


دانشکده‌ی علوم ریاضی

مقدمه‌ای بر رمزنگاری تحویل اصلی ۲۶ آبان ۱۴۰۲

تمرین : سری ۲

مدرّس : دکتر شهرام خزائی *تحویل نهایی ۳ آذر*

- 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 1 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.
- For any question contact Mohammad Amin Raeisi via `m.aminra81@gmail.com`.

Problem 1

1. Let $\mathsf{F} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a secure PRF (i.e. a PRF where the key space, input space, and output space are all $\{0,1\}^n$). Which of the following are PRFs? (Prove or give a counter-example for your answers)

   (a) $\mathsf{F}_1(k_1||k_2, x) := \mathsf{F}(k_1, x) \oplus \mathsf{F}(k_2, x)$

   (b) $\mathsf{F}_2(k_1||k_2, x_1||x_2) := \mathsf{F}(k_1, x_1) \oplus \mathsf{F}(k_2, x_2)$

   (c) $\mathsf{F}_3(k, x) := \mathsf{F}(k, x) \oplus \mathsf{F}(k, \mathsf{F}(k, x))$

   (d) $\mathsf{F}_4(k, x) := \mathsf{F}(k, x) \oplus x$

   (e) $\mathsf{F}_5(k, x) := \mathsf{F}(0^n, x)||\mathsf{F}(k, x)$

2. Prove or disprove the following statement: if $\mathsf{G} : \{0,1\}^n \to \{0,1\}^{2n}$ is a secure PRG then $\mathsf{F}(k, x) := \mathsf{G}(k||x)$ is a secure PRF where F maps an n-bit key and an n-bit input into a $4n$-bit output.

Problem 2

1. Let $\mathsf{F} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ be a secure PRF (i.e. a PRF where the key space and input space are $\{0,1\}^n$ and the output space is $\{0,1\}$). Construct a new PRF $\mathsf{F}' : \{0,1\}^{n+1} \times \{0,1\}^n \to \{0,1\}$ such that if the adversary knows the last bit of the key, this function is no longer pseudorandom.

2. Assuming that pseudorandom functions exist, construct an encryption scheme that is multi-message secure but not CPA secure.

Problem 3

Let $\mathsf{F} : \{0,1\}^n \times \{0,1\}^{3n} \to \{0,1\}^{3n}$ be a strong pseudorandom permutation. Prove that the following encryption scheme is CCA secure.

- To encrypt $x \in \{0,1\}^n$ with key k, choose $r \xleftarrow{R} \{0,1\}^n$, and output $F(k, x||r||0^n)$.
- To decrypt $y \in \{0,1\}^{3n}$, first compute $x||r||w = F^{-1}(k, y)$. If $w \neq 0^n$ then output $\perp$; Otherwise, output x.

Problem 4

Let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a CPA secure scheme. Prove that the scheme $\Pi' = (\mathsf{Gen}, \mathsf{Enc}', \mathsf{Dec}')$ such that $\mathsf{Enc}'(k, m) := \mathsf{Enc}(k, \mathsf{Enc}(k, m))$ is also CPA secure.