CS 601.442/642 – Modern Cryptography Instructors: Aditya Hegde and Harry Eldridge

Homework 5

Deadline: March 5; 2026, 11:59pm ET

Instructions

- The solutions must be submitted via Canvas.
- You must typeset your solutions. We suggest using LaTeX or Typst.

Problems

1. (10 points) Prove that if the Decisional Diffie-Hellman assumption (DDH) holds for a group G then the Discrete Log assumption holds for G.

2. (10 points) Recall that $\mathbb{Z}_p$ represents the set of integers $\{0, \ldots, p-1\}$. For a set S, let S^i represent the set of all i-tuples composed of elements of S. For example, $(5, 6) \in \mathbb{Z}_{11}^2$.

   Let $\mathbb{G}$ be a cyclic group of prime order p with generator g. Define the following candidate PRG $G : \mathbb{Z}_p^2 \to \mathbb{G}^3$.

   $$\boxed{\begin{array}{l} G(x, y) \\ \hline \textbf{return } (g^x, g^y, g^{xy}) \end{array}}$$

   Prove that G is a secure PRG if DDH holds for $\mathbb{G}$.

3. (20 points) Recall the DDH assumption we saw in class, which stated that for a cyclic group G of prime order p and with generator g:

   $$\left\{ (G, p, g, g^x, g^y, g^{xy}) \;:\; \begin{array}{r} x \leftarrow\!\$\; \mathbb{Z}_p \\ y \leftarrow\!\$\; \mathbb{Z}_p \end{array} \right\} \overset{c}{\approx} \left\{ (G, p, g, g^x, g^y, g^r) \;:\; \begin{array}{r} x \leftarrow\!\$\; \mathbb{Z}_p \\ y \leftarrow\!\$\; \mathbb{Z}_p \\ r \leftarrow\!\$\; \mathbb{Z}_p \end{array} \right\}$$

   Let $h \leftarrow\!\$\; G$ denote sampling an element uniformly at random from the group G. Recall that in a prime order cyclic group all non-identity elements are generators. We define a new assumption, which we will call the "Two Generators Assumption," below:

   $$\left\{ (G, p, g, h, g^u, h^u) \;:\; \begin{array}{r} h \leftarrow\!\$\; G \\ u \leftarrow\!\$\; \mathbb{Z}_p \end{array} \right\} \overset{c}{\approx} \left\{ (G, p, g, h, g^u, h^v) \;:\; \begin{array}{r} h \leftarrow\!\$\; G \\ u \leftarrow\!\$\; \mathbb{Z}_p \\ v \leftarrow\!\$\; \mathbb{Z}_p \end{array} \right\}$$

   Prove that the Decisional Diffie-Hellman assumption implies the Two Generators Assumption.

   Hint: You can do this by proving the *contrapositive*. Show that if there exists an adversary that successfully distinguishes between the Two Generators distributions, you can build an adversary that distinguishes between the DDH distributions.

4. (30 points) Below we define a new notion for public-key encryption that we call *key-privacy*.

We say that a public key encryption scheme $(\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ satisfies *key-privacy* if for all NUPPT $\mathcal{A}$, there exists a negligible function $\nu(\cdot)$ such that $\forall \lambda \in \mathbb{N}$:

$$\Pr[\mathcal{A} \text{ wins } \mathsf{KPGame}] \leq \frac{1}{2} + \nu(\lambda)$$

Where the KPGame is defined as below:

KPGame

C_G		$\mathcal{A}_G$
$b \leftarrow\!\!\$ \{0,1\}$		
$(pk_0, sk_0) \leftarrow \mathsf{KGen}(1^\lambda)$		
$(pk_1, sk_1) \leftarrow \mathsf{KGen}(1^\lambda)$		
	$\xrightarrow{(pk_0, pk_1)}$	
	$\xleftarrow{m}$	
$\mathsf{ct} \leftarrow \mathsf{Enc}(pk_b, m)$		
	$\xrightarrow{\mathsf{ct}}$	
	$\xleftarrow{b'}$	
$\mathcal{A}$ wins if $b = b'$		

Intuitively, the property requires that an adversary cannot determine which public key a ciphertext was encrypted under.

Define a public key encryption scheme, prove that it is *correct*, prove that it satisfies IND-CPA security, and prove that it does *not* satisfy key-privacy.

5. (30 points) Below we define a new notion for public-key encryption called IND-CPA$ security, which means that ciphertexts should be indistinguishable from uniformly random elements of the ciphertext space. For a ciphertext space $\mathcal{C}$ let $\mathsf{ct} \leftarrow\!\!\$ \mathcal{C}$ denote sampling an element from $\mathcal{C}$ uniformly at random.

We say that a public key encryption scheme $(\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ with ciphertext space $\mathcal{C}$ satisfies IND-CPA\$ security if for all NUPPT $\mathcal{A}$, there exists a negligible function $\nu(\cdot)$ such that $\forall \lambda \in \mathbb{N}$:

$$|\Pr[\mathcal{A} \text{ outputs 1 in } \mathsf{Game}_0] - \Pr[\mathcal{A} \text{ outputs 1 in } \mathsf{Game}_1]| \leq \nu(\lambda)$$

Where Game_0 and Game_1 are defined below.

Game_0

C_G		$\mathcal{A}_G$
$(pk, sk) \leftarrow \mathsf{KGen}(1^\lambda)$		
	$\xrightarrow{pk}$	
	$\xleftarrow{m}$	
$\mathsf{ct} \leftarrow \mathsf{Enc}(pk, m)$		
	$\xrightarrow{\mathsf{ct}}$	
	$\xleftarrow{b'}$	

Game_1

C_G		$\mathcal{A}_G$
$(pk, sk) \leftarrow \mathsf{KGen}(1^\lambda)$		
	$\xrightarrow{pk}$	
	$\xleftarrow{m}$	
$\mathsf{ct} \leftarrow_\$ \mathcal{C}$		
	$\xrightarrow{\mathsf{ct}}$	
	$\xleftarrow{b'}$	

Prove that if a public-key encryption scheme satisfies IND-CPA\$ security then it satisfies IND-CPA security.

Hint. You should prove this using a sequence of games (see the proofs of IND-CPA security from class).