COL759 Quiz 4

Anish

TOTAL POINTS

6 / 10

QUESTION 1

1 True False **6 / 6**

✓ **+ 2 pts** *(a) Correct answer and explanation*

+ 1 pts (a) correct, no/incorrect explanation

✓ **+ 2 pts** *(b) correct answer and explanation*

+ 1 pts (b) correct, no/incorrect explanation

✓ **+ 2 pts** *(c) correct answer and explanation*

+ 1 pts (c) correct, no/incorrect explanation

+ 0 pts all incorrect

QUESTION 2

2 **0 / 4**

+ 3 pts Correct scheme

+ 1 pts correctnes

✓ **+ 0 pts** *incorrect / vague*

Name: ANISH BANERJEE

2301-COL759 Quiz 4
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. A public key encryption scheme is said to have 'learnable randomness' if there exists an efficient algorithm such that, given the public key and a ciphertext, it can learn the randomness used to encrypt. It is possible to have CPA secure public key encryption with learnable randomness.

False

Suppose A learns the randomness of the encryption

$$\begin{array}{ccccc} C & \xrightarrow{pk} & B & & A \\ & \xleftarrow{m_0\ m_1} & & & \\ & \xrightarrow{Enc(pk, m_b; r)} & & \xrightarrow{Enc(pk, m_b; r)} & \\ & \xleftarrow{b} & & \xleftarrow{r} & \end{array}$$

Upon receiving $ct = Enc(pk, m_b; r)$ B forwards it to A to obtain r. Then it computes $Enc(pk, m_0; r)$ and $Enc(pk, m_1; r)$ and checks which one matches with ct

2. Let $N = p \cdot q$ where p and q are distinct primes. For any integer $y \in \mathbb{Z}_N^*$, there exists a unique integer x such that $x^2 \bmod N = y$.

False

Note: It is assumed that $x \in \mathbb{Z}_N^*$ [Not needed]

Take $N = 6$ $\mathbb{Z}_N^* = \{1, 5\}$ for $y = 5$, we have no $x \in \mathbb{Z}_N^*$ such that $x^2 \bmod 6 = 5$

Infact the assumption is not needed. Take $x \in \mathbb{Z}$

$x = 6k + r$ $0 \le r < 1$ $x^2 \bmod 6 = r^2 \bmod 6$ which can be in $\{1^2 \bmod 6, 2^2 \bmod 6 \cdots 5^2 \bmod 6\} = \{1, 4, 3, \cancel{5}\}$

3. Suppose there exists an efficient algorithm that, given any N which is a product of two distinct primes, can find a non-zero element $x \in \mathbb{Z}_N \setminus \mathbb{Z}_N^*$. Then this algorithm can be used to break the RSA assumption.

True

Let $N = pq$. If A finds $x \in \mathbb{Z}_N \setminus \mathbb{Z}_N^*$ then $\gcd(x, N) \neq 1$

Thus $\gcd(x, N) = p$ or q since p and q are the only prime factors of N. So, using A we can factor N and break the RSA assumption: Compute $\gcd(x, N)$

Output $\left(\gcd(x, N), \frac{N}{\gcd(x, N)}\right)$

From Key Exchange to Public Key Encryption (4 marks)

In this exercise, we will study Diffie-Hellman's two-message key-exchange protocol abstractly. A two-message key-exchange protocol with key space $\{0,1\}^\lambda$ consists of four algorithms AliceMsg, BobMsg, AliceKey, BobKey with the following properties:

- $(\mathsf{msg}_A, \mathsf{st}_A) \leftarrow \mathsf{AliceMsg}(1^\lambda)$: Alice uses the security parameter λ to generate her message msg_A, and keeps the state st_A.
- $(\mathsf{msg}_B, \mathsf{st}_B) \leftarrow \mathsf{BobMsg}(\mathsf{msg}_A)$: Bob, on receiving msg_A, computes his response msg_B, and also his keeps the state st_B.
- $k \leftarrow \mathsf{AliceKey}(\mathsf{st}_A, \mathsf{msg}_B)$: Alice uses her state st_A and Bob's message msg_B to compute the key $k \in \{0,1\}^\lambda$.
- $k \leftarrow \mathsf{BobKey}(\mathsf{st}_B, \mathsf{msg}_A)$: Bob uses his state st_B and Alice's message msg_A to compute the key $k \in \{0,1\}^\lambda$.

For correctness, we require the following: if $(\mathsf{msg}_A, \mathsf{st}_A) \leftarrow \mathsf{AliceMsg}(1^\lambda)$, $(\mathsf{msg}_B, \mathsf{st}_B) \leftarrow \mathsf{BobMsg}(\mathsf{msg}_A)$, $k \leftarrow \mathsf{AliceKey}(\mathsf{st}_A, \mathsf{msg}_B)$ and $k' \leftarrow \mathsf{BobKey}(\mathsf{st}_B, \mathsf{msg}_A)$, then $k = k'$.

For security, we require that no p.p.t. adversary can distinguish between the following two distributions:

$$\mathcal{D}_0 = \left\{ (k, \mathsf{msg}_A, \mathsf{msg}_B) \; : \; \begin{array}{c} (\mathsf{msg}_A, \mathsf{st}_A) \leftarrow \mathsf{AliceMsg}(1^\lambda) \\ (\mathsf{msg}_B, \mathsf{st}_B) \leftarrow \mathsf{BobMsg}(\mathsf{msg}_A) \\ k \leftarrow \mathsf{AliceKey}(\mathsf{st}_A, \mathsf{msg}_B) \end{array} \right\}$$

$$\mathcal{D}_1 = \left\{ (r, \mathsf{msg}_A, \mathsf{msg}_B) \; : \; \begin{array}{c} (\mathsf{msg}_A, \mathsf{st}_A) \leftarrow \mathsf{AliceMsg}(1^\lambda) \\ (\mathsf{msg}_B, \mathsf{st}_B) \leftarrow \mathsf{BobMsg}(\mathsf{msg}_A) \\ r \leftarrow \{0,1\}^\lambda \end{array} \right\}$$

Use the two-round key exchange protocol to design a CPA secure public key encryption scheme with message space $\{0,1\}^\lambda$. You should not use any other cryptographic primitives. Define the three algorithms (Setup, Enc, Dec), and discuss why your scheme is correct. You do not need to prove CPA security.

Setup $\quad pk = (msg_A, msg_B) \quad sk = K$

(Rough work)

A | B

$(msg_A, st_A) \leftarrow AM$ | $(msg_B, st_B) \leftarrow BM$

$\xleftarrow{\quad msg\,B \quad}$

$\xrightarrow{\quad msg\,A \quad}$

$K \leftarrow AK(st_A, m_B)$ | $K \leftarrow BK(st_B, m_A)$

$pk = (g \;\; g^a)\ \cancel{g^b}$ $\qquad a = sk$

$g^r,\ g^{ra} \cdot m$