CSE 107 Discussion 1/31

Activity 1: How to look for exploitable weaknesses in schemes

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 $\mathcal{E}$ which takes a $2n$-bit message as input:

$\mathcal{E}(K, M[1] \,\|\, M[2])$:
  $C[1] \leftarrow E(K, M[1] \oplus 0^{n-1}1)$
  $C[2] \leftarrow E(K, M[2] \oplus 0^{n-2}10)$
  Return $C = C[1] \,\|\, C[2]$

What exploitable weakness does this encryption algorithm have (with only one LR query)? Can you force $C[1] = C[2]$?

Question 2: Let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher. Consider the following encryption algorithm $\mathcal{E}$ which takes a $4n$-bit message as input:

$\mathcal{E}(K, M[1] \,\|\, M[2] \,\|\, M[3] \,\|\, M[4])$:
  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 $C = C[1] \,\|\, C[2] \,\|\, C[3] \,\|\, C[4]$

What exploitable weakness does this encryption algorithm have (with only one LR query)? Why are we specifying $4n$-bit messages and including a "mod 3" step?

Activity 2: A New Game

In this activity, you'll practice reading a new security definition and reasoning about how the game works and what the definition means.

Here's a new security definition you haven't seen before:

Game PRG_G
procedure Initialize
$b \xleftarrow{\$} \{0,1\}$
If $b = 0$ then $x \xleftarrow{\$} \{0,1\}^k$; $y \leftarrow G(x)$
Else $y \xleftarrow{\$} \{0,1\}^n$
return y
procedure Finalize(z)
If $(z = b)$ then return true
Else return false

Definition: Let $G : \{0,1\}^k \to \{0,1\}^n$, with $n > k$. Then $\mathbf{Adv}^{\text{PRG}}_G(A) = 2\Pr[\text{PRG}^A_G \Rightarrow \mathsf{true}] - 1$.

1. What is the initialization? The win condition? The adversary's special abilities (if any)?
2. What does the adversary know, and what is the adversary trying to do?
3. How does this compare to the PRF security definition – what are some similarities and some differences?
4. If n is much larger than k, can you think of anything a function satisfying this security definition might be useful for?

Activity 3: PRFs, block ciphers, and IND-CPA

In this activity, we will review some of the definitions we have seen so far. Ultimately, our goal is secure encryption, modelling something like "Only Alice and Bob can read the Signal messages in their chat." This will mean *correctness* for Alice and Bob, and *security* against anyone else.

Question 1: Let $F : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a family of functions. Could this be a correct encryption algorithm? What would corresponding decryption be?

Question 2: Let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher. Could this be a correct encryption algorithm? What would corresponding decryption D and key generation K be?

Question 3: Let $\mathcal{SE} = (K, E, D)$ from above, where E is a block cipher. Suppose that E is a pseudorandom function, meaning that it satisfies PRF security. (No efficient adversary has PRF advantage against E much larger than 0.) Does this mean $\mathcal{SE}$ is IND-CPA secure?

(a) If adversary A is allowed 2 queries in the IND-CPA game, can you achieve $\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{SE}}(A) = 1$?

(b) If adversary A is allowed 1 query in the IND-CPA game, can you achieve $\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{SE}}(A) \approx 1$? (Or, why is this question hard to definitively answer?)