Cryptography ENEE/CMSC/MATH 456: Homework 3

Extended Due by beginning of class on 3/2/2020.

1. Write a program that increments a counter $2^{24}, 2^{25}, 2^{26}, \ldots, 2^{33}$ times, and measure how many seconds your program takes to run in each case. Estimate how many years your program would take to increment a counter 2^{64} or 2^{128} times. Based on your findings, what do you think would be a reasonable setting for the security parameter k of a cryptosystem which is assumed to be secure against attackers running in time $2^{\sqrt{k}}$?

2. 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.

3. Prove the equivalence of Definition 3.8 and Definition 3.9.

4. Let G be a pseudorandom generator that on security paramter $n > 1$, takes as input bitstrings of length n and has expansion factor $\ell(n) > 2n$. In each of the following cases, say whether G' is necessarily a pseudorandom generator. If yes, give a proof; if not, show a counterexample.
   (a) Define $G'(s) = G(s_1, \ldots, s_{\lceil n/2 \rceil})$, where $s = s_1, \ldots, s_n$.
   (b) Define $G'(s) = G(0^{|s|} || s)$.
   (c) Define $G'(s) = G(\texttt{rotate}(s, 1))$, where $\texttt{rotate}(s, 1)$ rotates the bits of s to the right by one position.

5. There are two files on the course webpage rand_1.txt and rand_2.txt. One of these files contains the output (in hexadecimal) of a pseudorandom generator and the other file is not random nor pseudorandom. Can you distinguish which file is which? Use the statistical tests provided by NIST that can be downloaded from here `https://csrc.nist.gov/projects/random-bit-generation/documentation-and-software`. It will also be helpful to read the documentation (especially Section 5), which can be accessed here `http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-22r1a.pdf`.

   Make sure to justify your answer by providing screenshots and/or other documentation of the output of the NIST statistical tests.

   Choose two of the statistical tests (e.g. two from among ApproximateEntropy, BlockFrequency, CumulativeSums, FFT, etc.) and explain what these tests do and how they work.

6. Let $F : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$ be a pseudorandom function. For all $\text{SK} \in \{0,1\}^n$ and for all input $x \in \{0,1\}^n$, define $F'_{\text{SK}}(x) := F_{\text{SK}}(x) || F_{\text{SK}}(x+1)$. Is F' a pseudorandom function? If yes, prove it; if not, show an attack.

7. Consider the following keyed function F: For security parameter n, the key is an $n \times n$ Boolean matrix A and an n-bit Boolean vector b. Define $F_{A;b} := Ax + b$, where all operations are done modulo 2. Show that F is not a pseudorandom function.

8. Let F be a pseudorandom function and G be a psuedorandom generator with expansion factor $\ell(n) = n + 1$. For each of the following encryption schemes, state whether the scheme has indistinguishable encryptions in the presence of an eavesdropper and whether it is CPA-secure. (In each case, the shared key is a uniform $k \in \{0,1\}^n$.) Explain your answer.
   (a) To encrypt $m \in \{0,1\}^{n+1}$, choose uniform $r \in \{0,1\}^n$ and output the ciphertext $\langle r, G(r) \oplus m \rangle$.
   (b) To encrypt $m \in \{0,1\}^n$, output the ciphertext $m \oplus F_k(0^n)$.
   (c) To encrypt $m \in \{0,1\}^{2n}$, parse m as $m_1 || m_2$ with $|m_1| = |m_2|$, then choose uniform $r \in \{0,1\}^n$ and send $\langle r, m_1 \oplus F_k(r), m_2 \oplus F_k(r+1) \rangle$.