Exercise 2 – Introduction to Cryptography 89-656

Due Date: November 11, 2018

Exercise 1: The best algorithm known today for finding the prime factors of an n-bit number runs in time $2^{c \cdot n^{\frac{1}{3}} (\log n)^{\frac{2}{3}}}$. Assuming 4Ghz computers and $c = 1$ (and that the units of the given expression are clock cycles), estimate the size of numbers that cannot be factored for the next 100 years.

Exercise 2: Prove formally that the definition of indistinguishable encryptions in the presence of an eavesdropping adversary) cannot be satisfied if Π can encrypt arbitrary-length messages and the adversary is *not* restricted to output equal-length messages in experiment $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$.

Exercise 3: Let G be a pseudorandom generator where $|G(s)| > 2 \cdot |s|$.

1. Define $G'(s) \stackrel{\text{def}}{=} G(s0^{|s|})$. Is G' necessarily a pseudorandom generator?
2. Define $G'(s) \stackrel{\text{def}}{=} s_1, G(s_2)$, where $s = s_1, s_2$ and $s_1, s_2 \in \{0,1\}^{|s|/2}$. Is G' necessarily a pseudorandom generator?

Exercise 4: Let F be a length-preserving pseudorandom function. For the following constructions of a keyed function $F' : \{0,1\}^n \times \{0,1\}^{n-1} \to \{0,1\}^{2n}$, state whether F' is a pseudorandom function. If yes, prove it; if not, show an attack.

1. $F'_k(x) \stackrel{\text{def}}{=} F_k(0\|x) \,\|\, F_k(1\|x)$.
2. $F'_k(x) \stackrel{\text{def}}{=} F_k(0\|x) \,\|\, F_k(x\|1)$.

Exercise 5: Consider a variant of CBC-mode encryption where the sender simply increments the IV by 1 each time a message is encrypted (rather than choosing IV at random each time); this is called *nonce-based* encryption. Show that the resulting scheme is *not* CPA-secure.

Exercise 6: Let F be a pseudorandom permutation. Consider the mode of operation in which a uniform value $\mathsf{ctr} \in \{0,1\}^n$ is chosen, and the ith ciphertext block c_i is computed as $c_i := F_k(\mathsf{ctr}+i+m_i)$. Show that this scheme does not have indistinguishable encryptions in the presence of an eavesdropper.