دانشکدهٔ علوم ریاضی

مقدمه‌ای بر رمزنگاری	مدرس: دکتر شهرام خزایی

تمرین سری دو

گردآورنده: فاطمه زرین‌جویی، عارف نماینده

مهلت ارسال: ۲۵ آبان

- پاسخ‌های خود را در قالب یک فایل PDF با نام HW2-ID ارسال نمایید که ID شمارهٔ دانشجویی شما است.
- یادآوری می‌شود که در اختیار دادن راه‌حل‌های مکتوب به سایر دانشجویان و یا منتشر کردن آن در اینترنت یا شبکه‌های اجتماعی غیرمجاز است و عواقب آن بر عهدهٔ نویسنده پاسخ است.
- مشورت در تمرین‌ها مجاز است و توصیه می‌شود اما هر دانش‌جو موظف است که تمرین را به تنهایی انجام دهد و راه‌حل نهایی ارسال‌شده **باید توسط خود دانش‌جو** نوشته شده باشد. در صورت مشاهدهٔ هر گونه تخلف، نمرهٔ تمام تمرینات شخص خاطی صفر لحاظ خواهد شد.
- تمریناتی که به صورت دست‌نویس تحویل داده می‌شوند، باید به صورت کاملاً خوانا نوشته شود و با کیفیتی مطلوب و حجم پایین، اسکن و ارسال شود.
- **به ازای هر روز تاخیر، ۵ درصد از نمره‌ی کسب شده کم می شود. در هر سری، اجازه‌ی حداکثر ۵ روز تاخیر دارید. در مجموع کل تمرین‌ها، اجازه‌ی حداکثر ۱۰ روز تاخیر دارید.**
- **حداقل دو سری از تمرین‌ها باید با استفاده از LaTeX نوشته شده و تحویل داده شود. در غیر این‌صورت ۰٫۵ نمره از نمره‌ی نهایی کسر خواهد شد.**
- **لطفا فقط سه سوال را به انتخاب خود حل کنید؛ حل سوالات بیشتر نمره‌ی اضافی ندارد.**

Problem 1

(Nested encryption) For a encryption scheme $\Pi = (\mathsf{Enc}, \mathsf{Dec})$ define the nested cipher $\Pi' = (\mathsf{Enc}', \mathsf{Dec}')$ as

$$\mathsf{Enc}'((k_0, k_1), m) = \mathsf{Enc}(k_1, \mathsf{Enc}(k_0, m)) \quad \text{and} \quad \mathsf{Dec}'((k_0, k_1), c) = \mathsf{Dec}(k_0, \mathsf{Dec}(k_1, c)).$$

Our goal is to show that if Π is EAV-secure then Π' is EAV-secure; even if the adversary is given one of the keys k_0 or k_1.

(a) Consider the following EAV-secure experiments, Experiments 0 and 1: in Experiment b, for $b = 0, 1$, the adversary generates two messages m_0 and m_1 and gets back k_1 and $\mathsf{Enc}'((k_0, k_1), m_b)$. The adversary outputs $\hat{b} \in \{0,1\}$ and we define its advantage, NEadv$[\mathcal{A}, \Pi']$ as in the usual definition of EAV-secure experiment:

$$\text{NEadv}[\mathcal{A}, \Pi'] = |\Pr[\mathcal{A} \text{ outputs } 1|b = 1] - \Pr[\mathcal{A} \text{ outputs } 1|b = 0]|.$$

Show that for every nested encryption adversary $\mathcal{A}$ attacking Π', there exists an adversary $\mathcal{B}$ attacking Π with advantage

$$\text{SSadv}[\mathcal{B}, \Pi] = |\Pr[\mathcal{B} \text{ outputs } 1|b = 1] - \Pr[\mathcal{B} \text{ outputs } 1|b = 0]|,$$

such that

$$\text{NEadv}[\mathcal{A}, \Pi'] = \text{SSadv}[\mathcal{B}, \Pi].$$

Draw a diagram with $\mathcal{A}$ on the right, $\mathcal{B}$ in the middle, and $\mathcal{B}$'s challenger on the left. Show the message flow between these three parties that takes place in your proof of security.

(b) Repeat part (a), but now when the adversary gets back k_0 (instead of k_1) in Experiments 0 and 1. Draw a diagram describing the message flow in your proof of security as you did in part (a).

Problem 2

Let $G : \{0,1\}^{2n} \longrightarrow \{0,1\}^{2n+1}$ be a pseudorandom generator (PRG). For each part below, either prove or disprove that $G' : \{0,1\}^{2n} \longrightarrow \{0,1\}^{2n+1}$ is necessarily a PRG no matter which PRG G is used.

(a) $G'(x) := G(\pi(x))$, where $\pi : \{0,1\}^{2n} \longrightarrow \{0,1\}^{2n}$ is any poly(n)-time computable bijective function. (You may not assume that π^{-1} is poly(n)-time computable.)

(b) $G'(x||y) := G(x||x \oplus y)$, where $|x| = |y| = n$. (Note: x||y refers to the concatenation of two strings x and y.)

(c) $G'(x||y) := G(x||0^n) \oplus G(0^n||y)$, where $|x| = |y| = n$. (Note: 0^n and 1^n denote the string of 0s and 1s, respectively, of length n.)

(d) $G'(x||y) := G(x||y) \oplus (x||0^{n+1})$, where $|x| = |y| = n$.

Problem 3

Let $F : \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}^n$ be a pseudorandom function (PRF). For each of the following function F', say (and prove) whether it is necessarily a PRF or not.

(a) $F'_k(x) = F_k(x)||F_k(\bar{x})$.

(b) $F'_k(x) = F_{0^n}(x)||F_k(x)$.

(c) $F'_k(x) = F_k(x) \oplus x$.

(d) $F'_k(x) = F_k(x)$.

(e) $F'_k(x) = F_{k_1}(x)||F_{k_2}(x)$, where $k_1, k_2 \in \{0,1\}^n$ and $k = k_1||k_2 \in \{0,1\}^{2n}$ is the concatenation of k_1 and k_2.

(f) $F'_k(x) = F_{k_1}(x)||F_{k_2}(x)$, where $k_1 = F_k(0^n)$ and $k_2 = F_k(1^n)$.

(g) $F'_k(x) = F_k(x) \oplus k$.

Problem 4

Intuitively, encrypting a message twice should not harm security. It turns out that this is not always true. Let $(\mathsf{Enc}, \mathsf{Dec})$ be a encryption scheme and define the "encrypt-twice" encryption scheme $(\mathsf{Enc}_2, \mathsf{Dec}_2)$ where $\mathsf{Enc}_2(k, m) := \mathsf{Enc}(k, \mathsf{Enc}(k, m))$.

(a) Give an example of a encryption scheme $(\mathsf{Enc}, \mathsf{Dec})$ that is EAV-secure, but $(\mathsf{Enc}_2, \mathsf{Dec}_2)$ is not EAV-secure.

(b) Suppose $(\mathsf{Enc}, \mathsf{Dec})$ is CPA-secure. Prove that $(\mathsf{Enc}_2, \mathsf{Dec}_2)$ is also CPA-secure.

Problem 5

Let F be a pseudorandom function and G be a psuedorandom generator with expansion factor $l(n) = n + 1$. For each of the following encryption schemes, state whether the scheme has indistinguishable encryptions in the presence of an eavesdropper and whether it is CPA-secure. (In each case, the shared key is a uniform $k \in \{0,1\}^n$.) Explain your answer.

(a) To encrypt $m \in \{0,1\}^{n+1}$, choose uniform $r \in \{0,1\}^n$ and output the ciphertext $\langle r, G(r) \oplus m \rangle$.

(b) To encrypt $m \in \{0,1\}^n$, output the ciphertext $m \oplus F_k(0^n)$.

(c) To encrypt $m \in \{0,1\}^{2n}$, parse m as $m_1||m_2$ with $|m_1| = |m_2|$, then choose uniform $r \in \{0,1\}^n$ and send $\langle r, m_1 \oplus F_k(r), m_2 \oplus F_k(r+1) \rangle$.