دانشکده‌ی علوم ریاضی

رمز نگاری		تحویل اصلی ۱۸ خرداد
	# تمرین : سری ۷	
مدرّس : دکتر شهرام خزائی		*تحویل نهایی ۲۵ خرداد*

- 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 Arash ashoori via `arashashoori199821@gmail.com`.

Problem 1

(25 points) Let (G, S, V) be a secure signature scheme with message space $\{0,1\}^n$. Which one of the following signature schemes is secure? Either prove the security of the scheme, or construct an attacker.
G_1 and G_2 both run G twice and get two pairs of keys:
$G(1^n) \to (pk_0, sk_0)$, $G(1^n) \to (pk_1, sk_1)$.

Scheme1: Let the message space be $\{0,1\}^n$.
$S_1((sk_0, sk_1), m) = (S(sk_0, m), S(sk_1, m))$
$V_1((pk_0, pk_1), m, (\sigma_0, \sigma_1)) = 1 \iff [V(pk_0, m, \sigma_0) = 1 \ \vee \ V(pk_1, m, \sigma_1) = 1]$

Scheme2: Let the message space be $\{0,1\}^{2n}$. On each message m, the scheme parses init to two n-bits strings m_L, m_R (i.e. $m = m_L || m_R$).
$S_2((sk_0, sk_1), m) = (S(sk_0, m_L), S(sk_1, m_R))$
$V_2((pk_0, pk_1), m, (\sigma_0, \sigma_1)) = 1 \iff V(pk_0, m_L, \sigma_0) = V(pk_1, m_R, \sigma_1) = 1$

Problem 2

(25 points) For the following problem you may consult the following lecture note, or any other online/offline resources that you may find usefull. But you are not allowed to consult any person.
`https://www.cs.bu.edu/~reyzin/teaching/cryptonotes/notes-9.pdf`

A signature scheme Π is a one-time secure if there exists a negligible function $\epsilon(n)$ such that for all probabilistic polynomial time adversary $\mathcal{A}$, which can query the signature oracle once, we have:
$\Pr[\mathsf{Sign-Forge}_{\Pi,\mathcal{A}}(n) = 1] \le \epsilon(n)$.
Construct a one-time signature scheme with message space $\{0,1\}^k$ by using a one-way function.
Remark. A function $f : \{0,1\} \to \{0,1\}$ is called (strongly) one-way if the following two conditions holds:
1. *Easy to compute*: There exists a (deterministic) polynomial-time algorithm A such that on input x, the algorithm $\mathcal{A}$ outputs $f(x)$ (i.e., $\mathcal{A}(x) = f(x)$).
2. *Hard to invert*: For every probabilistic polynomial-time algorithm $\mathcal{A}$:
$\Pr[\mathcal{A}(f(U_n), 1^n) \in f^{-1}(f(U_n))] < \epsilon(n)$

Problem 3

For the following problem you may need to read some part of the following paper. Again, you are not allowed to consult any person.
`https://eprint.iacr.org/2018/847.pdf`

a) (10 points) A hinting PRG (GPRG) is informally defined as follows. Provide a formal definition of HPRG.
A HPRG is a PRG with a stronger security guarantee than the standard PRGs. A hinting PRG takes n bits as input, and outputs $(n+1)l$ output bits $z_0 z_1, \ldots, z_n$, where $|z_i| = l$. In the security game, the challenger outputs $2n+1$ strings, each of length l bits. In one scenario, all these $2n+1$ strings are uniformly random. In the other case, z_0 is always given to the adversary. More over, in the remaining $2n$ strings, half are obtained from the PRG evaluation, and the remaining half are uniformly random. Additionally, these $2n$ strings are arranged as a $2 \times n$ matrix, where in the i-th column, the top entry is pseudorandom (i.e., it is z_i) if the i-th bit of the input of the HPRG is 0, else the bottom entry is pseudorandom. For a hinting PRG scheme, it is required that these two senarios are indistinguishable for every PPT adversary.

b) (10 points) Show that a (standard) PRG is not necessarily hinting.

c) (10 points) CCA-1 security is a weaker variant of the CCA security game where the adversary is allowed to issue decryption queries **only** before sending the challenge messages.
The following construction turns a CPA-secure public key encryotion (PKE) scheme into a CCA-1-secure one. Provide a precise (i.e., formal) definition of the construction (i.e., the key generation, encryption and decryption algorithms).

Let $(\mathsf{Setup}, \mathsf{Enc}, \mathsf{Dec})$ be any CPA-secure PKE scheme, $H : \{0,1\}^n \to \{0,1\}^{(n+1)n}$ a hinting PRG, and G a pseudorandom generator with sufficiently long stretch.
The setup of the CCA-1-secure scheme runs the CPA-secure setup $2n$ times, obtaining $2n$ public/secret key pairs $\{pk_{b,i}, sk_{b,i}\}_{i \in \{1,..,n\}, b \in \{0,1\}}$.
To encrypt a message m, the encryption algorithm first chooses a uniformly random tag $t = t_1 t_2 ... t_n$, where each t_i is a sufficiently long string. Next, it chooses a seed $s \leftarrow \{0,1\}^n$ and computes $H(s) = z_0 z_1 ... z_n$ and the main ciphertext $c = m \oplus z_0$.
For each $i = 1, 2, \ldots, n$ the signal ciphertexts $c_{0,i}, c_{1,i}, c_{2,i}$ are computed as follows. If the i-th bit of s is 0, then $c_{0,i}$ is an encryption of a random string x_i using the public key $pk_{0,i}$ and randomness z_i, $c_{1,i}$ would be an encryption of 0^n using $pk_{1,i}$ (encrypted

using true randomness), and $c_{2,i} = G(x_i)$. And if the i-th bit of s is 1, then $c_{0,i}$ would be an encryption of 0^n using public key $pk_{0,i}$ (encrypted using true randomness), $c_{1,i}$ would be an encryption of a random string x_i using public key $pk_{1,i}$ and randomness z_i, and $c_{2,i} = G(x_i) + t_i$.
The final ciphertext includes the tag $t = (t_1 t_2 ... t_n)$, the main ciphertext c, and n signals ciphertexts $(c_{0,i}, c_{1,i}, c_{2,i})$.

d) (5 points) Prove the CCA-1 security of the above construction.