Homework 3

Due: October 6, 2023

CS 1510: Intro. to Cryptography and Computer Security

1 CPA Security from PRFs and PRGs

Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a PRF and G be a PRG with expansion factor $\ell(n) = n + 1$. Consider the following encryption schemes based on F and G, where in each case, the shared key is a uniform $k \in \{0,1\}^n$.

For each scheme, state 1) whether the scheme is semantically secure, and 2) whether it is CPA-secure. Explain your answer.

a. To encrypt a message $m \in \{0,1\}^{n+1}$, choose a uniform $r \in \{0,1\}^n$ and output the ciphertext $\langle r, G(r) \oplus m \rangle$.

b. To encrypt $m \in \{0,1\}^n$, output the ciphertext $m \oplus F_k(0^n)$.

c. To encrypt $m \in \{0,1\}^{2n}$, parse m as $m_1 || m_2$ with $|m_1| = |m_2|$, then choose uniform $r \in \{0,1\}^n$ an send $\langle r, m_1 \oplus F_k(r), m_2 \oplus F_k(r+1) \rangle$.

2 Insecure MACs from PRFs

Let F be a PRF, and consider each of the following MAC constructions. In each case, Gen outputs a uniform $k \in \{0,1\}^n$ and $\langle i \rangle$ denotes an $\frac{n}{2}$-bit binary representation of the integer i.

For each construction, explain why the MAC is insecure, even if it is used to authenticate only fixed-length messages.

a. To authenticate a message $m = m_1, \ldots, m_\ell$, where $m_i \in \{0,1\}^n$, compute

$$t := F_k(m_1) \oplus \ldots \oplus F_k(m_\ell).$$

b. To authenticate a message $m = m_1, \ldots, m_\ell$, where $m_i \in \{0,1\}^{n/2}$, compute

$$t := F_k(\langle 1 \rangle || m_1) \oplus \ldots \oplus F_k(\langle \ell \rangle || m_\ell).$$

c. **Extra Credit.** Here is the original problem statement:

To authenticate a message $m = m_1, \ldots, m_\ell$, where $m_i \in \{0,1\}^{n/2}$, choose a uniform $r \leftarrow_\$ \{0,1\}^n$, compute

$$t := F_k(r) \oplus F_k(\langle 1 \rangle || m_1) \oplus \ldots \oplus F_k(\langle \ell \rangle || m_\ell),$$

and let the tag be $\langle r, t \rangle$.

In the new version, we explore the ambituity of the step "chose a uniform $r \leftarrow_\$ \{0,1\}^n$," and how this ambiguity affects the overall security of the proposed MAC. In particular, it's not quite clear from the wording who chooses this r. The following problems illustrate the importance of resolving this ambiguity.

(a) If the adversary is allowed to choose r, give an attack showing the given MAC is insecure.

(b) If r is chosen by the MAC's tag generation algorithm Mac, prove that the given MAC scheme is secure even for arbitrary-length messages (for simplicity, assume all messages have length a multiple of $\frac{n}{2}$).

3 Insecure Variable-Length CBC-MACs

In this problem, we will explore some nuanced difficulties with using CBC-MAC to authenticate messages of different lengths.

a. Consider the case in which the sender and receiver do not agree on the message length in advance. In this case, we have $\mathsf{Verify}_k(m,t) = 1$ if and only if $t = \mathsf{Mac}_k(m)$, regardless of the length of m. Say the sender is careful to only authenticate messages of length $2n$. Show that an aversary can forge a valid tag on a message of length $4n$.

b. Say the receiver only accepts 3-block messages. In this case, we have $\mathsf{Verify}_k(m,t) = 1$ if and only if $t = \mathsf{Mac}_k(m)$ *and* m has length $3n$. Say the sender authenticates messages of any length that is a multiple of n. Show that an adversray can forge a valid tag on a new message.

4 Secure Variable-Length CBC-MACs

Consider the following modification of the basic CBC-MAC construction. First, $\mathsf{Mac}_k(m)$ computes $k_\ell = F_k(\ell)$, where F is a PRF and ℓ is the length of m. Then, compute the tag using basic CBC-MAC with key k_ℓ. Verify is the CBC-MAC verification algorithm.

Prove that this modification gives a secure MAC for arbitrary-length messages. For simplicity, assume all messages have length a multiple of the block length. You may assume fixed-length CBC-MAC is secure.

5 Summary Question

Summarize the most important insights from this week's material, including from the lectures, notes, textbooks, homework problems, and other resources you find helpful, into a one-page resource. You will be permitted to use this one-page resource (along with the other weeks' resources) on the midterm and final.

Changes to this document prior to the exams are permitted, but for each change, you will be asked to state what you changed and why. For example, if you dropped something and replaced it with something else, justify why the thing you dropped wasn't as important as the thing you inserted, why you think it might be more useful for the exam, etc.

Please note that the purpose of this question is to help you organize and synthesize the material for your own future use. It will be graded based on completion—we will not be checking it for correctness.