COL759 Quiz 1

Anish

TOTAL POINTS

5 / 10

QUESTION 1

1 Q1 **1 / 1**

✓ **+ 1 pts** *Correct*

QUESTION 2

2 Q2 **0 / 2**

✓ **+ 0 pts** *incorrect/insufficient explanation.*

QUESTION 3

3 Q3 **4 / 7**

✓ **+ 2 pts** *Correct reduction*

✓ **+ 2 pts** *Correct analysis for b=0*

1 Adv. A expects a message and ciphertext

2 why? insufficient explanation.

2301-COL759

Quiz 1
Total marks: 10

Name: Anish Banerjee
Entry no: 2021CS10134

Security against Key Recovery Attacks

Given a random message m and its encryption ct using a random key k, can an efficient adversary recover a secret key k' such that $\mathsf{Dec}(k', \mathsf{ct}) = m$? Note that k' may or may not be the same as the key used for encrypting; the goal of the adversary is to find some key that produces correct decryption. Such attacks are called **key recovery attacks**. We capture these attacks via the following security game:

Security against Key Recovery Attacks

1. Challenger picks a uniformly random key $k \leftarrow \mathcal{K}$, message $m \leftarrow \mathcal{M}$, computes $\mathsf{ct} \leftarrow \mathsf{Enc}(k, m)$ and sends (m, ct) to the adversary.
2. The adversary sends key k' and wins if $\mathsf{Dec}(k', \mathsf{ct}) = m$.

Figure 1: Security game for capturing key recovery attacks

Definition 1. An encryption scheme $\mathcal{E}$ is secure against key recovery attacks if, for any p.p.t. adversary $\mathcal{A}$, $p_{\mathcal{A},\mathcal{E}} = \Pr[\mathcal{A}$ wins the key recovery game w.r.t. $\mathcal{E}]$ is a negligible function (in the security parameter).

1. (1 mark) Consider the function $\mu : \mathbb{N} \to [0, 1]$ defined as follows:

$$\mu(n) = 1/n^i \text{ for all } n \in [2^i, 2^{i+1} - 1]$$

Is this function negligible? Provide a brief explanation for your answer.

Since the function,

$$\mu(n) = \begin{cases} 1 & n = 1 \\ 1/n & n = 2, 3 \\ 1/n^2 & n = 4, 5, 6, 7 \\ 1/n^3 \end{cases}$$

→ powers increase of the inverse polynomial

So for every c, we can find a suitable n_0 such that $\mu(n) \le \frac{1}{n^c}$ $\forall n \ge n_0$

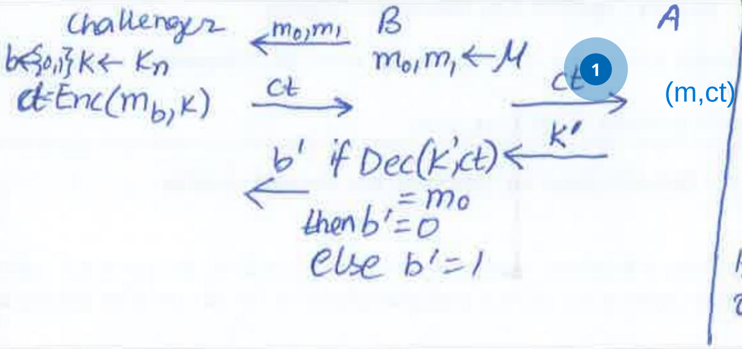
So it is negligible

2. (2 marks) Consider an encryption scheme $\mathcal{E}$ where the key space is fixed to be $\{0, 1\}^{100}$ for all security parameters. Show that this scheme does not satisfy security against key recovery attacks. Present an efficient probabilistic polynomial time adversary that wins the security game described in Figure 1, and compute the winning probability of your adversary.

The attacker can brute force all 2^100 keys to find k'.
The adversary is as follows:
On obtaining (m,ct), brute force through all the 2^100 keys to find a k' such that Enc(k',m)=ct and return k'
Running time is O(1), so, it is efficient.
Winning probability is 1

3. (7 marks) Consider an encryption scheme $\mathcal{E}$ where $\mathcal{K}_n = \{0,1\}^n$, $\mathcal{M}_n = \{0,1\}^{2n}$ (here n is the security parameter). Show that if $\mathcal{E}$ satisfies semantic security, then it also satisfies security against key recovery attacks. In particular, show that if there exists a p.p.t. adversary $\mathcal{A}$ that wins the key recovery game with probability ϵ, then there exists a p.p.t. algorithm $\mathcal{B}$ that wins the semantic security game with advantage close to ϵ.

a. Describe the reduction algorithm $\mathcal{B}$ (it uses $\mathcal{A}$ to win the semantic security game).



B wins if $b' = b$

On receiving k' from A, it checks if Dec(k',ct) = m0 If yes it returns 0, otherwise 1

b. Compute the probability of $\mathcal{B}$ outputting '0', conditioned on the challenger choosing $b = 0$.

$Pr[b' = 0 \mid b = 0] = \epsilon$

The winning probability of the key recovery game

c. Compute the probability of $\mathcal{B}$ outputting '0', conditioned on the challenger choosing $b = 1$.

$Pr[b' = 0 \mid b = 1] = 1/2^n$ 2

|K|/|M|