Exercises

May 16, 2016

1. Read the following:

   (a) The description of the DES and AES algorithms from Stinson's book.

   (b) Read a more personalized story of AES at
   http://www.moserware.com/2009/09/stick-figure-guide-to-advanced.html

   (c) It may be helpful to study the following notes by Mihir Bellare and Philip Rogaway:

   - Block ciphers: *http://cseweb.ucsd.edu/ mihir/cse207/w-bc.pdf*
   - Pseudorandom Functions: *http://cseweb.ucsd.edu/ mihir/cse207/w-prf.pdf*

2. For $k = (k_1, k_2, k_3)$ define $\mathsf{3DES}_k(X) = \mathsf{DES}_{k_3}\left(\mathsf{DES}_{k_2}^{-1}(\mathsf{DES}_{k_1}(X))\right)$. Let $P, C \in \{0,1\}^{64}$ be such that $C = \mathsf{3DES}_k(P)$. We apply the following algorithm for an exhaustive key search on 3DES

   Algorithm Exhaustive(P, C)
   for each possible key $K = (K_1, K_2, K_3)$
   if $\mathsf{3DES}_K(P) == C$,
   output $K = (K_1, K_2, K_3)$
   end if
   end for

   (a) How many calls to DES is performed by the above algorithm?

   (b) If we assume that DES behaves like a random permutation, i.e, for any fixed $P, C \in \{0,1\}^{64}$

   $$\Pr[k \xleftarrow{\$} \{0,1\}^{56} : \mathsf{DES}_k(P) = C] = \Pr[\pi \xleftarrow{\$} \mathrm{Perm}(64) : \pi(P) = C].$$

   Then, how many wrong keys would be output by the algorithm Exhaustive in average?

(c) Now, suppose you have at your disposal q plaintext/ciphertext pairs (P_i, C_i), such that $C_i = \mathsf{3DES}_k(P_i)$, for $1 \leq i \leq q$. Write an algorithm similar to the algorithm Exhaustive to perform an exhaustive search in this scenario such that the number of wrong keys displayed by the algorithm is reduced. How many DES encryption/decryption is performed by your algorithm.

(d) How many wrong keys are now displayed by the modified algorithm on average (give an estimate as a function of q). What would be the value of q such that we can be almost sure that no wrong key would be displayed by the algorithm.

3. We discussed pseudorandom permutation families in class. Analogously, we can define pseudorandom function families. Let $F : \mathcal{K} \times \{0,1\}^\ell \to \{0,1\}^n$ be a family of functions, i.e., F is a set of functions $\{F_K\}_{K \in \mathcal{K}}$, where each F_K maps ℓ bit strings to n bit strings. We denote the set of all functions from $\{0,1\}^\ell$ to $\{0,1\}^n$ by $\mathsf{Func}(\ell, n)$. We define the prf-advantage of an adversary $\mathcal{A}$ as

$$\mathbf{Adv}_F^{\text{prf}}(\mathcal{A}) = \Pr\left[K \xleftarrow{\$} \mathcal{K} : \mathcal{A}^{F_K(.)} \Rightarrow 1\right] - \Pr\left[\rho \xleftarrow{\$} \mathsf{Func}(\ell, n) : \mathcal{A}^{\rho(.)} \Rightarrow 1\right].$$

Further we define the family F to be pseudorandom if for all efficient adversaries $\mathcal{A}$, $\mathbf{Adv}_F^{\text{prf}}(\mathcal{A})$ is small.

(a) Given a pseudorandom function family $\mathcal{F} : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$, construct a family $G : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^{2n}$ as $G_K(X) = F_K(X)||F_K(F_K(X))$. Show that G is not a pseudorandom family.

(b) Given a pseudorandom function family $\mathcal{F} : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$, construct a family $H : \mathcal{K} \times \{0,1\}^{2n} \to \{0,1\}^n$ as $H_K(X_1||X_2) = F_K(X_1) \oplus F_K(X_2)$, where $|X_1| = |X_2| = n$. Show that H is not a pseudorandom family.

Note: To show a family to be not pseudorandom, it is enough to construct an efficient adversary whose advantage is big. Showing something to be pseudorandom is generally much more difficult.