دانشکده‌ی علوم ریاضی

رمزنگاری		تحویل اصلی ۳۰ دی
	# تمرین : سری ۳	
مدرّس : دکتر شهرام خزائی		*تحویل نهایی ۷ بهمن*

- 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 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.
- **One problem is optional.**
- For any question contact Ali Adibifar via @Aliadibifar.

Problem 1

Let (Gen_1, Enc, Dec) be any CPA secure encryption scheme, and let (Gen_2, MAC, Ver) be any MAC scheme that is existentially unforgeable under Chosen Message Attacks. Consider the encryption scheme (Gen_0, Enc_0, Dec_0), where Gen_0 generates K_1 according to Gen_1, and K_2 according to Gen_2, and where Enc_0 is one of the following encryption algorithms:

1. $\mathrm{Enc}_0((K_1, K_2), M) = M||\mathrm{MAC}(K_2, \mathrm{Enc}(K_1, M))$
2. $\mathrm{Enc}_0((K_1, K_2), M) = \mathrm{Enc}(K_1, M)||\mathrm{MAC}(K_2, M)$
3. $\mathrm{Enc}_0((K_1, K_2), M) = C||\mathrm{MAC}(K_2, C)$ where $C = \mathrm{Enc}(K_1, M)$
4. $\mathrm{Enc}_0((K_1, K_2), M) = \mathrm{Enc}(K_1, M||\mathrm{MAC}(K_2, M))$

where || denotes concatenation. For each of these encryption schemes, briefly explain why or why not the scheme is guaranteed to be CCA secure.

Problem 2

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

1. $\mathrm{Mac}'(k, m) = \mathrm{Mac}(k, m||m)$

   $\mathrm{Ver}'(k, m, t) = \mathrm{Ver}(k, m||m, t)$
2. $\mathrm{Mac}'(k, m) = \langle \mathrm{Mac}(k, m), \mathrm{Mac}(k, 0^n) \rangle$

   $\mathrm{Ver}'(k, m, \langle t_1, t_2 \rangle) = \mathrm{Ver}(k, m, t_1) \wedge \mathrm{Ver}(k, 0^n, t_2)$
3. $\mathrm{Mac}'(k_1||k_2, m) = \langle \mathrm{Mac}(k_1, m), \mathrm{Mac}(k_2, m) \rangle$

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

   $\mathrm{Ver}'(k, m, t) = \mathrm{Ver}(k, m, t) \vee \mathrm{Ver}(k, m \oplus 1^n, t)$

Problem 3

Let $\Pi = (\text{Gen}, H)$ be a collision resistant hash function and define the hash function $\Pi' := (\text{Gen}, \tilde{H})$ such that

$$\tilde{H}^s(x) := H^s(H^s(x)).$$

Prove or disprove: Π' is a collision resistant hash function.

Problem 4

Let F be a keyed function that is a secure (deterministic) MAC for messages of length n. (Note that F need not be a pseudorandom permutation.) Show that basic CBC-MAC is not necessarily a secure MAC (even for fixed-length messages) when instantiated with F.

Problem 5

Let h be a collision-resistant hash-function. Consider

- $$h_s^0(x) = \begin{cases} h_s(x)||1 & x_1 = 0 \\ 0^{|h_s(x)|+1} & \text{otherwise} \end{cases}$$

  $$h_s^1(x) = \begin{cases} h_s(x)||1 & x_1 = 1 \\ 0^{|h_s(x)|+1} & \text{otherwise} \end{cases}$$

- $\tilde{h}_s(x) = h_s^0(x)||h_s^1(x)$

Prove that $\tilde{h}$ is collision-resistant.