COL759 Quiz 3

Anish

TOTAL POINTS

6.5 / 10

QUESTION 1

1 T/F **5 / 5**

✓ **+ 2 pts** *Question 1 Correct*

+ 1 pts Question 1 Correct but explanation incorrect or not given

✓ **+ 2 pts** *Question 2 Correct*

+ 1 pts Question 2 Correct but explanation incorrect or not given

✓ **+ 1 pts** *Question 3 correct*

+ 0 pts not attempted

QUESTION 2

2 CCA attack **1.5 / 5**

+ 5 pts Correct

✓ **+ 1.5 pts** *Attempt*

+ 0 pts Not attempted

Name: Anish Banerjee

2301-COL759 Quiz 3
Total marks: 10

Entry No: 2021CS10134

True False (5 marks)

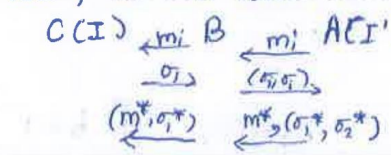
State whether the following are true or false. Prove a short (one/two line) explanation for your answer.

1. Let $\mathcal{I} = (\mathsf{Sign}, \mathsf{Verify})$ be a secure MAC with **deterministic signing**. Consider the following scheme $\mathcal{I}' = (\mathsf{Sign}', \mathsf{Verify}')$ which works as follows:

   - $\mathsf{Sign}'(k, m)$: $(\mathsf{Sign}(k, m), \mathsf{Sign}(k, m))$
   - $\mathsf{Verify}'(k, m, (\sigma_1, \sigma_2))$: Output 1 if $\sigma_1 = \sigma_2$ and $\mathsf{Verify}(k, m, \sigma_1) = 1$.

   Then $\mathcal{I}'$ is a secure MAC scheme.

   True, we can have this reduction:

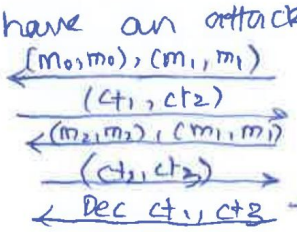
   If A wins I' game with non-negl prob. then B wins I game with non-negl prob.

2. Let $\mathcal{E}_{cca} = (\mathsf{Enc}, \mathsf{Dec})$ be an encryption scheme with message space $\{0,1\}^n$, key space $\{0,1\}^n$, that is secure against chosen ciphertext attacks. Consider the following encryption scheme with message space $\{0,1\}^{2n}$ and key space $\{0,1\}^n$:

   - $\mathsf{Enc}'(k, (m_1, m_2))$: Output $(\mathsf{Enc}(k, m_1), \mathsf{Enc}(k, m_2))$.
   - $\mathsf{Dec}'(k, \mathsf{ct} = (\mathsf{ct}_1, \mathsf{ct}_2))$: Compute $y_1 = \mathsf{Dec}(k, \mathsf{ct}_1)$ and $y_2 = \mathsf{Dec}(k, \mathsf{ct}_2)$. Output $\perp$ if either $y_1 = \perp$ or $y_2 = \perp$. Else output (y_1, y_2).

   The new encryption scheme $(\mathsf{Enc}', \mathsf{Dec}')$ is CCA secure.

   False, we can have an attack

   If Dec outputs m, m, then send 1 else send 0

3. Hash functions can be used for encrypting long messages by first hashing the long message to a short digest, then encrypting the short digest.

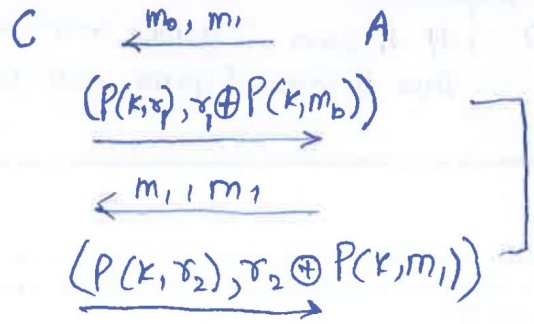
   False. We won't be able to decrypt it since a Hash function is many-one (Non-invertible)

CCA Attack (5 marks)

Let $P : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a secure PRP. Consider the following encryption algorithm:

- $\mathsf{Enc}(k, m)$: Pick a random string $r \leftarrow \{0,1\}^n$, output $(P(k,r), r \oplus P(k,m))$.
- $\mathsf{Dec}(k, \mathrm{ct} = (\mathrm{ct}_1, \mathrm{ct}_2))$: Output $P^{-1}\left(k, P^{-1}(k, \mathrm{ct}_1) \oplus \mathrm{ct}_2\right)$.

Show that (Enc, Dec) is not CCA secure by presenting a chosen ciphertext attack. For partial marks, in case you are unable to find an attack, submit the attempts you tried, and discuss why they don't work.



$r_1 \oplus r_2$ if $b = 1$

~~Can't decline~~

Won't work as can't use decryption on it

Idea: Symmetry of the encryption can give out k or r