COL759 Quiz 5

Anish

TOTAL POINTS

9 / 10

QUESTION 1

1 Quiz5 9 / 10

✓ **+ 2 pts** *T/F 1 : Correct answer and reasoning*

+ 1 pts T/F 1 : Correct answer, incorrect reasoning

✓ **+ 2 pts** *T/F 2 : Correct answer and reasoning*

+ 1 pts T/F 2 : Correct answer, incorrect reasoning

✓ **+ 2 pts** *T/F 3 : Correct answer and reasoning*

+ 1 pts T/F 1 : Correct answer, incorrect reasoning

✓ **+ 4 pts** *Offline/online : correct*

+ 2 pts Offline/online: partial

+ 0 pts all questions incorrect

- 1 *Point adjustment*

1 ?

Name: ANISH BANERJEE

2301-COL759 Quiz 5
Total marks: 10

Entry No: 2021CS10134

True False (6 marks)

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

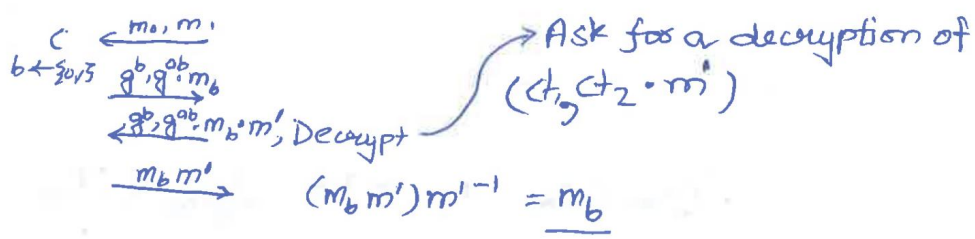
1. If a public key encryption scheme is secure against chosen ciphertext attacks, then it satisfies plaintext integrity (that is, no efficient algorithm can produce an encryption of a new message, even after seeing the public key and many encryptions on messages of its choice).

False

We can't satisfy plaintext integrity in the public key setting as adversary can always encrypt a new message and send to the challenger

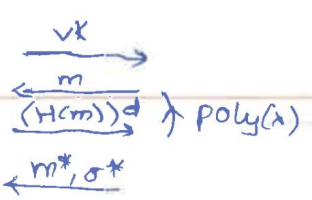
2. The Elgamal encryption scheme is **not** CCA secure (in the standard model).

True



3. Suppose there exists a signature scheme that is proven secure in the random oracle model. Then, we can use a collision-resistant hash function in the scheme to achieve security in the standard model.

False



~~It can't be~~

We can't prove it in the similar way since ~~we~~ he can't control the CRHF queries as ~~we~~ he controlled in the RO model

the challeng

Online/Offline Signatures (4 marks)

One-time signatures (such as the ones we saw in last class) are much faster as compared to signature schemes that allow unbounded queries. Let $\mathcal{S}_{\text{ot}} = (\mathsf{Setup}_{\text{ot}}, \mathsf{Sign}_{\text{ot}}, \mathsf{Verify}_{\text{ot}})$ be a one-time secure signature scheme, and $\mathcal{S}_{\text{unb}} = (\mathsf{Setup}_{\text{unb}}, \mathsf{Sign}_{\text{unb}}, \mathsf{Verify}_{\text{unb}})$ a regular signature scheme. The running time of $\mathsf{Sign}_{\text{ot}}(\mathsf{sk}_{\text{ot}}, m)$ (resp. $\mathsf{Sign}_{\text{unb}}(\mathsf{sk}_{\text{unb}}, m)$) is T_{ot} (resp. T_{unb}), and $T_{\text{ot}} \ll T_{\text{unb}}$. Assume the setup times of both schemes is very small.

We will combine $\mathcal{S}_{ot}$ with $\mathcal{S}_{unb}$ to build an online/offline signature scheme $\mathcal{S} = (\mathsf{Setup}, \mathsf{Sign}_{on}, \mathsf{Sign}_{off}, \mathsf{Verify})$ where the running time of online signing Sign_{on} is close to T_{ot}, while Sign_{off} is allowed to be close to T_{unb}. You must define Sign_{off}, Sign_{on} and Verify appropriately.

- $\mathsf{Setup}(1^\lambda)$: Choose $(\mathsf{sk}_{unb}, \mathsf{vk}_{unb}) \leftarrow \mathsf{Setup}_{unb}(1^\lambda)$. The secret key is sk_{unb}, the verification key is vk_{unb}.
- $\mathsf{Sign}_{off}(\mathsf{sk}_{unb})$: The offline signing part is done without seeing the message to be signed. It generates a partial signature σ_{off} and some secret state st_{off}.

$(sk_{ot}, vk_{ot}) \leftarrow Setup_{ot}(1^d)$

$Sign_{off}(sk_{unb}) = \underbrace{Sign_{Ubb}(sk_{Ubb}, vk_{ot})}_{\sigma_{off}}, \underbrace{sk_{ot}, vk_{ot}}_{st_{off}}$

- $\mathsf{Sign}_{on}(\mathsf{st}_{off}, \sigma_{off}, m)$: The online signing part receives the message, together with the partial signature σ_{off} and the secret state st_{off}. It generates the final signature σ.

$Sign_{on}(st_{off}, \sigma_{off}, m) = Sign_{ot}(sk_{ot}, m)$

- $\mathsf{Verify}(\mathsf{vk}_{unb}, m, \sigma)$: The verification algorithm takes the verification key, the message, the signature generated by Sign_{on}. It outputs 0/1.