دانشکده‌ی علوم ریاضی

مقدمه‌ای بر رمزنگاری		مهلت اصلی: ۲۴ اردیبهشت ۹۸
	تمرین شماره ۳	
مدرّس: دکتر شهرام خزائی		مهلت نهایی: ۳۱ اردیبهشت 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 $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a secure PRF (i.e. a PRF where the key space, input space, and output space are all $\{0,1\}^n$) and say $n = 128$. Which of the following is a secure PRF (there is more than one correct answer): (20 Points)

1. $F'(k,x) = \begin{cases} F(k,x) & x \neq 0^n \\ 0^n & \text{otherwise} \end{cases}$

2. $F'(k,x) = \begin{cases} F(k,x) & x \neq 0^n \\ k & \text{otherwise} \end{cases}$

3. $F'(k_1||k_2), x) = F(k_1, x) \oplus F(k_2, x)$

4. $F'(k,x) = \text{reverse}(F(k,x))$ where $\text{reverse}(y_1 \ldots y_t) = y_t \ldots y_1$ where y_i is a bit

5. $F'(k,x) = F(k,x) \oplus 1^n$

6. $F'(k,x) = k \oplus x$

Problem 2*

Consider an extension of the definition of secure message authentication where the adversary is provided with both a Mac and a Vrfy oracle.

1. Provide a formal definition of security for this case. (10 Points)

2. Assume Π is a deterministic MAC using canonical verification (defined below) that satisfies Definition 3 in Lecture 16. Prove that Π also satisfies your definition. (10 Points)

> **Canonical verification.** For deterministic message authentication codes (that is, where Mac is a deterministic algorithm), the canonical way to perform verification is to simply re-compute the tag and check for equality. In other words, $\mathsf{Vrfy}_k(m,t)$ first computes $\tilde{t} = \mathsf{Mac}_k(m)$ and then outputs 1 if and only if $\tilde{t} = t$.

Problem 3*

Let G be a finite cyclic group with generator g for which the Diffie-Hellman function $\mathrm{DH}_g(g^x, g^y) = g^{xy}$ is difficult to compute when x, y are chosen unirformly at random from $\mathbb{Z}_{|G|}$. Which of the following functions is also difficult to compute: (20 Points)

1. $f(g^x, g^y) = g^{x-y}$

2. $f(g^x, g^y) = g^{2xy}$

3. $f(g^x, g^y) = \sqrt{g^{xy}}$

4. $f(g^x, g^y) = g^{x+y}$

Give a precise reduunction for one of the difficult ones.

Problem 4*

Let $(\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ 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. (25 Points)

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

2. $\mathsf{Mac}'(k,m) = \mathsf{Mac}(k,m)$
   $\mathsf{Vrfy}'(k,m,t) = \begin{cases} \mathsf{Vrfy}(k,m,t) & m \neq 0^n \\ 1 & \text{oth} \end{cases}$

3. $\langle t, t\rangle \leftarrow \mathsf{Mac}'(k,m)$ where $t \leftarrow \mathsf{Mac}(k,m)$
   $\mathsf{Vrfy}'(k,m,\langle t_1,t_2\rangle) = \begin{cases} \mathsf{Vrfy}(k,m,t_1) & t_1 = t_2 \\ 0 & \text{oth} \end{cases}$

4. $\langle \mathsf{Mac}(k,m), \mathsf{Mac}(k,0^n)\rangle \leftarrow \mathsf{Mac}'(k,m)$
   $\mathsf{Vrfy}'(k,m,\langle t_1,t_2\rangle) = \mathsf{Vrfy}(k,m,t_1) \wedge \mathsf{Vrfy}(k,0^n,t_2)$

5. $\langle \mathsf{Mac}(k_1,m), \mathsf{Mac}(k_2,m)\rangle \leftarrow \mathsf{Mac}'(k_1||k_2,m)$
   $\mathsf{Vrfy}'(k_1||k_2,m,\langle t_1,t_2\rangle) = \mathsf{Vrfy}(k_1,m,t_1) \wedge \mathsf{Vrfy}(k_2,m,t_2)$

6. $\mathsf{Mac}'(k,m) = \mathsf{Mac}(k,m)$
   $\mathsf{Vrfy}'(k,m,t) = \mathsf{Vrfy}(k,m,t) \vee \mathsf{Vrfy}(k, m \oplus 1^n, t)$

Problem 5*

Let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a chosen ciphertext secure public-key encryption system with message space$\{0,1\}^{128}$. For which of the following $\Pi' = (\mathsf{Gen}, \mathsf{Enc}', \mathsf{Dec}')$ is also chosen ciphertext secure? (20 Points)

1. $\mathsf{Enc}'_{pk}(m) = \langle \mathsf{Enc}_{pk}(m), \mathsf{Enc}_{pk}(m)\rangle$
   and $\mathsf{Dec}'(sk,\langle c_1,c_2\rangle) = \mathsf{Dec}(sk,c_1)$ if $\mathsf{Dec}(sk,c_1) = D(sk,c_2)$ and $\perp$ otherwise.

2. $\mathsf{Enc}'_{pk}(m) = \langle \mathsf{Enc}_{pk}(m), \mathsf{Enc}_{pk}(0^{128})\rangle$ and $\mathsf{Dec}'(sk,\langle c_1,c_2\rangle) = \mathsf{Dec}(sk,c_1)$ if $\mathsf{Dec}(sk,c_2) = 0^{128}$ and $\perp$otherwise.

3. $\langle c, c\rangle \leftarrow \mathsf{Enc}'_{pk}(m)$ where $c \leftarrow \mathsf{Enc}_{pk}(m)$ and $\mathsf{Dec}'(sk,\langle c_1,c_2\rangle) = \mathsf{Dec}(sk,c_1)$ if $c_1 = c_2$ and $\perp$ otherwise.

4. $\mathsf{Enc}'_{pk}(m) = \mathsf{Enc}_{pk}(m \oplus 1^{128})$ and $\mathsf{Dec}'(sk,c) = \mathsf{Dec}(sk,c) \oplus 1^{128}$

Problem 6

Let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a symmetric encryption system with message space $\mathcal{M} = \{0,1\}^{256}$. Define the MAC system $(\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ for messages in $\mathcal{M}$ with

$$\mathsf{Mac}_k(m) := \mathsf{Enc}_k(m)$$

$$\mathsf{Vrfy}_k(m,t) := \begin{cases} 1 & \text{if } \mathsf{Dec}_k(t) = m \\ 0 & \textit{otherwise} \end{cases}$$

What is the property that the encryption system Π needs to satisfy for this MAC system to be secure? (10 Points)

Problem 7

Let $R := \{0,1\}^n$ and consider the familly of keyed functions $\{f_n : R^{n+1} \times R \to R\}_{n \in \mathbb{N}}$ defined as follows:

function $f_n(k, x)$
  [*assumes* $k = k[0], \ldots, k[n], x = x_0 \ldots x_{n-1}$ *where* $k[i] \in \{0,1\}^n, x_i \in \{0,1\}$]
  $t = k[0]$
  for $i = 1$ **to** n **do**
    if $x_{i-1} = 1$ **then**
      $t = t \oplus k[i]$
    end if
  end forreturn t
end function

For example for $n = 4$, we have $F(k, 0101) = k[0] \oplus k[2] \oplus k[4]$. Is this a secure PRF? (15 Points)

Problem 8

Suppose we modify the Diffie-Hellman protocol so that Alice operates as usual, namely chooses a random a in $\mathbb{Z}_p$ and sends to Bob $A \leftarrow g^a$. Bob, however, chooses a random b in $\mathbb{Z}_p^*$ and sends to Alice $B \leftarrow g^{1/b}$. What shared secret can they generate and how would they do it? (10 Points)

Problem 9

Let G be a finite cyclic group of order n and consider the following variant of ElGamal encryption in G:

- Gen: choose a random generator g in G and a random x in $\mathbb{Z}_n$. Output $pk = \langle g, h = g^x \rangle$ and $sk = \langle g, x \rangle$.
- $\mathsf{Enc}_{pk}(m)$: for $m \in G$, choose a random r in $\mathbb{Z}_n$ and output $\langle g^r, m \cdot h^r \rangle$.
- $\mathsf{Dec}_{sk}(\langle c_0, c_1 \rangle)$: output $\frac{c_1}{c_0^x}$

We showed in the class that this variant, called plain ElGamal, is CPA-secure under an appropriate assumption about G. Show that it is not however chosen-ciphertext secure. (10 Points)

Hint: use the homomorphic property of ElGamal.

Problem 10

Recall that with symmetric ciphers it is possible to encrypt a 32-bit message and obtain a 32-bit ciphertext (e.g., with the one time pad). Can the same be done with a secure public-key system?(only for fixed length messages such as 32-bits) (10 Points)

Problem 11

Consider the following MAC (a variant of this was used for WiFi encryption in 802.11b WEP). Let F be a PRF defined over $(\mathcal{K}, \mathcal{R}, \mathcal{X})$ where $\mathcal{X} := \{0,1\}^{32}$. Let CRC32 be a simple and popular error-detecting code meant to detect random errors; CRC32(m) takes inputs $m \in \{0,1\}^{\leq l}$ and always outputs a 32-bit string. For this exercise, the only fact you need to know is that $CRC32(m_1) \oplus CRC32(m_2) = CRC32(m_1 \oplus m_2)$. Define the following MAC system $(\mathsf{Mac}, \mathsf{Vrfy})$:

$$\mathsf{Mac}_k(m) := \{\text{samples } r \text{ randomley from } R,\ t \leftarrow F_k(r) \oplus CRC32(m),\ \text{output } (r,t)\}$$

$$\mathsf{Vrfy}_k(m,(r,t)) := \{\text{accept if } t = F_k(r) \oplus CRC32(m) \text{ and reject otherwise}\}$$

Show that this MAC system is insecure.(25 Points)

Problem 12

For a given PRG $G : S \to \{0,1\}^L$, and a given adversary $\mathcal{A}$, consider the following attack game:

- the adversary sends an index i, with $0 \leq i \leq L-1$, to the challenger.
- the challenger chooses a random s from S and computes $r = G(s)$ and sends $r[0], r[1], ..., r[i-1]$ to the adversary. ($r[i]$ is the i'th bit of r)
- the adversary outputs $g \in \{0,1\}$

We say that $\mathcal{A}$ **wins** if $r[i] = g$, and we define $\mathcal{A}$'s **advantage** $\mathrm{adv}^{\mathrm{Pre}}_{\mathcal{A},\mathrm{G}}$ to be:

$$|\Pr[\mathcal{A}\ wins] - \frac{1}{2}|$$

We say that G is ***unpredictable*** if the value $\mathrm{adv}^{\mathrm{Pre}}_{\mathcal{A},\mathrm{G}}$ is negligible for all p.p.t adversaries $\mathcal{A}$.

Show that if G is secure, then it is unpredictable. (20 Points)

Problem 13

Let $\mathbb{G}$ be a cyclic group of prime order q generated by $g \in \mathbb{G}$.
Consider the following PRG defined over $(\mathbb{Z}_q^2, \mathbb{G}^3)$:

$$G(\alpha, \beta) := (g^\alpha, g^\beta, g^{\alpha\beta})$$

Show that G is a secure PRG assuming DDH holds in $\mathbb{G}$. (15 Points)

Problem 14

Let F be a pseudorandom permutation, and define a fixed-length encryption scheme $(\mathsf{Enc}, \mathsf{Dec})$ as follows: On input $m \in \{0,1\}^{\frac{n}{2}}$ and key $k \in \{0,1\}^n$, algorithm Enc chooses a uniform string $r \in \{0,1\}^{\frac{n}{2}}$ of length $\frac{n}{2}$ and computes $c := F_k(r||m)$. Show how to decrypt, and prove that this scheme is CPA-secure for messages of length $\frac{n}{2}$. (20 Points)