دانشکده‌ی علوم ریاضی

مقدمه‌ای بر رمزنگاری

آزمون میانترم

مدرّس: دکتر شهرام خزائی

تاریخ: ۱۳۹۹/۹/۲۳

Problem 1

i. The book claims that perfectly-secret public-key encryption is impossible. Prove this claim.

2. Give formal security definitions of second-preimage and preimage-resistance.

Problem 2

Let $\Pi = (\mathsf{Gen}, \mathsf{MAC}, \mathsf{Verify})$ be a secure MAC that uses canonical verification. Prove Π is a strong MAC.
Recall: The canonical way to perform verification is to simply re-compute the tag and check for equality.

Problem 3

Let $(\mathsf{Gen}, \mathsf{H})$ be a collision-resistant hash function. Argue whether each of the following is collision-resistant. Provide a proof or counterexample for your answers.

1. $(\mathsf{Gen}, \mathsf{H}_2)$ with $\mathsf{H}_2^s(m) \coloneqq \mathsf{H}^s(m)||\mathsf{H}^s(m)$.

2. $(\mathsf{Gen}, \mathsf{H}_1)$ with $\mathsf{H}_1^s(m) \coloneqq \mathsf{H}^s(\mathsf{H}^s(m))$.

Problem 4

Let $(\mathsf{Enc}, \mathsf{Dec})$ be a secure authenticated encryption scheme. Show whether the following is a secure authenticated encryption scheme. Provide a proof or counterexample for your answer.

$$\mathsf{Enc}_1(k,m) \coloneqq (\mathsf{Enc}(k,m), \mathsf{Enc}(k,m));$$
$$\mathsf{Dec}_1(k,(c_1,c_2)) \coloneqq \begin{cases} \mathsf{Dec}(k,c_1) & if\, \mathsf{Dec}(k,c_1) = \mathsf{Dec}(k,c_2) \\ \perp & otherwise \end{cases}$$