


دانشکدهٔ علوم ریاضی

مقدمه‌ای بر رمزنگاری — مدرس: دکتر شهرام خزایی

تمرین سری سه

گردآورنده: علی توسلی، امیرمتین شهنازی، آرمان کشازرع — مهلت ارسال: ۱۶ آذر

- **از بین ۵ سوال این تمرین، به ۳ سوال به دلخواه پاسخ دهید.**
- پاسخ‌های خود را در قالب یک فایل PDF با نام HW3-ID ارسال نمایید که ID شمارهٔ دانشجویی شماست.
- 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 ارسال شده **باید توسط خود دانشجو** نوشته شده باشد. در صورت مشاهدهٔ هرگونه 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 تأخیر، ۵ درصد از نمرهٔ کسب شده کم می‌شود. در هر سری، اجازهٔ حداکثر ۵ روز تأخیر دارید. در مجموع کل تمرین‌ها، اجازهٔ حداکثر ۱۰ روز تأخیر دارید.**
- **حداقل دو سری از تمرین‌ها باید با استفاده از LaTeX نوشته شده و تحویل داده شود. در غیر این صورت ۰٪۵ نمره از نمرهٔ نهایی کسر خواهد شد.**

Problem 1

Suppose that $\{f_k : \{0,1\}^n \to \{0,1\}^n\}_{k\in\{0,1\}^n}$ is a family of pseudo-random functions. Consider an encryption scheme that its encryption algorithm is as follows:

$$\mathrm{Enc}_k(m) = \begin{cases} (r, f_k(r) \oplus m, f_k(0^n)) & \text{if } m \neq f_k(0^n), \\ (r, f_k(r) \oplus m, k) & \text{if } m = f_k(0^n), \end{cases}$$

where r is randomly selected from n-bit strings. Show that this encryption scheme is multi-message secure but not CPA secure.

Problem 2

Consider the Data Encryption Standard (DES) encryption. What happens if the S-boxes are replaced with linear functions? Specifically, assume $S_i : \{0,1\}^6 \to \{0,1\}^4$ is defined as:

$$S_i(x_1, x_2, \ldots, x_6) = (x_2 \oplus x_3, x_1 \oplus x_4 \oplus x_5, x_1 \oplus x_6, x_2 \oplus x_3 \oplus x_6)$$

Analyze the implications for the scheme's CPA security and attempt to break it.
Fact: Even if S_i are not completely linear but are functions close to linear, the scheme is also not secure. This is why the S-boxes are chosen very carefully.

Problem 3

Prove that the following encryption scheme is CCA secure. Let $\{p_k\}$ be a collection of pseudorandom permutations mapping $\{0,1\}^{3n}$ to $\{0,1\}^{3n}$.

- To encrypt $x \in \{0,1\}^n$ with key k, do the following: choose $r \leftarrow_R \{0,1\}^n$, and send $p_k(x \parallel r \parallel 0^n)$ (where $\parallel$ denotes concatenation).
- To decrypt $y \in \{0,1\}^{3n}$, compute $x \parallel r \parallel w = p_k^{-1}(y)$. If $w \neq 0^n$, then output $\perp$. Otherwise, output x.

Problem 4

Let $\pi : \mathcal{X} \to \mathcal{X}$ be a fixed public permutation (i.e., a one-to-one function) where $\mathcal{X} := \{0,1\}^n$. When we say that π is public, we mean that anyone can compute $\pi(x)$ and $\pi^{-1}(x)$ for a given x in $\mathcal{X}$. The Even-Mansour cipher $(\mathrm{Enc}, \mathrm{Dec})$ derived from π is defined as:

$$\mathrm{Enc}((k_0, k_1), m) := \pi(m \oplus k_0) \oplus k_1.$$

(a) Explain how $\mathrm{Dec}((k_0, k_1), c)$ works.

(b) Show that $\mathrm{Enc}_1(k_1, m) := \pi(m) \oplus k_1$, with the corresponding Dec_1, is not a secure PRP.

(c) Show that $\mathrm{Enc}_2(k_0, m) := \pi(m \oplus k_0)$, with the corresponding Dec_2, is not a secure PRP.

Problem 5

(Predictable IVs) Let us see why in CBC mode an unpredictable IV is necessary for CPA security. Suppose a defective implementation of CBC encrypts a sequence of messages by always using the last ciphertext block of the ith message as the IV for the $(i+1)$-st message. The TLS 1.0 protocol, used to protect Web traffic, implements CBC encryption this way. Construct an efficient adversary that wins the CPA game against this implementation with an advantage close to 1. We note that the Web-based BEAST attack exploits this defect to completely break CBC encryption in TLS 1.0.