دانشکده‌ی علوم ریاضی

مقدمه‌ای بر رمزنگاری   تحویل اصلی: ۳ اردیبهشت ۱۴۰۰

تمرین شماره ۴

مدرّس: دکتر شهرام خزائی   تحویل نهایی: ۱۰ اردیبهشت ۱۴۰۰

- Upload your answers on courseware with the name: StudentNumber.pdf
- Upload a PDF file. Image and zip formats are not accepted.
- Similar answers will not be graded.
- NO answers will be accepted via e-mail.
- You can’t upload files bigger than 2 Mb, so you’d better type.
- Deadline time is always at 23:55 and will not be extended.
- You should submit your answers before soft deadline.
- You will lose 5 percent for each day delay if you submit within a week after soft deadline.
- You can not submit any time after hard deadline.
- This problem sets include 55 points.
- For any question contact Sara Sarfaraz via sarassm60@gmail.com.

Problem 1

(20 points) Let F be a strong pseudorandom permutation, and define the following fixed-length encryption scheme: On input a message $m \in \{0,1\}^{n/2}$ and key $k \in \{0,1\}^n$, algorithm Enc chooses a uniform $r \in \{0,1\}^{n/2}$ and outputs the ciphertext $c := \mathsf{F}_k(m||r)$. Prove that this scheme is CCA-secure.

Problem 2

(20 Points) Let F be a pseudorandom function. In each of the following cases, prove or disprove the security of the given MAC. (In each case Gen outputs a uniform $k \in \{0,1\}^n$. Let $\langle i \rangle$ denote an $n/2$-bit encoding of the integer i.)

(a) To authenticate a message $m = m_1, ..., m_l$, where $m_i \in \{0,1\}^{n/2}$, compute
$t := \mathsf{F}_k(\langle 1 \rangle || m_1) \oplus ... \oplus \mathsf{F}_k(\langle l \rangle || m_l)$.

(b) To authenticate a message $m = m_1, ..., m_l$, where $m_i \in \{0,1\}^{n/2}$,
choose uniform $r \leftarrow \{0,1\}^n$, compute $t := \mathsf{F}_k(r) \oplus \mathsf{F}_k(\langle 1 \rangle || m_1) \oplus ... \oplus \mathsf{F}_k(\langle l \rangle || m_l)$, and let the tag be the pair of $\langle r, t \rangle$.

Problem 3

(15 points) Show that the CBC mode of encryption does not yield CCA-secure encryption.

Problem 4 (Optional)

(20 points) Let (S, V) be a secure MAC defined over (K, M, T) where $T = \{0,1\}^n$. Define a new MAC (S_2, V_2) as follows:
$S_2(k, m)$ is the same as $S(k, m)$, except that the last eight bits of theoutput tag t are truncated. That is, S_2 outputs tags in $\{0,1\}^{n-8}$. Algorithm $V_2(k, m, t')$ accepts if there is some $b \in \{0,1\}^8$ for which $V(k, m, t'||b)$ accepts. Is (S_2, V_2) a secure MAC? Give an attack or argue security.