University of Maryland
CMSC456 — Introduction to Cryptography
Professor Jonathan Katz

Problem Set 3

Due at the *beginning* of class on Oct. 3

1. The energy radiated by the sun in 1 year is about $1.21 \cdot 10^{34}$ Joules. According to our current understanding of physics, the minimum amount of energy needed to flip a bit at 4.2 Kelvin (the temperature of liquid helium) is roughly $5.8 \cdot 10^{-23}$ Joules.

   Assume we harness all the energy output by the sun to implement a 256-bit counter (at 4.2 Kelvin), and assume that it takes just a single bit-flip to update the counter value. How many years would it take to cycle through all possible values of the counter? Note that the current estimated age of the universe is $\approx 2^{33}$ years. Do you expect brute-force search of 256-bit keys to be feasible any time soon?

2. Let G be a function that maps strings of length n to strings of length $2n$. Define

   $$\gamma(n) \stackrel{\text{def}}{=} \Pr[\text{the } (n+1)^{\text{st}} \text{ bit of } G(x) \text{ is equal to `1'}],$$

   where the probability is taken over random choice of $x \in \{0,1\}^n$. Prove that if G is a pseudorandom generator, then there is a negligible function ϵ with $\gamma(n) \leq \frac{1}{2} + \epsilon(n)$. (You should give a formal proof, not just an intuitive argument.)

3. Let G be a pseudorandom generator mapping n-bit strings to $2n$-bit strings, and consider the following private-key encryption scheme Π: $\mathsf{Gen}(1^n)$ outputs a key $k \in \{0,1\}^n$ chosen uniformly at random. $\mathsf{Enc}_k(m_1 \| m_2)$, with $k \in \{0,1\}^n$ and[1] $m_1, m_2 \in \{0,1\}^{2n}$, outputs the ciphertext $c_1 \| c_2$ where

   $$c_1 := G(k) \oplus m_1 \quad \text{and} \quad c_2 := G(k) \oplus m_1 \oplus m_2.$$

   (a) Show how decryption can be performed.

   (b) Show that this scheme does *not* have indistinguishable encryptions in the presence of an eavesdropper. Do this formally using the definition; i.e., give an explicit adversary $\mathcal{A}$ and show that $\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n) = 1] - \frac{1}{2}$ is not negligible.

4. Define a length-preserving function F as follows: $F_k(x) = k \oplus x$. Prove, using Definition 3.23, that F is not a pseudorandom function. That is, describe a polynomial-time distinguisher D and then show that the relevant expression in Definition 3.23 is not negligible.

5. (Exercise 3.16.) 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 the IV at random each time. (Technically, this means the sender maintains state and so this does not fit with our syntax for encryption. Ignore this for the purposes of this problem.) Show that the resulting scheme is not CPA-secure.

[1] '$\|$' denotes concatenation, so the message space here is all binary strings of length $4n$.