write "I don't know how to do this" to receive 15% credit for that question.
- Discussion with peers is strongly encouraged, but you must write up your solutions on your own and list your discussion partners. Cite any external sources you use.
- AI use is permitted. If you use AI to solve the homework, list the exact model as a collaborator and include your prompts in an appendix. We strongly recommend solving the questions yourself: the final exam will mostly contain variants of homework questions.
- Use the course forum for clarification questions, but do not post solutions there.

1. Let $(Auth, Ver)$ be a MAC, and assume $Auth$ is deterministic (i.e., it does not toss any coins on its own) and that for secret key of size n it produces tags of size n.

   (a) (20 pts) Consider the function $G : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^{3n}$ defined as:

   $$G(sk, r) = r, \langle Auth_{sk}(1), r\rangle, \langle Auth_{sk}(11), r\rangle, \ldots, \langle Auth_{sk}(1^{2n}), r\rangle \ ,$$

   where $\langle \cdot, \cdot \rangle$ denotes inner product modulo 2. Show that G is a PRG.

   (b) (5 pts) Consider the function $G : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^{3n+1}$ defined as:

   $$G(sk, r) = r, \langle Auth_{sk}(r), r\rangle, \langle Auth_{sk}(1), r\rangle, \langle Auth_{sk}(11), r\rangle, \ldots, \langle Auth_{sk}(1^{2n}), r\rangle \ .$$

   Prove that this function is also a PRG, or give a counter example.

2. (20 pts) Let H be a collision-resistant hash family with keys $hk \in \{0,1\}^n$ and $H_{hk} : \{0,1\}^{2n} \to \{0,1\}^n$. Define

   $$f(hk, x) := (hk, H_{hk}(x)) \ .$$

   Show that f is a one-way function.

3. Let H be a collision-resistant hash function that for a key $hk \in \{0,1\}^n$ maps $\{0,1\}^{2n}$ to $\{0,1\}^n$. We would like to use H to construct a new collision-resistant H^* for inputs of arbitrary length. We first focus on inputs whose length is a power of two, 2^ℓ for some ℓ. We consider the following construction (known as *Merkle's tree hash*).

   Given a key hk for H, and an input x of length 2^ℓ, consider the following labeling $\{L_v\}_v$ of the binary tree of depth ℓ whose nodes are represented by $\{v \in \{0,1\}^i, i \in \{0, \ldots, \ell\}\}$:

- For every leaf $v \in \{0,1\}^\ell$, $L_v := x_v 0^{n-1}$ (the vth bit of x padded).
- For every intermediate node, $L_v = H_{hk}(L_{v0} L_{v_1})$ (the hash of its children).

The hash $H^*_{hk}(x)$ is then set to be the root label L_ε.

(a) (15 pts) Show that H^* is also collision resistant in the sense that it is hard to find two inputs $x \neq x'$ of *the same* length 2^ℓ, which collide under H^*_{hk}.

(b) (5 pts) Briefly explain how to extend H^* to inputs of any size (not necessarily a power of two), and so that it is hard to find collisions $x \neq x'$ also for inputs that are not of the same length. No need to prove.

4. In this question, we will understand the relations between the different security notions of encryption. In what follows, let (G, E, D) be an encryption scheme. To present the definitions in a way that applies to both the secret and the public settings we shall agree that $G(1^n)$ outputs three keys (sk, ek, pk):

   - sk is the secret decryption key.
   - ek is an encryption key.
   - pk is a public key.
   - In the secret key setting, $ek = sk$ and pk is empty, whereas in the public-key setting $ek = pk$.

   We consider the following security notions:

   Known Plaintext Attacks: The scheme is t-message KPA-secure, for a polynomially bounded function t, if any n.u. PPT adverasry $A = \{A_n\}$ wins the following game with probability at most $1/2 + \mu(n)$ for some negligible μ.

   - A_n submits $t(n)$ pairs of equal length messages $(m_{0,1}, m_{1,1}), \ldots, (m_{0,t}, m_{1,t})$.
   - A_n obtains $pk, Enc_{ek}(m_{b,1}), \ldots, Enc_{ek}(m_{b,t})$ for a random $b \leftarrow \{0,1\}$.
   - A_n outputs a bit b', and wins if $b = b'$.

   Chosen Plaintext Attacks: The scheme is CPA-secure, if any n.u. PPT adverasry $A = \{A_n\}$ wins the following game with probability at most $1/2 + \mu(n)$ for some negligible μ.

   - A_n obtains pk.
   - A_n can repeatedly submit a message m and obtain an encryption $E_{ek}(m)$.
   - A_n submits two equal-length messages m_0, m_1 and obtains $Enc_{ek}(m_b)$ for a random $b \leftarrow \{0,1\}$.
   - A_n can once more repeatedly submit a message m and obtain an encryption $E_{ek}(m)$.
   - A_n outputs a bit b', and wins if $b = b'$.

   Show that:

   (a) (15 pts) Any scheme that is CPA-secure is also t-message KPA-secure for any polynomial t (in either the secret-key or public-key setting).

   (b) (5 pts) If there exist secret-key encryption schemes that are t-message KPA-secure for any polynomial t, than there exist ones that are not CPA secure.

   (c) (15 pts) Any public-key bit-encryption scheme that is 1-message KPA-secure is CPA secure.