دانشکده‌ی علوم ریاضی

مقدمه‌ای بر رمزنگاری		مهلت اصلی: ۱۰ خرداد ۹۸
	تمرین شماره ۴	
مدرّس: دکتر شهرام خزائی		مهلت نهایی: ۱۷ خرداد ۹۸

- 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.
- 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 before hard deadline.
- You can not submit any time after hard deadline.
- All problem sets include at least 150 points which is the full score.
- Answering questions marked with (*) is mandatory.
- You can gain up to 180 points by answering unmarked questions.
- For any question contact `pouria.fallahpour@gmail.com`

Problem 1*

Let H be a collision resistant hash function. Which of the following is collision resistant? briefly prove your answer. (as usual, we use $\|$ to denote string concatenation) (20 Points)

1. $H_1(m) = H(m\|0)$
2. $H_2(m) = H(m\|m)$
3. $H_3(m) = H(m)[0, \ldots, 31]$ (i.e. output the first 32 bits of the hash)

4. $H_4(m) = H(m) \| H(0)$
5. $H_5(m) = H(|m|)$ (i.e. hash the length of m)
6. $H_6(m) = H(m) \oplus H(m \oplus 1^{|m|})$ (where $m \oplus 1^{|m|}$ is the complement of m)

Problem 2*

Let $H : \{0,1\}^\star \to \{0,1\}^n$ be a *good* hash function. We know that finding a collision on H can be done with $O(2^{n/2})$ random samples of H. How many random samples would it take until we obtain a three way collision, namely distinct strings x,y,z such that $H(x) = H(y) = H(z)$? (15 Points)

Problem 3*

Let F be a pseudorandom function. Show that the following MAC for messages of length $2n$ is insecure: The shared key is a random $k \in \{0,1\}^n$. To authenticate a message $m_1||m_2$ with $|m_1| = |m_2| = n$, compute the tag $\langle F_k(m_1), F_k(F_k(m_2))\rangle$. (10 Points)

Problem 4*

An attacker intercepts the following ciphertext (hex encoded):

```
20814804c1767293b99f1d9cab3bc3e7 ac1e37bfb15599e5f40eef805488281d
```

He knows that the plaintext is the ASCII encoding of the message "`Pay Bob 100 $`" (excluding the quotes). He also knows that the cipher used is CBC encryption with a random IV using AES as the underlying block cipher. Show that the attacker can change the ciphertext so that it will decrypt to "`Pay Bob 500 $`". What is the resulting ciphertext (hex encoded)? This shows that CBC provides no integrity. (10 Points)

Problem 5*

Say $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ is a secure MAC, and for $k \in \{0,1\}^n$ the tag generation algorithm Mac_k always outputs tags of length $t(n)$. Prove that t must be supe-logarithmic or, equivalently, that if $t(n) = O(\log n)$ then Π cannot be a secure MAC. (15 Points)
Hint: Consider the probability of randomly guessing a valid tag.

Problem 6

Provide formal definitions for second pre-image resistance and pre-image resistance. Prove that any hash function that is collision resistant is second pre-image resistant, and that any hash function that is second pre-image resistant is pre-image resistant. (30 Points)

Problem 7

Suppose H_1 and H_2 are collision resistant hash functions. Argue about the collision resistance of $G_1(m) = H_2(H_1(m))$ and $G_2(m) = H_1(m) \| H_1(m)$. Now suppose that H_1 is collision resistant but H_2 is not. How do you answer the question this time? What about $G_3(m) = H_1(H_2(m))$? (15 Points)

Problem 8

Let (Gen_1, H_1) and (Gen_2, H_2) be two hash functions. Define (Gen, H) so that Gen runs Gen_1 and Gen_2 to obtain keys s_1 and s_2 , respectively. Then define $H^{s_1,s_2}(x) = H_1^{s_1}(x)||H_2^{s_2}(x)$.

- Prove that if at least one of (Gen_1, H_1) and (Gen_2, H_2) is collision resistant, then (Gen, H) is collision resistant.(10 Points)
- Determine whether an analogous claim holds for second pre-image resistance and pre-image resistance, respectively. Prove your answer in each case. (15 Points)

Problem 9

We call the triple $\Pi = (\mathsf{Gen}, \mathsf{E}, \mathsf{D})$ a tweakable block cipher on message space $\mathcal{M}$ and tweak space $\mathcal{T}$

- $k \leftarrow \mathsf{Gen}(1^n)$ is the key generation algorithm that on input 1^n generates a key $k \in \mathcal{K}$
- $c \leftarrow \mathsf{E}_k(t, m)$ is deterministic permutation that maps a message $m \in \mathcal{M}$, a key $k \in \mathcal{K}$ and a tweak value $t \in \mathcal{T}$ to $c \in \mathcal{M}$
- $m \leftarrow \mathsf{D}_k(t, c)$ is the inverse permutation that maps a ciphertext $c \in \mathcal{M}$, a key $k \in \mathcal{K}$ and a tweak value $t \in \mathcal{T}$ to message $m \in \mathcal{M}$ such that $\forall m \in \mathcal{M}\ \forall k \in \mathcal{K}\ \forall t \in \mathcal{T} : \mathsf{Dec}_k(t, \mathsf{Enc}_k(t, m)) = m$.

A tweakable block cipher is said to be secure if no efficient adversary can distinguish it from random permutations even for tweak values of his choice. Give a formal definition of the security of a tweakable block cipher. (15 Points)
Let $\mathsf{E}_k(x)$ be a (normal) secure block cipher with $\mathcal{K} = \{0,1\}^n$ and $\mathcal{M} = \{0,1\}^n$ for security parameter n. Consider the following tweakable block cipher:

$$\mathsf{E}'_{k_1\|k_2}(t,x) = \mathsf{E}_{k_1}(x) \oplus \mathsf{E}_{k_2}(t)$$

What is the corresponding inverse permutation. Is this tweakable block cipher secure? (15 Points)

Problem 10

Suppose we are given a block cipher $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ operating on domain χ. We want a block cipher $(\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ that operates on a smaller domain $\chi' \subset \chi$ and defined as follows:

$\mathsf{Enc}'(k,x) := y \leftarrow \mathsf{Enc}(k,x)$
while $y \notin \chi'$ do: $y \leftarrow \mathsf{Enc}(k,y)$
output y

$\mathsf{Dec}'(k,y)$ is defines analogously, applying $\mathsf{Dec}(k,.)$ until the result falls in χ'. Clearly $(\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ are defined on domain χ'.

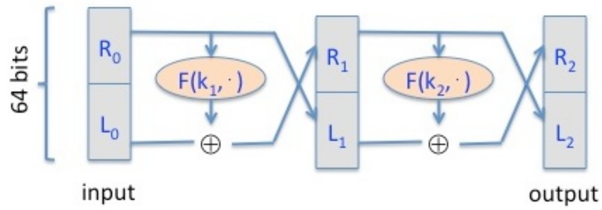
- With $t := |\chi|/|\chi'|$, how many evaluations of Enc are needed in expectation to evaluate $\mathsf{Enc}'(k,x)$ as a function of t? (15 Points)
- Show that if $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is a secure block cipher with domain χ then $(\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ is a secure block cipher with domain χ'. Try proving security bu induction on $|\chi| - |\chi'|$ (25 Points)

Problem 11

Find real collisions for the following two compression functions:

- $f_1(x,y) = AES(y,x) \oplus y$, and
- $f_2(x,y) = AES(x,x) \oplus y$

where $AES(x,y)$ is the AES-128 encryption of y under key x. You can use any publicly available AES source code. (15 Points)



Problem 12

- Show that DES has the property that $DES_k(x) = \overline{DES_{\bar{k}}(\bar{x})}$ for every key k and input x (where z denotes the bitwise complement of z). This is called the complementarity property of DES. (The description of DES given in chapter 5 of Katz-Lindell is sufficient for this exercise.)(10 Points)

- Use the previous exercise to show how it is possible to find the secret key in DES (with probability 1) in time 2^{55}. (Hint: Use a chosen-plaintext attack with two carefully chosen plaintexts.) (15 Points)

Problem 13

Recall that the Luby-Rackoff theorem states that applying a four round Feistel network to a secure PRF gives a secure block cipher. Let's see what goes wrong if we only use a two round Feistel. Let $F : \{0,1\}^n \times \{0,1\}^{32} \to \{0,1\}^{32}$ be a secure PRF. Recall that a 2-round Feistel defines the follwoing keyed permutation $E : \{0,1\}^{2n} \times \{0,1\}^{64} \to \{0,1\}^{64}$ where R_0 is the right 32 bits of the 64-bit input and L_0 is the left 32 bits:

1. Draw the inverse permutation. (5 Points)

2. One of the following lines is the output of E using a random key, while the other three are the output of a truly random permutation $f : \{0,1\}^{64} \to \{0,1\}^{64}$. All 64-bit outputs are encoded as 16 hex characters. Can you say which is the output of the PRP? (10 Points)

   (a) On input 0^{64} the output is `9d1a4f78 cb28d863`. On input $1^{32}0^{32}$ the output is `75e5e3ea 773ec3e6`.

   (b) On input 0^{64} the output is `7b50baab 07640c3d`. On input $1^{32}0^{32}$ the output is `ac343a22 cea46d60`.

   (c) On input 0^{64} the output is `e86d2de2 e1387ae9`. On input $1^{32}0^{32}$ the output is `1792d21d b645c008`.

(d) On input 0^{64} the output is `4af53267 1351e2e1`. On input $1^{32}0^{32}$ the output is `87a40cfa 8dd39154`.

3. Give a formal proof that why E is not a PRP by constructing an adversary $\mathcal{A}$ and computing its advantage. (10 Points)

Problem 14

Give a formal definition of security of a symmetric cryptosystem that is able to encrypt messages of length up to $l(n)$, for some polynomial $l(\cdot)$, and is able to hide the *length* of the message from *active* and *efficent* adversaries. (20 Points)