# COMP6453 Tutorial Week 4

## 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.

## 2 Indistinguishability: 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 $\frac{\epsilon}{m}$.

(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 $A \approx_c C$.

**Remark for Math Nerds**: The probability a distinguisher outputs 1 when fed a sample from a distribution induces a metric space on the space of probability distributions over strings. The hybrid lemma is a restatement of the triangle inequality on this metric space.

(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).

## 3 Basic Number Theory Calculations

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

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