International Institute of Information Technology, Hyderabad.
Introduction to Information Security

Problem Set

February 26, 2020

---

1. Using a coin with Pr[Heads] = p, for some unkown p, design a method to simulate an *unbiased* coin.

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

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

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

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

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

3. Let G be a pseudorandom generator mapping $n-$bit strings to $2n-$bit strings, and consider the following private-key encryption scheme Π: $\texttt{Gen}(1^n)$ outputs a key $k \in \{0,1\}^n$, chosen uniformly at random. $\texttt{Enc}_k(m_1||m_2)$ 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, i.e., give an explicit adversary $\mathcal{A}$ and show that:
   Pr[Output of Eavesdropping Game $= 1] - 1/2$ is not negligible

4. Consider the following private-key encryption scheme: The shared key is $k \in \{0,1\}^n$. To encrypt message $m \in \{0,1\}^n$, choose random $r \in \{0,1\}^n$ and output $(r, F_r(k) \oplus m)$, where F is a block cipher. Show that this scheme is not CPA-secure.

5. Consider the following key-agreement protocol:

   (a) **Alice** chooses $k, r \leftarrow \{0,1\}^n$ at random, and sends $s := k \oplus r$ to **Bob**.

   (b) **Bob** chooses $t \leftarrow \{0,1\}^n$ at random and sends $u := s \oplus t$ to **Alice**.

   (c) **Alice** computes $w := u \oplus r$ and sends w to **Bob**.

   (d) **Alice** outputs k and **Bob** computes $w \oplus t$

   Show that **Alice** and **Bob** output the same key. Analyze the security of the scheme (i.e., either prove its security or show a concrete attack)

6. Give Shannon's definition of perfect secrecy and also give the adversarial indistinguishable definition of perfect secrecy (game-based definition where an unbounded adversary is able to differentiate (better than guessing) between the encryptions of two distinct plaintexts). Prove that both these definitions are equivalent.

7. The node A wishes to establish a secret key with node D using the Diffie-Hellman key exchange algorithm. However, *one* of the (six) channels in the network is suspected to be actively corrupt by a computationally *unbounded* adversary who can easily solve the discrete logarithm problem as well as modify the messages sent across the channel. Design a protocol for key agreement between A and D that works correctly and securely no matter which channel is corrupt. Illustrate your protocol via an example.

8. Fermat primes are prime numbers of the form $2^n + 1$. A Fermat number is a positive integer of the form $2^{2^n} + 1$. A Mersenne number is a positive integer of the form $2^n - 1$. A Mersenne prime is a Mersenne number that is prime. Answer the following questions.

   (a) How many Fermat primes are also Mersenne primes? Prove your answer.

   (b) Prove that 2 is the *only* Fermat prime that is not a Fermat number.

   (c) Prove that if $2^n - 1$ is prime then n is prime.

   (d) Show that Diffie-Hellman key-exchange protocol is *insecure* in $\mathbb{Z}_p$, if p is a Fermat prime.

9. Let f, g be negligible functions. Decide whether:

   (a) $H(n) = f(n) + g(n)$

   (b) $H(n) = f(n) \times g(n)$

   (c) $H(n) = f(n)/g(n)$

   are necessarily negligible functions (for arbitrary f; g) or not. If it is, prove it. If not, give a counterexample.

10. Let G be a multiplicative group of order n. Consider an element g in G. Prove that order of g divides n.

11. Prove that if $2^n - 1$ is prime then n is prime.

12. A number is said to be an exact-power if it is of the form a^b. There exists a polynomial-time algorithm for testing if the given number is an exact-power.

13. 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 $c \in \mathcal{C}$

$$\mathrm{P}[M = m | C = c] = \mathrm{P}[M = m' | C = c]$$

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

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

   (a) Show how decryption can be performed.

   (b) Show that this scheme does *not* have indistinguishable encryptions in the presence of an eavesdropper, i.e., give an explicit adversary $\mathcal{A}$ and show that:
   Pr[Output of Eavesdropping Game $= 1] - 1/2$ is not negligible

15. After having studied the Diffie-Hellman protocol, a young cryptographer decides to implement it. In order to simplify the implementation, he decides to use the additive group $(Z_p; +)$ instead of the multiplicative one $(Z_p^*; \times)$. As an experienced cryptographer, what do you think about this new protocol?