Principles Of Information Security - Spring 2025

Mid Semester Examination

Maximum Time : 90 Minutes Total Marks : 50

1. [5 points] Let F be a pseudorandom function. Show that the following MAC for messages of length $2n$ is not secure: Gen outputs a uniform $k \in \{0,1\}^n$. To authenticate a message $m1||m2$ with $|m_1| = |m_2| = n$, compute the tag $F_k(m_1)||F_k(F_k(m_2))$.

2. [5 points] Consider a MAC for arbitrary-length messages by $\text{Mac}_{s,k}(m) = H^s(k||m)$ where H is a collision-resistant hash function. Is this a secure MAC when H is constructed via the Merkle-Damgård transform? (Assume the hash key s is known to the attacker, and only k is kept secret.)

3. [5 points] Consider a variant of CBC-MAC where the message size is appended to the end of the message prior to passing to basic CBC-MAC. Prove that this variant is not secure for any arbitrary-length messages.

4. [5 points] Is it known that for every one-way function, one can construct a hard-core predicate? What is the Goldreich-Levin theorem?

5. [5 points] Consider a modification of the substitution cipher, where instead of applying only the substitution, we first apply a substitution and then apply a shift cipher on the substituted values. Give a formal description of this scheme and show how to break the substitute and shift cipher.

6. [5 points] Show that if H_1 and H_2 are distinct collision resistant functions with range $\mathcal{T} := \{0,1\}^n$, then $H(x) := H_1(x) \oplus H_2(x)$ need not be collision resistant.

7. [5 points] Explain the El-Gamal public key scheme in detail. Prove that it is not CCA secure?

8. [5 points] If $2^n + 1$ is an odd prime for some integer n, prove that n is a power of 2.

9. [5 points] An old woman goes to market and a horse steps on her basket and crashes the eggs. The rider offers to pay for the damages and asks her how many eggs she had brought. She does not remember the exact number, but when she had taken them out five at a time, there were two eggs left. The same happened when she picked them out nine at a time, but when she took them seven at a time there were three left. What is the smallest number of eggs she could have had? What is the second smallest number of eggs she could have had? In general, what is the k^{th} smallest number of eggs she could have had? Prove your answers.

10. [5 points] Let $G : \{0,1\}^* \to \{0,1\}^*$ be a function that doubles the length of its input, i.e. $|G(s)| = 2.|s|$. Show an algorithm A (that does not necessarily run in polynomial time) for which

$$|Pr[A(G(s)) = 1] - Pr[A(r) = 1]| \geq 1/2$$

for n large enough. Can we conclude that "perfect PRGs" do not exist, why?