CSE 107 Midterm Exam

April 26, 2022

Answer the questions in the spaces provided on the question sheets. You may use the back side of the paper as scratch. Write legibly. If we can't read your writing or your answer is not within the specified answer space, you will not receive credit.

You may use a single, double-sided, letter-size page of handwritten notes for reference.

You may **not** use your computer, tablet, phone, or smartwatch during the exam.

The second page contains definitions of many of the security concepts we discussed in lecture for you to use during the exam.

There are 5 questions, for a total of 40 points. The last question is optional.

Name: ______________________________

PID: ______________________________

Question:	1	2	3	4	5	Total
Points:	10	10	10	10	0	40
Score:						

Block ciphers: Definition

Definition: block cipher

Let E: Keys $\times$ D $\rightarrow$ R be a family of functions.
We say that E is a block cipher if

- R = D, meaning the input and output spaces are the same set.
- E_K: D $\rightarrow$ D is a permutation for every key $K \in$ Keys, meaning has an inverse E_K^{-1}: D $\rightarrow$ D such that $E_K^{-1}(E_K(x)) = x$ for all $x \in$ D.

We let E^{-1}: Keys $\times$ D $\rightarrow$ D, defined by $E^{-1}(K, y) = E_K^{-1}(y)$, be the inverse block cipher to E.

In practice we want that E, E^{-1} are efficiently computable.

If Keys $= \{0,1\}^k$ then k is the key length as before.
If R = D $= \{0,1\}^\ell$ we call ℓ the block length.

Consistent Key Recovery: Game and Advantage

Let E: Keys $\times$ D $\rightarrow$ R be a family of functions, and A an adversary.

Game KR_E

procedure Initialize $K \xleftarrow{\$}$ Keys **procedure Fn**(M) Return $E(K, M)$	**procedure Finalize**(K') For $j = 1, \ldots, i$ do If $E(K', M_j) \neq C_j$ then Return false If $M_j \in \{M_1, \ldots, M_{j-1}\}$ then Return false Return true

The game returns true if (1) The key K' returned by the adversary is consistent with $(M_1, C_1), \ldots, (M_q, C_q)$, and (2) $M_1, \ldots, M_q$ are distinct.

A is a q-query adversary if it makes q distinct queries to its **Fn** oracle.

Definition of Adv$^{\mathrm{kr}}$

$$\mathbf{Adv}_E^{\mathrm{kr}}(A) = \Pr[\mathrm{KR}_E^A \Rightarrow \mathsf{true}].$$

Games defining prf advantage of an adversary against F

Let F: Keys $\times$ D $\rightarrow$ R be a family of functions.

Game Real_F	Game Rand_R
procedure Initialize $K \xleftarrow{\$}$ Keys **procedure Fn**(x) return $F_K(x)$	**procedure Initialize** $T[] \leftarrow (\perp$ for all $x)$ **procedure Fn**(x) if $\mathrm{T}[x] = \perp$ then $\mathrm{T}[x] \xleftarrow{\$}$ R return $\mathrm{T}[x]$

Definition of Adv$^{\mathrm{prf}}$

The (prf) advantage of A is

$$\mathbf{Adv}_F^{\mathrm{prf}}(A) = \Pr\left[\mathrm{Real}_F^A \Rightarrow 1\right] - \Pr\left[\mathrm{Rand}_R^A \Rightarrow 1\right]$$

Security: F is a (secure) PRF if $\mathbf{Adv}_F^{\mathrm{prf}}(A)$ is "small" for ALL A that use "practical" amounts of resources.

Games for ind-cpa-advantage of an adversary A

Let $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be an encryption scheme

Game $\mathrm{Left}_{\mathcal{SE}}$	Game $\mathrm{Right}_{\mathcal{SE}}$
procedure Initialize $K \xleftarrow{\$}$ Keys **procedure LR**(M_0, M_1) return $\mathcal{E}_K(M_0)$	**procedure Initialize** $K \xleftarrow{\$}$ Keys **procedure LR**(M_0, M_1) return $\mathcal{E}_K(M_1)$

Definition of Adv$^{\text{ind-cpa}}$

The (ind-cpa) advantage of A is

$$\mathbf{Adv}_{\mathcal{SE}}^{\text{ind-cpa}}(A) = \Pr\left[\mathrm{Right}_{\mathcal{SE}}^A \Rightarrow 1\right] - \Pr\left[\mathrm{Left}_{\mathcal{SE}}^A \Rightarrow 1\right]$$

Security: $\mathcal{SE}$ is IND-CPA-secure if $\mathbf{Adv}_{\mathcal{SE}}^{\text{ind-cpa}}(A)$ is "small" for ALL A that use "practical" amounts of resources.

Collision-resistance of a function family

The formalism considers a family H : Keys $\times D \rightarrow R$ of functions, meaning for each $K \in$ Keys we have a function $H_K : D \rightarrow R$ defined by $H_K(x) = H(K, x)$.

Game CR_H

procedure Initialize $K \xleftarrow{\$}$ Keys Return K **procedure Fn**(x) Return $H_K(x)$	**procedure Finalize**(x_1, x_2) If $(x_1 = x_2)$ then return false If $(x_1 \notin D$ or $x_2 \notin D)$ then return false Return $(H_K(x_1) = H_K(x_2))$

Let

$$\mathbf{Adv}_H^{\mathrm{cr}}(A) = \Pr\left[\mathrm{CR}_H^A \Rightarrow \mathsf{true}\right].$$

UF-CMA

Let $\mathcal{T}$: Keys $\times D \rightarrow R$ be a message authentication code. Let A be an adversary.

Game $\mathrm{UFCMA}_{\mathcal{T}}$

procedure Initialize $K \xleftarrow{\$}$ Keys ; $S \leftarrow \emptyset$ **procedure Tag**(M) $T \leftarrow \mathcal{T}_K(M)$; $S \leftarrow S \cup \{M\}$ return T	**procedure Finalize**(M, T) If $M \in S$ then return false If $M \notin D$ then return false Return $(T = \mathcal{T}_K(M))$

Definition: uf-cma advantage

The uf-cma advantage of adversary A is

$$\mathbf{Adv}_{\mathcal{T}}^{\text{uf-cma}}(A) = \Pr\left[\mathrm{UFCMA}_{\mathcal{T}}^A \Rightarrow \mathsf{true}\right]$$