CSE 107 Discussion 1/24

Activity 1: How to analyze an adversary

Let $\mathsf{AES} : \{0,1\}^{128} \times \{0,1\}^{128} \rightarrow \{0,1\}^{128}$ be the AES (Advanced Encryption Standard) block cipher. Note that AES and AES^{-1} are public and efficient algorithms.

Suppose we propose a new block cipher, the Ultra Encryption Standard, where
$U : \{0,1\}^{128} \times \{0,1\}^{128} \rightarrow \{0,1\}^{128}$ is defined by $U(K, M) = \mathsf{AES}(M, K)$.

Show that U is not a secure PRF by presenting in pseudocode an adversary A such that

- $\mathbf{Adv}^{\mathrm{prf}}_{U}(A) = 1 - 2^{-128}$
- A makes at most 2 queries to its **Fn** oracle
- A is very efficient.

Prove that your A has the above properties, following the outline below. (This format of problem and answer is what exam questions will look like in CSE 107).

(i) First, write pseudocode for adversary A. It should make two **Fn** queries and return a bit.

(ii) Second, what is the running time of A? Why is this "very efficient"?

(iii) What is $\Pr\left[\mathrm{REAL}_{U}^{A} \Rightarrow 1\right]$ (and why)?

(iv) What is $\Pr\left[\mathrm{RAND}_{\{0,1\}^{128}}^{A} \Rightarrow 1\right]$ (and why)?

(v) Now, what is $\mathbf{Adv}^{\mathrm{prf}}_{U}(A)$?

Activity 2: Fun with Pseudorandom Functions

Let $F : \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}^\ell$ be a secure pseudorandom function. Here are three ways of trying to use F to build a new PRF whose output is 2ℓ bits long.

Which of these PRF constructions (if any) do you think are probably secure? Which (if any) do you think you can break? Come up with an adversary for each one you think is broken. How many queries do you need?

Assume ℓ and k are large enough that brute-force or birthday attacks aren't a concern.

As usual in this class, $a \| b$ means the concatenation of a and b, and $\overline{a}$ means the bitwise NOT of a.

1. $F_1(K, X) = F(K, X) \| \overline{F(K, X)}$
2. $F_2(K, X) = F(K, X) \| F(K, \overline{X})$
3. $F_3(K, X) = F(K, X) \| F(\overline{K}, X)$

<u>*Note*</u>: F_3 is tricky! The answer is that it could be a secure PRF, but it depends on F. We encourage you to think about this one, but it's harder than what CSE 107 will usually ask.