**دانشکده‌ی علوم ریاضی**

| | | |
|---|---|---|
| **رمز نگاری** | | تحویل اصلی ۲۲ آذر ۱۴۰۲ |
| | # تمرین : سری ۴ | |
| *مدرّس : دکتر شهرام خزائی* | | *تحویل نهایی ۶ دی* |

- 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 Emad Zinoghli via `emadzinoghli@gmail.com`.

## Problem 1

Let $\Pi_E = (\text{Gen}_1, \text{Enc}, \text{Dec})$ be any CPA secure encryption scheme, and let $\Pi_M = (\text{Gen}_2, \text{Mac}, \text{Vrfy})$ be any MAC scheme that is existentially unforgeable under chosen message attacks. Consider the following encryption systems and argue whether they are an authenticated encryption scheme. Note that $K_1, K_2$ are the outputs of $\text{Gen}_1, \text{Gen}_2$, respectively.

1. $\text{E}_{K_1,K_2}(M) = (M, \text{Mac}_{K_2}(\text{Enc}_{K_1}(M)))$.
2. $\text{E}_{K_1,K_2}(M) = (C = \text{Enc}_{K_1}(M), \text{Mac}_{K_2}(C))$.
3. $\text{E}_{K_1,K_2}(M) = (\text{Enc}_{K_1}(M), \text{Mac}_{K_2}(M))$.
4. $\text{E}_{K_1,K_2}(M) = \text{Enc}_{K_1}((M, \text{Mac}_{K_2}(M)))$.

## Problem 2

Consider the following hash functions and describe how to efficiently find collisions in each .

1. $H((x, y)) = \pi(y, x \oplus y) \oplus y$ where $\pi : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ is an efficient pseudorandom permutation.
2. $H((x, y)) = \pi(x \oplus y, x)$ where $\pi : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ is an efficient pseudorandom permutation.
3. $H : \{0,1\}^{n+1} \to \{0,1\}^n$ such that

$$H((x, b)) = \begin{cases} H'(x) & b = 0 \\ H'(H'(x)) & b = 1 \end{cases} \tag{1}$$

   where $H' : \{0,1\}^* \to \{0,1\}^n$ is a collision resistant hash function.

## Problem 3

Suppose $\Pi_M = (\text{Gen}_M, \text{Mac}, \text{Vrfy})$ is existentially unforgeable under chosen message attack and $\Pi_H = (\text{Gen}_H, H)$ is a collision resistant hash function. Define $\Pi'_M = (\text{Gen}', \text{Mac}', \text{Vrfy}')$ as follows.

1. On $1^n$, $\text{Gen}'$ runs $\text{Gen}_M$ and $\text{Gen}_H$ to obtain $k$ and $s$, respectively.
2. $\text{Mac}'_k(m) = \text{Mac}_k(H^s(m))$.
3. $\text{Vrfy}'_k(m, \sigma) = \text{Vrfy}_k(H^s(m), \sigma)$.

Prove $\Pi'_M$ is existentially unforgeable under chosen message attack ($s$ is public).

# Problem 4

Assume collision resistant hash functions exist. Show a construction of a fixed-length hash function $(\text{Gen}, h)$ that is non collision resistant, but its Merkle-Damgard transform (according to construction 5.3) $(\text{Gen}, H)$ is collision resistant.

# Problem 5

For each of the following modifications to the Merkle–Damgard transform (Construction 5.3), determine whether the result is collision resistant. If yes, provide a proof; if not, demonstrate an attack.

1. Modify the construction so that the input length is not included at all (i.e., output $z_B$ and not $z_{B+1} = h^s(z_B L)$). (Assume the resulting hash function is only defined for inputs whose length is an integer multiple of the block length.)
2. Modify the construction so that instead of outputting $z = h^s(z_B L)$, the algorithm outputs $z_B L$.
3. Instead of using an $IV$, just start the computation from $x_1$. That is, define $z_1 := x_1$ and then compute $z_i := h^s(z_{i-1} x_i)$ for $i = 2, \ldots, B+1$ and output $z_{B+1}$ as before.
4. Instead of using a fixed $IV$, set $z_0 := L$ and then compute $z_i := h^s(z_{i-1} x_i)$ for $i = 1, \ldots, B$ and output $z_B$.