

Problem Set 2

Instructions: You **must** typeset your solution in LaTeX using the provided template. Please submit your problem set via Gradescope. Include your name and the names of any collaborators at the top of your submission.

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

Problem 1: 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 $F : \mathcal{K} \times \mathcal{R} \rightarrow \mathcal{Y}$ 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 that requires only a single MAC query and a very small number of additional operations, and succeeds with probability 1. You don't need to know anything about how CRC32 works to do the attack.

$\text{Sign}(k, m) := r \stackrel{\mathcal{R}}{\leftarrow}$

$t \leftarrow F(k, r) \oplus \text{CRC32}(m)$

Output (r, t)

Verify($k, m, (r, t)$): if $t = F(k, r) \oplus \text{CRC32}(m)$: output "accept"

else: output "reject"

Problem 2: 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 $G : \{0, 1\}^\lambda \rightarrow \{0, 1\}^n$ is a secure PRG. Use G to construct a new PRG $G' : \{0, 1\}^\lambda \rightarrow \{0, 1\}^n$ such that (i) G' is still a secure PRG, and (ii) G' is not collision-resistant.

- State your PRG G' and show that it is not collision-resistant. Note that G must take in λ bits and output n bits, same as G .
- Prove that G' is a secure PRG assuming G is.

Problem 3: AE Practice [20 points]. For this problem, assume that the cipher (Enc, 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) $\text{Enc}'(k, m) := c \leftarrow \text{Enc}(k, m)$; Output (c, c)
 $\text{Dec}'(k, (c_1, c_2)) := \text{Dec}(k, c_1)$ 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) $\text{Enc}'(k, m) := c \leftarrow \text{Enc}_{\text{CPA}}(k, m)$; Output $(c, H(c))$
 $\text{Dec}'(k, (c_1, c_2)) := \text{Dec}_{\text{CPA}}(k, c_1)$ if $H(c_1) = c_2$; \perp otherwise

Problem 4: 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. For this problem only, you are allowed to follow the link provided by the Boneh-Shoup textbook to the paper that presents the original attack.

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 the anonymous feedback form. 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?