# COMP6453: Week 4 Answers

## 1 MAC

Consider the following MAC for messages of length $l(n) = 2n - 2$ using a pseudorandom function $F(k, m)$. On an input message $m_0||m_1$ (with $|m_0| = |m_1| = n - 1$) and key $k \in \{0, 1\}^n$, algorithm Mac outputs $t = F(k, (0||m_0))||F(k, (1||m_1))$. Algorithm $Ver$ is defined in the natural way. Is $(KeyGen, TG, Ver)$ secure? Prove your answer.

**Answer:**

Take 2 messages $m = m_0||m_1$, and $m' = m'_0||m'_1$. The oracle outputs tags $t = t_0||t_1$ and $t' = t'_0||t'_1$. Now the adversary can output a message tag pair $m'' = m_0||m'_1$ and tag $t'' = t_0||t'_1$. The adversary wins the MAC security game because $t''$ passes the verification for $m''$ and $m''$ is not the same as $m$ or $m'$.

## 2 Hybrid Lemma and an Application

**(i).** Let $X^{(1)}, X^{(2)}, ..., X^{(m)}$ be a sequence of probability distributions. Assume that there exists an adversary $\mathcal{A}$ that distinguishes $X^{(1)}$ and $X^{(m)}$ with probability at least $\epsilon$. Show that there exists $i \in 1, ..., m$ such that $\mathcal{A}$ distinguishes distributions $X^{(i)}$ and $X^{(i+1)}$ with probability at least $\frac{\epsilon}{m}$.

**Answer:**

We have

$$\left|Pr[x_1 \leftarrow X^{(1)}; \mathcal{A}(x_1) = 1] - Pr[x_m \leftarrow X^{(m)} \mathcal{A}(x_m) = 1]\right| \geq \epsilon.$$

Let $g_i = Pr[x_i \leftarrow X^{(i)}; \mathcal{A}(x_i) = 1]$. Then we see that $|g_1 - g_m| \geq \epsilon$. We have that

$$\begin{aligned} |g_1 - g_m| &= |g_1 - g_2 + g_2 - g_3 + ... + g_{m-1} - g_m| \\ &\leq |g_1 - g_2| + |g_2 - g_3| + ... + |g_{m-1} - g_m|. \end{aligned}$$

So we must have that one of $|g_i - g_{i+1}| > \epsilon/m$. This completes the proof.

**(ii).** (Transitivity property of Computational Indistinguishability) Use $(i)$ to conclude that if $A$, $B$, and $C$ are distributions with $A \approx_c B$ and $B \approx_c C$, then $A \approx_c C$.

**Answer:**

We prove the contrapositive. Assume that distributions $A$ and $C$ are not computationally indistinguishable. Then there exists a distinguisher $D$ such that

$$\left|Pr[a \leftarrow A; D(a) = 1] - Pr[c \leftarrow C; D(c) = 1]\right| > p,$$

where $p$ is nonnegligible. Let

$$p_1 = \left|Pr[a \leftarrow A; D(a) = 1] - Pr[b \leftarrow B; D(b) = 1]\right|$$

and

$$p_2 = \left|Pr[b \leftarrow B; D(b) = 1] - Pr[c \leftarrow C; D(c) = 1]\right|.$$

By part (i), we must have either $p_1 > p/2$ or $p_2 > p/2$. In either case, this would imply that $D$ distinguishes $A$ and $B$ with nonneglibible probability, or $D$ distinguishes $B$ and $C$ with nonnegligible probability.

**(iii).** Lets say we have a semantically secure public key encryption scheme $Pub = (Setup, Enc, Dec)$. Using only this scheme, construct a symmetric key encryption scheme $(Setup', Enc', Dec')$ satisfying multi message security.

(Hint: Multi message security (aka CPA security) means that for all pairs $(x_1, ..., x_n)$ and $(y_1, ..., y_n)$ where $x_i, y_i$ are messages and $n$ is polynomially long, we have that the two distributions

$$(Enc'(sk', x_1), ..., Enc'(sk', x_n)) \approx_c (Enc'(sk', y_1), ..., Enc'(sk', y_n))$$

where $sk'$ is randomly sampled from the secret key space. You may use the fact that any semantically secure public key encryption scheme is also multi-message secure).

**Answer:**

Let $x$ be the message we want to encrypt. We start by defining $Setup'(\lambda)$. We simply define $Setup'(\lambda) = Setup(\lambda)$. This generates the pair $sk' = (Pk, Sk)$, which will be our secret key.

$Enc'(sk', x)$ is defined as $CT = Enc(Pk, x)$. $Dec'(sk', CT) = Dec(sk, CT)$. Correction is satisfied by hypothesis, as we assume that $Dec'(sk', CT) = Dec(sk, CT) = x$. We now give the security proof.

Consider messages $x_1, ..., x_n$ and $y_1, ..., y_n$. We show that

$$X^{(1)} = \{Enc'(sk', x_1), ..., Enc'(sk', x_n)\} \approx_c \{Enc'(sk', y_1), ..., Enc'(sk', y_n)\} = X^{(4)}$$

.

Note that $X^{(1)}$ is identically distributed to $X^{(2)} = \{Enc(Pk, x_1), ..., Enc(Pk, x_n)\}$ by our definition of $Enc(sk', x)$.

Recall our assumption of $Pub$ being semantically secure. Since we proved that any semantically secure public scheme is multi message secure, we see that $X^{(2)}$ is computationally indistinguishable to

$$X^{(3)} = \{Enc(Pk, y_1), ..., Enc(Pk, y_n)\}$$

Finally, note that $X^{(3)} \approx_c X^{(4)} = \{Enc'(sk', y_1), ..., Enc'(sk', y_n)\}$ by the same reasoning for why $X^{(1)} \approx_c X^{(2)}$.

Finally by the hybrid lemma, it follows that $X^{(1)} \approx_c X^{(4)}$ as desired.

# 3 Basic Number Theory Calculations

(i). Use the Euclidean Algorithm to find $gcd(342, 194)$.

**Answer:**

$342 = 1 \times 194 + 148$

$194 = 1 \times 148 + 46$

$148 = 3 \times 46 + 10$

$46 = 4 \times 10 + 6$

$10 = 1 \times 6 + 4$

$6 = 1 \times 4 + 2$

$4 = 2 \times 2 + 0 \implies gcd = 2.$

(ii). Calculate $7^{120} \pmod{143}$

**Answer:**

We use the properties of Euler phi function that if $gcd(m, n) = 1)$, then $\phi(ab) = \phi(a) \cdot \phi(b)$ for $a, b$ pairwise coprime. We have that $\phi(143) = \phi(11) \cdot \phi(13) = 10 \cdot 12 = 120$. Since 7 is coprime to 120, we can use Euler's theorem to conclude that $7^{120} \equiv 1 \pmod{143}$.