


دانشکده علوم ریاضی

مقدمه‌ای بر رمزنگاری تحویل اصلی ۱۹ آذر ۱۴۰۲

تمرین: سری ۳

مدرّس : دکتر شهرام خزائی *تحویل نهایی: ۲۶ 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 Sina Ghasemi Nezhad via the Telegram ID `@Sina_Qane` or the email `sina.ghaseminejad@gmail.com`.

Problem 1

Let $\{p_k\}_{k\in\{0,1\}^*}$ be a pseudorandom permutation collection, where for $k \in \{0,1\}^n$, p_k is a permutation over $\{0,1\}^m$.

1. Consider the following encryption scheme $(E, D) : E_k(x) = p_k(x), D_k(y) = p_k^{-1}(y)$. Prove that this scheme is not a CPA-secure encryption.

2. Consider the following scheme (E, D) that encrypts $m/2$-bit messages in the following way: on input $x \in \{0,1\}^{m/2}$, E_k chooses random $r \leftarrow_R \{0,1\}^{m/2}$ and outputs $p_k(x, r)$ (where comma denotes concatenation), on input $y \in \{0,1\}^m$, D_k computes $(x, r) = p_k^{-1}(y)$ and outputs x. Prove that (E, D) is a CPA-secure encryption scheme.

Problem 2

Show that CBC-MAC is not a secure MAC when an adversary can obtain authorization tags on massages of different lengths.

Problem 3

Let $(\text{Gen}; \text{Mac}; \text{Ver})$ be a secure MAC defined with key, message and tag spaces K, M and T where $M = \{0,1\}^n$ and $T = \{0,1\}^{128}$. Which of the following is a secure MAC? provide a brief proof for your answer.

1. $\text{Mac}'(k, m) = \text{Mac}(k, m||m)$
   $\text{Ver}'(k, m, t) = \text{Ver}(k, m||m, t)$

2. $\text{Mac}'(k, m) = \langle \text{Mac}(k, m), \text{Mac}(k, 0^n) \rangle$
   $\text{Ver}'(k, m, \langle t_1, t_2 \rangle) = \text{Ver}(k, m, t_1) \wedge \text{Ver}(k, 0^n, t_2)$

3. $\text{Mac}'(k_1||k_2, m) = \langle \text{Mac}(k_1, m), \text{Mac}(k_2, m) \rangle$
   $\text{Ver}'(k_1||k_2, m, \langle t_1, t_2 \rangle) = \text{Ver}(k_1, m, t_1) \wedge \text{Ver}(k_2, m, t_2)$

4. $\text{Mac}'(k, m) = \text{Mac}(k, m)$
   $\text{Ver}'(k, m, t) = \text{Ver}(k, m, t) \vee \text{Ver}(k, m \oplus 1^n, t)$

Problem 4

Let h be a collision-resistant hash-function.

1. Consider
$$h_s^0(x) = \begin{cases} h_s(x)||1 & \text{if } x_1 = 0 \\ 0^{|h_s(x)|+1} & \text{otherwise} \end{cases}$$
$$h_s^1(x) = \begin{cases} h_s(x)||1 & \text{if } x_1 = 1 \\ 0^{|h_s(x)|+1} & \text{otherwise} \end{cases}$$
Prove that $\hat{h}_s(x) = h_s^0(x)||h_s^1(x)$ is collision-resistant.

2. Now let
$$h_s^a(x) = h_s(x)_1 \dots h_s(x)_{\lceil \frac{|h_s(x)|}{2} \rceil}$$
$$h_s^b(x) = h_s(x)_{\lceil \frac{|h_s(x)|}{2} \rceil + 1} \dots h_s(x)_{|h_s(x)|}$$
where the i-th bit of a string x is denoted by x_i. Prove or disprove that at least one of h_s^a and h_s^b is collision resistant.

3. Answer part 2 in the case that the output of h_s^a and h_s^b is equal for every input x. Prove your answer.

Problem 5

1. Suppose we are given two hash functions $H_1, H_2 : \{0,1\}^* \to \{0,1\}^n$ and are told that both hash functions are collision resistant. We, however, do not quite trust these claims. Our goal is to build a hash function $H_{12} : \{0,1\}^* \to \{0,1\}^m$ that is collision resistant assuming at least one of H_1, H_2 are collision resistant. Give the best construction you can for H_{12} and prove that a collision finder for your H_{12} can be used to find collisions for both H_1 and H_2 (this will prove collision resistance of H_{12} assuming one of H_1 or H_2 is collision resistant). Note that a straight forward construction for H_{12} is fine, as long as you prove security in the sense above.

2. Same questions as part 1 for Message Authentication Codes (MACs). Prove that an existential forger under a chosen message attack on your MAC_{12} gives an existential forger under a chosen message attack for both MAC_1 and MAC_2. Again, a straight forward construction is acceptable, as long as you prove security. The proof of security here is a bit more involved than in part 1.