


دانشکده‌ی علوم ریاضی

مقدمه‌ای بر رمزنگاری

آزمون میانترم

مدرّس: دکتر شهرام خزائی

تاریخ: ۱۳۹۹/۹/۲۳

Problem 1

Give an example of a an encryption scheme that is CCA-secure but not an authenticated encryption scheme.
Remark: This shows that the converse of the statement "authenticated encryption implies CCA-security" is false.

Problem 2

Consider a variant of MAC which the security experiment is defined exactly as before except that the adversary is forced to announce the message m^* for which it will produce a forgery at the beginning of the game. The experiment outputs 1 if and only if the adversary outputs a tag t^* such that $\mathsf{Verify}_k(m^*, t^*) = 1$. We call this security notion *selective unforgeability under an adaptive chosen-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 selective unforgeable under an adaptive chosen-message attack. Prove that then there exists also a MAC scheme which is secure in this sense, but insecure in the sense of existentially unforgeable under an adaptive chosen-message attack.

Problem 3

Let $(\mathsf{Enc}_{\mathsf{CBC}}, \mathsf{Dec}_{\mathsf{CBC}})$ be a randomized CBC-mode encryption scheme built from a block cipher $F : \mathcal{K} \times \mathcal{X} \to \mathcal{X}$. Let $\mathsf{H} : \mathcal{X}^{\leq L} \to \mathcal{X}$ be a collision resistant hash function. Define the following candidate authenticated encryption scheme $(\mathsf{Enc}, \mathsf{Dec})$:

- $\mathsf{Enc}(k, m)$: Output $c \leftarrow \mathsf{Enc}_{\mathsf{CBC}}(k, \mathsf{H}(m)||m)$.
- $\mathsf{Dec}(k, c)$: Compute $(t, m) \leftarrow \mathsf{Dec}_{\mathsf{CBC}}(k, c)$ and output m if $t = \mathsf{H}(m)$ and $\perp$ otherwise.

1. Show that $(\mathsf{Enc}, \mathsf{Dec})$ does not provide ciphertext integrity.
2. Show that $(\mathsf{Enc}, \mathsf{Dec})$ is not CCA-secure.
3. Would the above problems go away if the construction had used randomized counter mode encryption instead of CBC-mode encryption? Give a brief explanation.