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.

<table>
<thead>
<tr>
<th>Question</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Points</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>0</td>
<td>40</td>
</tr>
<tr>
<td>Score:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Block ciphers: Definition

**Definition: block cipher**

Let $E: \text{Keys} \times D \rightarrow R$ 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 $k \in \text{Keys}$, meaning it is a permutation.

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

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

If Keys = $\{0, 1\}^k$ then $k$ is the key length as before. If $R = D = \{0, 1\}^k$ we call $f$ 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 $K_{\text{uf-cma}}$**

- **procedure Initialize**
  - $K \leftarrow \text{Keys}$
  - **procedure Finalize**($E_k$)
  - **procedure $F_n(M)$**
    - Return $E_k(M)$

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

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

**Definition of $\text{Adv}^\text{uf-cma}$**

$$\text{Adv}^\text{uf-cma}_A = \Pr[\text{UF-CMA}_A \Rightarrow \text{true}]$$

Games defining prf advantage of an adversary against $F$

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

**Game $\text{Real}_X$**

- **procedure Initialize**
  - $K \leftarrow \text{Keys}$
  - **procedure $F_n(x)$**
    - return $F_X(x)$

**Game $\text{Rand}_X$**

- **procedure Initialize**
  - $T \leftarrow (\bot$ for all $x$)
  - **procedure $F_n(x)$**
    - if $T[x] = \bot$ then $T[x] \leftarrow R$
    - return $T[x]$

**Definition of $\text{Adv}^\text{prf}$**

The (prf) advantage of $A$ is

$$\text{Adv}^\text{prf}_A = \Pr[\text{Real}_X \Rightarrow 1] - \Pr[\text{Rand}_X \Rightarrow 1]$$

Security: $F$ is a (secure) PRF if $\text{Adv}^\text{prf}_A$ is “small” for ALL $A$ that use “practical” amounts of resources.

Games for ind-cpa-advantage of an adversary $A$

Let $SE = (K, E, D)$ be an encryption scheme.

**Game $\text{Left}_S$**

- **procedure Initialize**
  - $K \leftarrow \text{Keys}$
  - **procedure $LR(M_0, M_1)$**
    - return $E_K(M_0)$

**Game $\text{Right}_S$**

- **procedure Initialize**
  - $K \leftarrow \text{Keys}$
  - **procedure $LR(M_0, M_1)$**
    - return $E_K(M_1)$

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

The (ind-cpa) advantage of $A$ is

$$\text{Adv}^\text{ind-cpa}_S = \Pr[\text{Right}_S \Rightarrow 1] - \Pr[\text{Left}_S \Rightarrow 1]$$

Security: $SE$ is IND-CPA-secure if $\text{Adv}^\text{ind-cpa}_S(A)$ 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 $k \in \text{Keys}$ we have a function $H_k: D \rightarrow R$ defined by $H_k(x) = H(k, x)$.

**Game $\text{CR}_H$**

- **procedure Initialize**
  - $K \leftarrow \text{Keys}$
  - Return $K$
  - **procedure $F_n(x)$**
    - return $H_k(x)$

Let

$$\text{Adv}^\text{cr}_H = \Pr[\text{CR}_H \Rightarrow \text{true}]$$

UF-CMA

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

**Game $\text{UF-CMA}_T$**

- **procedure Initialize**
  - $K \leftarrow \text{Keys}$
  - $S \leftarrow \emptyset$
  - **procedure $Tag(M)$**
    - $T \leftarrow T_k(M)$, $S \leftarrow S \cup \{M\}$
    - return $T$

**Definition of $\text{uf-cma}$ advantage**

The uf-cma advantage of adversary $A$ is

$$\text{Adv}^\text{uf-cma}_A = \Pr[\text{UF-CMA}_T \Rightarrow \text{true}]$$