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

Mid Semester Examination

February 25, 2020

Time: **90 mins.** Max. Marks: **40.**

There are *eight* questions, 5 marks each. Attempt all questions.

---

1. 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.

2. 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 $c \in C$

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

3. 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. Moreover, 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) $h(x) \stackrel{def}{=} f(x) \oplus g(x)$.

   (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 $|x_1| = |x_2|$.

4. 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

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

   in the experiment above.

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

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

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

(b) X = Pseudorandom generator, Y = Pseudorandom function.

(c) X = Pseudorandom function, Y = Invertible pseudorandom function.

(d) X = Pseudorandom function, Y = Message Authentication Code

(e) X = MAC and PRF, Y = CCA-Secure Encryption Scheme

6. Show that the basic CBC-MAC as described in class is insecure if the sender authenticates messages of different lengths.

7. Describe and prove an improved version (that starts off with a collision resistant hash function with lesser compression ratio) of Merkle-Damgard Transform.

8. If A and B are connected by *two* insecure channels, where the adversary may choose to actively corrupt any one among them and passively eavesdrop on the other, design a secure key establishment protocol using the DDH assumption (or argue its impossibility if you so think).

ALL THE BEST