CSE 107 Discussion 2/7

Activity 1: Left over from last discussion

This activity will provide some practice of finding patterns you could exploit when designing an adversary for the IND-CPA security game.

Question 1: Let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher. Consider the following encryption algorithm Enc which takes a $4n$-bit message as input:

$\mathsf{Enc}(K, M[1] \,\|\, M[2] \,\|\, M[3] \,\|\, M[4])$:
  For $i = 1 \ldots 4$:
    $K_i \leftarrow K \oplus \mathsf{int\_to\_string}(i \bmod 3, k)$
    $C[i] \leftarrow E(K_i, M[i])$
  Return $C = C[1] \,\|\, C[2] \,\|\, C[3] \,\|\, C[4]$

Note that a single message M is interpreted as having four blocks $M = M[1] \,\|\, M[2] \,\|\, M[3] \,\|\, M[4]$. For example, if $n = 2$, a valid message is $M = 01101100$. Each 2-bit block will then be handled over 4 iterations of the for loop.

What exploitable weakness does this encryption algorithm have (with only one LR query)? Let $\mathcal{SE}$ be the symmetric encryption scheme based on Enc. Write pseudocode for an adversary A which makes one LR query and achieves $\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{SE}}(A) = 1$.

Activity 2: What are block ciphers good for?

Suppose that a block cipher $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ is a pseudorandom function (meaning, it has good PRF security).

Question 1: Let D be E^{-1} and let K output a random k-bit string. Now we have symmetric encryption scheme $\mathcal{SE} = (K, E, D)$. If E is PRF-secure does this mean $\mathcal{SE}$ is IND-CPA-secure? If adversary A is allowed 2 queries in the IND-CPA game, can you achieve $\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{SE}}(A) = 1$?

Question 2: Recall the CR (collision resistance) game for a hash function H: Adversary A is given $K \xleftarrow{\$} \{0,1\}^k$ and is trying to output (x_1, x_2) such that $x_1 \neq x_2$ and $H_K(x_1) = H_K(x_2)$. There are no oracles in the CR game.

A hash function is called collision-resistant if it is hard for any A to find a collision (x_1, x_2). If E is a block cipher, is it collision-resistant? Would E be a good hash function? Why or why not?

Activity 3: Fun with MACs

For MACs (message authentication codes), the security goal we consider is UF-CMA:

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

Game $\mathrm{UFCMA}_{\mathcal{T}}$	
procedure Initialize $K \xleftarrow{\$} \mathsf{Keys}$; $S \leftarrow \emptyset$ **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 $(T = \mathcal{T}_K(M))$

The uf-cma advantage of adversary A is

$$\mathbf{Adv}^{\text{uf-cma}}_{\mathcal{T}}(A) = \Pr\left[\mathrm{UFCMA}^{A}_{\mathcal{T}} \Rightarrow \mathsf{true}\right] . \tag{1}$$

Question 1: Which of the following do you think could be a UF-CMA-secure MAC? Which of the following can you break?

(a) Let $\mathcal{T}(K, M) = K \oplus M$, where keys and messages are both n-bit strings.

(b) Let $\mathcal{T}(K, M) = H(K, M)$ for a hash function H that is collision-resistant.

(c) Let $\mathcal{T}(K, M) = E(K, M)$ for a block cipher E that is PRF-secure.