International Institute of Information Technology, Hyderabad.
Principles of Information Security

Problem Set

February 23, 2020

---

1. An encryption scheme is formally defined by algorithms `Gen`, `Enc` and `Dec` as well as a message space $\mathcal{M}$. Give formal specifications of these components for the shift cipher, the substitution cipher, and the Vigenere cipher (for the latter, you may assume the key always has length).

2. Consider an improved version of the Vigenere cipher, where instead of using multiple shift ciphers, multiple mono-alphabetic substitution ciphers are used. That is, the key consists of t random permutations of the alphabet, and the plaintext characters in positions i; $t+i$; $2t+i$ and so on are encrypted using the ith permutation. Show how to break this version of the cipher.

3. Prove or refute: For every encryption scheme that is perfectly secret it holds that for every distribution over the message space $\mathcal{M}$ every $m, m' \in \mathcal{M}$ and every $c \in \mathcal{C}$

$$\Pr[M = m | C = c] = \Pr[M = m' | C = c]$$

4. Let f, g be *negligible functions.* Decide whether (a) $H(n) = f(n) \times g(n)$ and (b) $H(n) = f(n)/g(n)$ are necessarily *negligible functions* (for arbitrary f, g) or not. If it is, prove it. If not, give a counterexample.

5. Let f, g be length preserving one-way function (so, e.g., $|f(x)| = |x|$). For each of the following functions h, decide whether it is necessarily a one-way function (for arbitrary f, g) or not. If it is, prove it. If not, show a counterexample.

   (a) $h(x) \overset{def}{=} f(x) \oplus g(x)$.

   (b) $h(x) \overset{def}{=} f(f(x))$.

   (c) $h(x_1 \parallel x_2) \overset{def}{=} f(x_1) \parallel g(x_2)$, ($\parallel$ means concatenation)

   (d) $h(x_1, x_2) = (f(x_1), x_2)$ where $|x_1| = |x_2|$.

6. Given an efficiently-computable function $G : \{0,1\}^* \to \{0,1\}^*$ with $|G(x)| = l(|x|)$ consider the following experiment defined for an algorithm A and parameter n:

   (a) Choose random $s \in \{0,1\}^n$ and set $y_0 = G(s)$. Choose random $y_1 = \{0,1\}^{l(n)}$.

   (b) Choose a random bit $b \in \{0,1\}$.

   (c) Give y_b to A, who outputs a bit b'.

   say G is an *indistinguishable* PRG if for all probabilistic, polynomial-time algorithms A, there exists a negligible function ϵ such that

$$\mathtt{Pr}[b' = b] \leq \tfrac{1}{2} + \epsilon(n)$$

   in the experiment above.

   Prove that this definition is equivalent to the definition of a pseudorandom generator.

7. The energy radiated by the sun in 1 year is about $1.21 \cdot 10^{34}$. 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?

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

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

   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 $\gamma(n) \leq 1/2 + \epsilon(n)$. (Give a formal proof, not just an intuitive argument.)

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

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

   (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 $\Pr[\mathtt{PrivK}^{eav}_{\mathcal{A},\Pi} = 1] - 1/2$ is not negligible.

10. Give complete details (and if possible present an example illustrating the methods you describe) of how to use an X to design a Y where:

    (a) $X =$ One-way permutation, $Y =$ Pseudorandom generator.

    (b) $X =$ Pseudorandom generator, $Y =$ One-way function.

    (c) $X =$ Pseudorandom generator, $Y =$ Pseudorandom function.

    (d) $X =$ Pseudorandom function, $Y =$ Invertible pseudorandom function.