Problem Set 1

Instructions: You must typeset your solution in LaTeX using the provided template. Please submit your problem set via Gradescope.

Bugs: If it looks like there might be a mistake in the statement of a problem, please ask a clarifying question on Piazza.

Acknowledgment: Several of the problems in this problem set come from the Boneh-Shoup textbook.

Problem 1: Self-Referential Encryption [10 points]. Let us show that encrypting a key under itself can be dangerous. Let $E$ be a (one-time) semantically secure cipher defined over $(K, M, C)$, where $K \subseteq M$, and let $k \leftarrow R K$. A ciphertext $c* := Enc(k, k)$ that encrypts $k$ using $k$ is called a self referential encryption.

(a) Construct a cipher $E' = (Enc', Dec')$ derived from $E$ such that $E'$ is semantically secure, but becomes insecure if the adversary is given $Enc'(k, k)$ at the beginning of the semantic security game. Please provide the cipher, the attack, and a 1-2 sentence explanation for why it remains semantically secure if the adversary is not given $Enc'(k, k)$.

(b) Construct a cipher $E' = (Enc', Dec')$ derived from $E$ such that $E'$ is semantically secure and remains semantically secure (provably) even when the adversary is given $Enc'(k, k)$ at the beginning of the semantic security game. To prove that $E'$ is semantically secure, you should show the following: for every adversary $A$ that attacks $E'$, there exists an adversary $B$ that attacks $E$ such that (i) the running time of $B$ is about the same as that of $A$, and (ii) $SSAdv[A, E'] \leq SSAdv[B, E] + negl$.

Problem 2: Exercising the PRG definition [15 points]. Suppose $G$ is a secure PRG that outputs bit strings in $\{0,1\}^n$. Which of the following generators derived from $G$ are secure? For each one, either state “secure” or “insecure” followed by a short (1-2 sentence) justification. If it’s insecure, your justification should state an attack on PRG security.

(a) $G'(s) = (G(s), G(s))$

(b) $G'(s) = G(s) \oplus 1^n$

(c) $G'(s_1 || s_2) = G(s_1) \oplus G(s_2)$

(d) $G'(s_1 || s_2) = G(s_1) \land G(s_2)$ where $\land$ denotes bitwise AND

(e) $G'(s_1 || s_2) = (s_1, G(s_2))$

Problem 3: Key Leakage in PRFs [15 points]. Let $F$ be a secure PRF defined over $(K, X, Y)$, where $K = X = Y = \{0,1\}^n$. Let $K' = \{0,1\}^{n+1}$. Construct a new PRF $F'$, defined over $(K', X, Y)$, with the following properties: (i) the PRF $F'$ is secure, but (ii) if the adversary learns the last bit of the key then the PRF is no longer secure.
(a) Describe your construction for \( F' \), and show that it is insecure against an adversary who learns the last bit of the key, i.e., the challenger gives the adversary the last bit of the key at the beginning of the PRF security game. Please give a complete description of the PRF security adversary and state its advantage \( \text{PRFAdv}_{A,F} \). This shows that leaking even a single bit of the secret key can completely destroy the PRF security property. 

[Hint: Try changing the value of \( F \) at a single point.]

(b) Show that if \( F \) is a secure PRF, then \( F' \) is a secure PRF.

(c) Show how to use \( F \) to construct a PRF \( F'' \) that remains secure against an adversary who learns any single bit of the secret key, i.e., at the beginning of the PRF security game, the adversary sends the challenger a bit \( i \), and the challenger responds with the \( i \)th bit of the key. Your solution should not assume any property about \( F \) beyond the fact that it is a secure PRF. You do not need to give a full security proof for \( F'' \), just a short description of why it is secure and the general approach for the proof. 

[Hint: Consider using a larger key space.]

**Problem 4: CRHF Combiners [10 points].** We want to build a CRHF \( H \) using two CRHFs \( H_1 \) and \( H_2 \) such that if at some future time one of \( H_1 \) or \( H_2 \) is broken (but not both), then \( H \) is still secure.

(a) Show that \( H'(x) = H_1(H_2(x)) \) may not be secure if one of \( H_1 \) or \( H_2 \) is broken.

(b) Suppose \( H_1 \) and \( H_2 \) are defined over \((\mathcal{M},\mathcal{T})\). Let \( H(m) := (H_1(m), H_2(m)) \). Show that \( H \) is a secure CRHF if either \( H_1 \) or \( H_2 \) is secure.

**Problem 5: The 802.11b Insecure MAC [5 points].** Consider the following MAC (a variant of which was used for WiFi encryption in 802.11b WEP). Let \( F : K \times R \rightarrow \mathcal{Y} \) be a PRF where \( \mathcal{Y} = \{0,1\}^{32} \). Let the function \( \text{CRC32} : \{0,1\}^{\leq \ell} \rightarrow \{0,1\}^{32} \) be the simple and popular error-detecting code by that name, which is designed to detect random errors. Show that this attempted MAC scheme is insecure by describing an attack on existential unforgeability.

\[
\text{Sign}(k,m) := r \leftarrow \mathcal{R} \\
\quad t \leftarrow F(k,r) \oplus \text{CRC32}(m) \\
\quad \text{Output } (r,t) \\
\text{Verify}(k,m,(r,t)) : \text{if } t = F(k,r) \oplus \text{CRC32}(m): \text{output “accept”} \\
\quad \text{else: output “reject”}
\]

**Problem 6: Pseudorandomness and collision-resistance [10 points].** In class we saw that collision-resistance does not imply pseudorandomness. In this problem we will show that pseudorandomness doesn’t imply collision-resistance either. Suppose that \( G : \{0,1\}^k \rightarrow \{0,1\}^n \) is a secure PRG. Use \( G \) to construct a new PRG \( G' \) such that (i) \( G' \) is still a PRG, and (ii) \( G' \) is not collision-resistant.

(a) State your PRG \( G' \) and show that it is not collision-resistant.

(b) Prove that \( G' \) is a secure PRG assuming \( G \) is.
Problem 7: AE Practice [20 points]. For this problem, assume that the cipher $(\text{Enc}, \text{Dec})$ provides authenticated encryption, that $(\text{Enc}_{\text{CPA}}, \text{Dec}_{\text{CPA}})$ provides CPA security, and that $H$ is a collision resistant hash function. For each proposed cipher, state whether it provides AE, provides CPA security only, or provides neither AE nor CPA security. In each case, provide an attack on AE/CPA security and/or a proof sketch (in at most a few sentences each). Note that if you say a cipher provides CPA security, you will need to both show an attack on AE (ciphertext integrity) and a proof sketch for CPA security.

(a) $\text{Enc}'(k, m) := (\text{Enc}(k, m), \text{Enc}(k, m))$
   $\text{Dec}'(k, (c_1, c_2)) := \text{Dec}(k, c_1)$ if $\text{Dec}(k, c_1) = \text{Dec}(k, c_2)$; $\perp$ otherwise

(b) $\text{Enc}'(k, m) := (\text{Enc}(k, m), \text{Enc}(k, m))$
   $\text{Dec}'(k, (c_1, c_2)) := \text{Dec}(k, c_1)$ if $c_1 = c_2$; $\perp$ otherwise

(c) $\text{Enc}'(k, m) := (\text{Enc}_{\text{CPA}}(k, m), H(m))$
   $\text{Dec}'(k, (c_1, c_2)) := \text{Dec}_{\text{CPA}}(k, c_1)$ if $H(\text{Dec}_{\text{CPA}}(k, c_1)) = c_2$; $\perp$ otherwise

(d) $\text{Enc}'(k, m) := (\text{Enc}_{\text{CPA}}(k, m), H(\text{Enc}_{\text{CPA}}(k, m)))$
   $\text{Dec}'(k, (c_1, c_2)) := \text{Dec}_{\text{CPA}}(k, c_1)$ if $H(c_1) = c_2$; $\perp$ otherwise

Problem 8: An Attack on Android KeyStore [10 points]. Let $(E, D)$ be a secure block cipher (PRP) defined over $(\mathcal{K}, \mathcal{X})$, and let $(E_{\text{cbc}}, D_{\text{cbc}})$ be the cipher derived from $(E, D)$ using randomized CBC mode. Let $H : \mathcal{X}^{\leq L} \rightarrow \mathcal{X}$ be a collision resistant hash function. Consider the following attempt to build an AE-secure cipher over $(\mathcal{K}, \mathcal{X}^{\leq L}, \mathcal{X}^{\leq L+2})$:

$E'(k, m) := E_{\text{cbc}}(k, (H(m), m))$
$D'(k, c) : (t, m) \leftarrow D_{\text{cbc}}(k, c, )$
   if $t = H(m)$: output $m$
   else: output $\perp$

Note that, under this scheme, the encryption of a one-block message $m \in \mathcal{X}$ is a three-block ciphertext: the IV, a ciphertext block corresponding to $H(m)$, and a ciphertext block corresponding to $m$. Show that $(E', D')$ is not AE-secure by giving a chosen ciphertext attack on it. That is, show that it does not satisfy CCA security.

This construction was once used to protect secret keys in Android KeyStore. The chosen ciphertext attack resulted in a compromise of the key store, and this scheme is no longer in use.

[Hint: The attack only needs a single decryption query.]

Optional Feedback [5 points]. Please answer the following questions to help design future problem sets. You are not required to answer these questions (the points are free), and if you would prefer to answer anonymously, please use Piazza’s anonymous private post feature. However, we do encourage you to provide feedback on how to improve the course experience.

(a) Roughly how long did you spend on this problem set?

(b) What was your favorite problem on this problem set?
(c) What was your least favorite problem on this problem set?

(d) Any other feedback for this problem set? Was it too easy/difficult?

(e) Any other feedback on the course so far?