


دانشکده‌ی علوم ریاضی

مقدمه‌ای بر رمزنگاری

آزمون میانترم

مدرّس: دکتر شهرام خزائی

تاریخ: ۱۳۹۹/۹/۲۳

Problem 1

Give an example of a hash function which is preimage resistance, but not collision resistant.

Problem 2

Consider a variant of MAC which the security experiment is defined exactly as before except that the MAC_k oracle does **not** take any input. Instead, whenever the adversary queries MAC_k, then this procedure samples a random message $m \leftarrow \{0,1\}^n$, where n is the security parameter, and outputs (m, t) where $t \leftarrow \mathsf{MAC}_k(m)$. We call this security notion *existential unforgeability under random-message attack*.

- Prove that existential unforgeability under an adaptive chosen-message attack implies security in the above sense.
- Show that existential unforgeability under an adaptive chosen-message attack is strictly stronger.
  Hint: Assume there exists at least one MAC scheme which is existentially unforgeable under random-message attack. Prove that then there exists also a MAC scheme which is existentially unforgeable under random-message attack, but not existentially unforgeable under an adaptive chosen-message attack.

Problem 3

Show that KEMs and PKEs are equivalent in the following sense: If there exists an IND-CPA secure PKE scheme, then there exists an IND-CPA secure KEM, and vice versa.