1 (a). The crypto pledge (1 mark)

I promise that once I see how simple cryptographic constructions really are, I will not implement them in ***production code*** *even though it will be really fun. This agreement will remain in effect until I learn all about side-channel attacks and countermeasures to the point where I lose all interest in implementing them myself.*[1]

Name:

Entry Number:

Signature:

(This part is intentionally left blank for extra workspace)

[1] Taken from the course textbook, originally due to Jeff Moser.

1 (b). True/False (4 marks)

For each of the following questions, indicate whether the statement is true or false, and **provide a one-line justification for your answer**.

1. (1 mark) The signing algorithms of all MAC systems are also secure pseudorandom functions.

No! Consider MAC'(k,m)=MAC(k,m)||MAC(k,m)

2. (1 mark) Let $G : \{0,1\}^n \to \{0,1\}^{2n}$ be a secure pseudorandom generator. Since it is a secure PRG, the statistical distance of the following two distributions is bounded by a negligible function of n:

$$\mathcal{D}_0 := \left\{\text{Sample uniformly random } s \leftarrow \{0,1\}^n, \text{ output } G(s)\right\}$$
$$\mathcal{D}_1 := \left\{\text{Output uniformly random } u \leftarrow \{0,1\}^{2n}\right\}$$

No, the distance is in fact close to 1. Consider those points which are not in the range of G

3. (1 mark) If $(\mathsf{Sign}, \mathsf{Verify})$ is a secure MAC system, then at least some bits of m are guaranteed to be hidden if I give out $\sigma = \mathsf{Sign}(m, k)$.

This is not necessary. We can even make sign(m,k)=m||F(m,k)

4. (1 marks) If $G : \{0,1\}^n \to \{0,1\}^{2n}$ is a secure pseudorandom generator, then so is $H : \{0,1\}^n \to \{0,1\}^{2n}$ where $H(s) = G(s) \oplus G(0^n)$ for all $s \in \{0,1\}^n$.

Yes

1 (c). Multiple Choice Questions (8 marks)

For each of the following MCQs, select the correct option. **Provide a short justification**.

1. (2 marks) Consider a symmetric key encryption scheme $\mathcal{E}$ that satisfies Semantic Security. Then,

   (A) $\mathcal{E}$ is No-Query-Semantic-Security secure against **ALL (computationally unbounded)** adversaries.

   (B) There exists a **computationally unbounded** adversary that wins the No-Query-Semantic-Security game against scheme $\mathcal{E}$ with probability greater than 1/2.

   (C) Neither of the above. It depends on the scheme $\mathcal{E}$.

Let $F : \mathcal{X} \times \mathcal{K} \to \mathcal{Y}$ be a secure pseudorandom function with $\mathcal{X} = \mathcal{K} = \mathcal{Y} = \{0,1\}^n$ (here $\mathcal{K}$ is the key space). Consider the following keyed functions. For each of them, indicate whether the keyed function is a provably secure PRF, may be/may not be a secure PRF (depends on some additional properties of F), or is definitely insecure.

2. (2 marks) $F'(x,k) = F(x,k) \mid\mid F(x, F(x,k))$

   (A) F' is provably secure, assuming F is.

   (B) F' may/may not be a secure PRF. It requires some additional properties of F.

   (C) F' is an insecure PRF.

3. (2 marks) $F'(x, k) = F(x, k) \oplus x$

(A) F' is provably secure, assuming F is.

(B) F' may/may not be a secure PRF. It requires some additional properties of F.

(C) F' is an insecure PRF.

4. (2 marks) $F'(x, k) = F(x, k) \mid\mid F(x, x \oplus k)$

(A) F' is provably secure, assuming F is.

(B) F' may/may not be a secure PRF. It requires some additional properties of F.

(C) F' is an insecure PRF.

0^n

2. PRGs with large expansion (4 marks)

Let $G_1 : \{0,1\}^n \to \{0,1\}^{2n}$, and $G_2 : \{0,1\}^n \to \{0,1\}^{3n}$ be secure pseudorandom generators. Consider the following function $H : \{0,1\}^n \to \{0,1\}^{6n}$ defined as follows:

$$
\begin{gathered}
H(s) = y_1 \mid\mid y_2 \mid\mid \ldots \mid\mid y_5 \mid\mid y_6 \\
\text{where} \\
G_1(s) = s_0 \mid\mid s_1 \\
y_1 \mid\mid y_2 \mid\mid y_3 = G_2(s_0) \\
y_4 \mid\mid y_5 \mid\mid y_6 = G_2(s_1)
\end{gathered}
$$

Here, each y_i, s_0 and s_1 are n bit strings.

We will show that H is a secure pseudorandom generator, assuming G_1 and G_2 are secure PRGs. The proof will go via a sequence of hybrids. In World-0, the challenger samples a uniformly random $s \leftarrow \{0,1\}^n$ and sends $H(s)$. In World-1, the challenger chooses a $6n$-bit uniformly random string $u \leftarrow \{0,1\}^{6n}$ and sends u.

Define the intermediate hybrids required to prove security of H. No need to provide reductions for showing indistinguishability of hybrids.

(This page is intentionally left blank for extra workspace)

3. A broken encryption scheme (4 marks)

Let $P : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a secure pseudorandom permutation, and let P^{-1} be its inverse (that is, for all x, k, $P^{-1}(P(x,k),k) = x$). Consider the following encryption scheme with message space $\{0,1\}^{\ell \cdot n}$ for some $\ell > 3$:

- KeyGen: choose a random PRP key $k \leftarrow \{0,1\}^n$.
- $\mathsf{Enc}\Big(m = (m_1, \ldots, m_\ell), k\Big)$: choose a uniformly random string $x_0 \leftarrow \{0,1\}^n$ and set $\mathsf{ct}_0 = P(x_0, k)$.

  For $i = 1$ to ℓ, do the following:

  - set $x_i = m_i \oplus x_{i-1}$
  - compute $\mathsf{ct}_i = P(x_i, k)$.

  Output $\mathsf{ct} = (\mathsf{ct}_0, \mathsf{ct}_1, \mathsf{ct}_2, \ldots, \mathsf{ct}_\ell)$ as the final ciphertext.

- $\mathsf{Dec}\Big(\mathsf{ct} = (\mathsf{ct}_0, \mathsf{ct}_1, \ldots, \mathsf{ct}_\ell), k\Big)$: Let $y_0 = P^{-1}(\mathsf{ct}_0, k)$. For each $i = 1$ to ℓ, do the following:

  - compute $y_i = P^{-1}(\mathsf{ct}_i, k)$.
  - set $m_i = y_i \oplus y_{i-1}$

  Output $m = (m_1, m_2, \ldots, m_\ell)$ as the final decryption.

Show that the above scheme does not satisfy $\mathsf{No\text{-}Query\text{-}Semantic\text{-}Security}$**.**

(This page is intentionally left blank for extra workspace)

4. A new MAC scheme (4+1 marks)

Let $\mathsf{MAC} = (\mathsf{Sign}, \mathsf{Verify})$ be a MAC scheme with message space $\mathcal{M}$, key space $\mathcal{K}$ and signature space $\mathcal{T}$, satisfying **weak** unforgeability. Consider the following MAC scheme $\mathsf{MAC}' = (\mathsf{Sign}', \mathsf{Verify}')$:

- $\mathsf{Sign}'(m, k)$ = Compute $\sigma_1 \leftarrow \mathsf{Sign}(m, k)$, $\sigma_2 \leftarrow \mathsf{Sign}(m, k)$, output (σ_1, σ_2).
- $\mathsf{Verify}'(m, (\sigma_1, \sigma_2), k)$: Output 1 if either $\mathsf{Verify}(m, \sigma_1, k) = 1$ or $\mathsf{Verify}(m, \sigma_2, k) = 1$.

1. Is MAC' a **weakly** unforgeable MAC scheme, assuming MAC is? Yes

2. Suppose MAC is a **strongly** unforgeable message auth. code. Can we conclude that MAC' is also **strongly** unforgeable?

(This page is intentionally left blank for extra workspace)

(This page is intentionally left blank for extra workspace)

(This page is intentionally left blank for extra workspace)

(This page is intentionally left blank for extra workspace)

Definitions

Definition 04.01. *A function $\mu : \mathbb{N} \to [0,1]$ is said to be negligible if, for any polynomial $p(\cdot)$, there exists $n_0 \in \mathbb{N}$ such that for all $n > n_0$, $\mu(n) < 1/p(n)$.*

Definition 04.02. *An encryption scheme* $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *is said to satisfy no-query-semantic-security if, for any probabilistic polynomial time adversary $\mathcal{A}$, there exists a negligible function $\mu(\cdot)$ such that for all n,*

$$\Pr\left[\mathcal{A} \text{ wins the } \mathsf{No\text{-}Query\text{-}Semantic\text{-}Security} \text{ game}\right] \leq 1/2 + \mu(n)$$

where the No-Query-Semantic-Security *game is defined in Figure 1.*

> No-Query-Semantic-Security
>
> 1. Adversary sends two messages m_0, m_1 to the challenger, such that $|m_0| = |m_1|$.
> 2. The challenger chooses a bit $b \leftarrow \{0,1\}$, key $k \leftarrow \mathcal{K}$ and sends $\mathsf{Enc}(m_b, k)$ to the adversary.
> 3. The adversary sends its guess b', and wins the security game if $b = b'$.

Figure 1: The No-Query Semantic Security Game

Definition 05.01. *A deterministic polynomial time computable function $G : \{0,1\}^n \to \{0,1\}^\ell$ is a secure pseudorandom generator (PRG) if $\ell > n$, and for any prob. poly. time adversary $\mathcal{A}$, there exists a negligible function $\mu(\cdot)$ such that for all n,*

$$\Pr\left[\mathcal{A} \text{ wins the PRG security game against } G\right] \leq 1/2 + \mu(n),$$

where the PRG game is defined in Figure 2.

> PRG-Security
>
> 1. The challenger chooses a bit $b \leftarrow \{0,1\}$, string $s \leftarrow \{0,1\}^n$, $u_1 \leftarrow \{0,1\}^\ell$. It computes $u_0 = G(s)$, and sends u_b to the adversary.
> 2. The adversary sends its guess b', and wins the security game if $b = b'$.

Figure 2: The PRG Security Game

Definition 09.01. *A keyed function $F : \mathcal{X} \times \mathcal{K} \to \mathcal{Y}$ is a pseudorandom function (PRF) if, for any p.p.t. adversary $\mathcal{A}$, there exists a negligible function $\mu(\cdot)$ s.t. for all n,*

$$\Pr\left[\mathcal{A} \text{ wins the PRF security game}\right] \leq 1/2 + \mu(n),$$

where the PRF security game is defined in Figure 3.

PRF-Game

1. Challenger chooses a bit $b \leftarrow \{0,1\}$. If $b=0$, challenger chooses a key $k \leftarrow \mathcal{K}$ and sets function $F_0 \equiv F(\cdot, k)$. If $b=1$, challenger chooses a truly random function F_1 from the set of all functions mapping $\mathcal{X}$ to $\mathcal{Y}$. [a]
2. The adversary sends polynomially many queries. For each query $x \in \mathcal{X}$, the challenger sends $F_b(x)$.
3. Finally, after polynomially many queries, the adversary sends a guess b' and wins if $b' = b$.

[a] Note: there are only $|\mathcal{K}|$ keys, but the number of functions from $\mathcal{X}$ to $\mathcal{Y}$ is much more. In some sense, this is similar to what we saw for PRGs: in one case, the set of possible outputs was equal to the size of input domain, while in the other case, it was equal to size of output domain.

Figure 3: PRF Security Game

Definition 13.01. *Given two distributions $\mathcal{D}_0$ and $\mathcal{D}_1$ over the same sample space Ω, the statistical distance of $\mathcal{D}_0$ and $\mathcal{D}_1$ is defined as*

$$\mathsf{SD}(\mathcal{D}_0, \mathcal{D}_1) = \frac{1}{2}\left(\sum_{i\in\Omega}\left|\Pr_{x\leftarrow\mathcal{D}_0}[x=i] - \Pr_{x\leftarrow\mathcal{D}_1}[x=i]\right|\right)$$

Definition 15.01. *An encryption scheme $\mathcal{E} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ is said to satisfy* Semantic Security *if, for any p.p.t. adversaries $\mathcal{A}$, there exists a negligible function $\mu(\cdot)$ such that for all n,*

$$\Pr[\mathcal{A} \textit{ wins the } \mathsf{semantic\ security} \textit{ game }] \leq 1/2 + \mu(n)$$

where the probability is over the choice of key k, randomness used in Enc*, and the adversary's randomness.*

Semantic Security

1. **Setup:** Challenger chooses an encryption key $k \leftarrow \mathcal{K}$ and a bit $b \leftarrow \{0,1\}$.
2. **Challenge encryption queries:** Adversary sends polynomially many challenge encryption queries (adaptively). The i^{th} challenge pair consists of two messages $m_{i,0}, m_{i,1}$. The challenger sends $\mathsf{ct}_i = \mathsf{Enc}(m_{i,b}, k)$ to the adversary.

   Note that the bit b and key k were chosen during setup, and the same bit and key are used for all queries.
3. **Guess:** The adversary sends its guess b', and wins the security game if $b = b'$.

Figure 4: Semantic Security Game

Definition 18.01. *A MAC scheme $(\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Verify})$ is said to satisfy* Strong-UF-CMA *if, for any p.p.t. adversary $\mathcal{A}$, there exists a negligible function $\mu(\cdot)$ such that for all n,*

$$\Pr[\mathcal{A} \textit{ wins the strong unforgeability game}] \leq \mu(n).$$

Strong-UF-CMA

1. **Setup:** Challenger chooses a signing key k.
2. **Signature queries:** Adversary sends polynomially many signing queries (adaptively). The i^{th} query is a message m_i. The challenger sends $\sigma_i = \mathsf{Sign}(m_i, k)$ to the adversary.

   Note that the key k was chosen during setup, and the same key is used for all queries.
3. **Forgery:** The adversary sends a message m^* together with a signature σ^*, and wins if $(m^*, \sigma^*) \neq (m_i, \sigma_i)$ for all i, and $\mathsf{Verify}(m^*, \sigma^*, k) = 1$.

Figure 5: Security Game for MACs: Strong Unforgeability under Chosen Message Attack