CSE 5014: Cryptography and Network Security
2023 Spring Semester Written Assignment # 3
Due: May 9th, 2023, please submit at the beginning of class

Q.1 Let G be a pseudorandom generator (PRG) where $|G(s)| > 2 \cdot |s|$.

1. Define $G'(s) := G(s||0^{|s|})$. Is G' necessarily a pseudorandom generator?
2. Define $G'(s) := s_1||G(s_2)$, where $s = s_1||s_2$ and $s_1, s_2 \in \{0,1\}^{|s|/2}$. Is G' necessarily a pseudorandom generator?

Q.2 Consider the following keyed function F: for the security parameter n, the key is a matrix $A \in \mathbb{M}(n \times n, \mathbb{F}_2)$ and a vector $b \in \mathbb{F}_2^n$, where $\mathbb{F}_2$ denotes the field with 2 elements, i.e., $\mathbb{F}_2 = (\{0,1\}, \oplus, \cdot)$ and $\mathbb{F}_2^n$ denotes the corresponding vector space of dimension n. Now we define $F_{A,b} := \mathbb{F}_2^n \to \mathbb{F}_2^n$ by

$$F_{A,b} = Ax + b.$$

Decide whether F is a PRF and prove your answer.

Q.3 Let $\Pi = (Gen, Enc, Dec)$ be the CTR mode encryption scheme and $\tilde{\Pi} = (\tilde{Gen}, \tilde{Enc}, \tilde{Dec})$ be the encryption scheme obtained from Π by using a *truly random* function f instead of a pseudorandom function F_k (This is to say that $\tilde{Gen}$ picks uniformly $f \in Func_n$, while Gen picks uniformly $k \in \{0,1\}^n$, and $\tilde{Enc}$ uses f where Enc uses F_k. Show that there is a negligible function $negl$, such that for any PPT adversary A, it holds that

$$\left|\Pr[PrivK^{CPA}_{A,\Pi}(n) = 1] - \Pr[PrivK^{CPA}_{A,\tilde{\Pi}}(n) = 1]\right| \leq negl(n).$$

Q.4 Let F_k be a PRF and G be a PRG with expansion factor $n \mapsto n + 1$. For each of the following encryption schemes, decide whether the scheme has indistinguishable encryptions in the presence of an eavesdropper and whether it is a CPA-secure. (In each case, the shared key is a uniform $k \in \{0,1\}^n$.) Explain your answer.

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

(b) The one-time pad.

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

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

Q.5 The CBC construction is often used to get an encryption for larger message size. If $p : \{0,1\}^m \to \{0,1\}^m$ is a permutation, then $CBC_\ell\langle p \rangle$ is a permutation from $\{0,1\}^{\ell \cdot m}$ to $\{0,1\}^{\ell \cdot m}$ defined in the following way: for $x_1, \ldots, x_\ell \in \{0,1\}^m$, let $y_0 = 0^m$ and define $y_i = p(y_{i-1} \oplus x_i)$. Then, $CBC_\ell\langle p \rangle(x_1, \ldots, x_\ell) = (y_1, \ldots, y_\ell)$. Note that the inverse of $CBC_\ell\langle p \rangle$ can be computed in a similar way using the inverse of $p(\cdot)$.

Let $\{p_k\}$ be a pseudorandom permutation collection. Determine the CPA-security of the following two encryption schemes which are based on the CBC construction. That is, for each scheme either prove that it is CPA-secure or give an attack showing that it is not. For simplicity, we consider only the 3-block variant of the scheme (i.e., $\ell = 3$).

1. (*Padding in the end*) Given $p_k : \{0,1\}^m \to \{0,1\}^m$ and a message $x = x_1, x_2 \in \{0,1\}^{2m}$, E_k chooses $r \leftarrow_R \{0,1\}^m$ and outputs $CBC_3\langle p_k \rangle(x_1, x_2, r)$. Decrypting done in the obvious way.

2. (*Padding in the start*) Given $p_k : \{0,1\}^m \to \{0,1\}^m$ and a message $x = x_1, x_2 \in \{0,1\}^{2m}$, E_k chooses $r \leftarrow_R \{0,1\}^m$ and outputs $CBC_3\langle p_k \rangle(r, x_1, x_2)$. Decrypting done in the obvious way.

Q.6 Let F_k be a PRF. Show that each of the following MACs is insecure, even if used to authenticate fixed-length messages. (In each case *Gen* outputs a uniform $k \in \{0,1\}^n$ and $[i]_2$ denotes the $\frac{n}{2}$-bit binary encoding of i).

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

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

(b) To authenticate a message $m = m_1 \cdots m_\ell$, where $m_i \in \{0,1\}^{\frac{n}{2}}$, compute

$$t := F_k([1]_2||m_1) \oplus \cdots \oplus F_k([\ell]_2||m_\ell).$$

(c) To authenticate a message $m = m_1 \ldots m_\ell$, where $m_i \in \{0,1\}^{\frac{n}{2}}$, choose uniform $r \leftarrow \{0,1\}$, and compute

$$t := (r, F_k(r) \oplus F_k([1]_2||m_1) \oplus \cdots \oplus F_k([\ell]_2||m_\ell)).$$

Q.7 Let F_k be a PRF. Show that the following MAC for messages of length $2n$ is *insecure*: *Gen* outputs a uniform $k \in \{0,1\}^n$. To authenticate a message $m_1||m_2$ with $|m_1| = |m_2| = n$, compute the tag $F_k(m_1)||F_k(F_k(m_2))$

Q.8 Let (E, D) be a CPA secure scheme with key-size = message-size = n, and let $\{f_k\}$ be a collection of PRFs such that for every $k \in \{0,1\}^n$, $f_k : \{0,1\}^n \to \{0,1\}^n$. Consider the following scheme (E', D'):
Key k, k' each chosen uniformly and independently from $\{0,1\}^n$.
Encrypt $E'_{k,k'}(x) = (y, t)$ where $y = E_k(x)$ and $t = f_{k'}(y)$.
Decrypt $D'_{k,k'}(y, t) = \perp$ if $f_{k'}(y) \neq t$ and $D_k(y)$ otherwise.

1. Prove that the scheme (E', D') is CCA secure.

2. Let (E'', D'') be the same scheme except that we reuse the key for the PRFs and encryption. That is, we set $k = k'$ to be the same string chosen at random in $\{0,1\}^n$. Prove that this scheme is *not* necessarily even CPA secure! That is, show that there exists a CPA secure (E, D) and a PRF collection $\{f_k\}$ such that if we build (E'', D'') using these components then the resulting scheme is not CPA secure. Also, show that it is not CCA secure. (This example show that "reusing" or "recycling" keys in cryptography is very dangerous.)

Q.9 Prove the following modifications of basic CBC-MAC do not yield a secure MAC (even for fixed-length messages).

(1) Mac outputs all blocks $t_1, \ldots, t_\ell$, rather than just t_ℓ. (Verification only checks whether t_ℓ is correct.)

(2) A random initial block is used each time a message is authenticated. That is, choose uniform $t_0 \in \{0,1\}^n$, run basic CBC-MAC over the "message" t_0, $m_1, \ldots, m_\ell$, and output the tag $\langle t_0, t_\ell \rangle$. Verification is done in the natural way.

Q.10 Suppose that the Shenzhen Traffic Police Department comes up with a new license plate with a special serial number format. This serial number format consists of only 3 letters: first two being a digit (0 to 9) and last one being an English uppercase letter (A to Z). Each serial number is randomly generated when issued.

(1) Suppose that Alica and Bob apply for this new license plate. What is the probability that both of them receive the same plate number?

(2) Suppose that the Shenzhen Traffic Police Department wants to ensure that the probability that at least two license plates have the same number is less than 1%. What is the maximum number of this type of license plates that they can issue?

(3) Suppose that the Shenzhen Traffic Police Department wants to issue exactly 50 license plates. How many more DIGITs should be added at the end of this serial number format in order to ensure that the probability that at least two license plates have the same number is still less than 1%?

Q.11 Let (Gen, H) be a collision resistant hash function and define the hash function $\tilde{H} = (Gen, \tilde{H})$ such that

$$\tilde{H}^s(x) := H^s(H^s(x)).$$

Prove or disprove: $\tilde{H}$ is a collision resistant hash function.