


دانشکده‌ی علوم ریاضی

مقدمه‌ای بر رمزنگاری

آزمون میانترم

مدرّس: دکتر شهرام خزائی

تاریخ: ۱۳۹۹/۹/۲۳

Problem 1

Consider an extension of the definition of secure MAC where the adversary is provided with oracles for both producing tags $\mathcal{O}.\mathsf{MAC}$ and verification $\mathcal{O}.\mathsf{Verify}$. Provide a formal definition of security in an experiment that provides access to $\mathcal{O}.\mathsf{MAC}$ and $\mathcal{O}.\mathsf{Verify}$, in such a way that there is no eventual output from the adversary, i.e. the win condition is built into $\mathcal{O}.\mathsf{Verify}$ queries.

Recall: As the Katz-Lindell book mentioned on p. 115, the verification oracle allows the adversary to interact with an honest receiver, sending m', t' to the receiver to learn whether $\mathsf{Verify}_k(m', t') = 1$.

Problem 2

Show a CPA-secure private-key encryption scheme that is unforgeable but is not CCA-secure.

Problem 3

Construct a MAC scheme which is strongly secure, but when used in encrypt-then-authenticate and the **same key** is used for both the underlying encryption scheme and the MAC, then the resulting combined encryption scheme is not even IND-CPA secure. This should hold regardless of the security of the underlying encryption scheme, which could be IND-CCA secure, for instance.