Q1 *Dual Asymmetry* **(0 points)**

Alice wants to send two messages M_1 and M_2 to Bob, but they do not share a symmetric key.

Clarification during exam: Assume that p is a large prime and that g is a generator $\mod p$, like in ElGamal. Assume that all computations are done modulo p in Scheme A.

Q1.1 Scheme A: Bob publishes his public key $B = g^b$. Alice randomly selects r from 0 to p-2. Alice then sends the ciphertext $(R, S_1, S_2) = (g^r, M_1 \times B^r, M_2 \times B^{r+1})$.

Select the correct decryption scheme for M_1:

- ◯ (A) $R^{-b} \times S_1$
- ◯ (B) $R^b \times S_1$
- ◯ (C) $B^{-b} \times S_1$
- ◯ (D) $B^b \times S_1$
- ◯ (E) ——
- ◯ (F) ——

Q1.2 Select the correct decryption scheme for M_2:

- ◯ (G) $B^{-1} \times R^{-b} \times S_2$
- ◯ (H) $B \times R^{-b} \times S_2$
- ◯ (I) $B^{-1} \times R^b \times S_2$
- ◯ (J) $B^{-1} \times R \times S_2$
- ◯ (K) ——
- ◯ (L) ——

Q1.3 Is Scheme A IND-CPA secure? If it is secure, briefly explain why (1 sentence). If it is not secure, briefly describe how you can learn something about the messages.

Clarification during exam: For Scheme A, in the IND-CPA game, assume that a single plaintext is composed of two parts, M_1 and M_2.

- ◯ (A) Secure
- ◯ (B) Not secure
- ◯ (C) ——
- ◯ (D) ——
- ◯ (E) ——
- ◯ (F) ——

Q1.4 Scheme B: Alice randomly chooses two 128-bit keys K_1 and K_2. Alice encrypts K_1 and K_2 with Bob's public key using RSA (with OAEP padding) then encrypts both messages with AES-CTR using K_1 and K_2. The ciphertext is $\text{RSA}(\mathsf{PK}_{\text{Bob}}, K_1 \| K_2), \text{Enc}(K_1, M_1), \text{Enc}(K_2, M_2)$.

Which of the following is required for Scheme B to be IND-CPA secure? Select all that apply.

☐ (G) K_1 and K_2 must be different

☐ (H) A different IV is used each time in AES-CTR

☐ (I) M_1 and M_2 must be different messages

☐ (J) M_1 and M_2 must be a multiple of the AES block size

☐ (K) M_1 and M_2 must be less than 128 bits long

☐ (L) None of the above

Q2 *PRNGs and Diffie-Hellman Key Exchange* **(0 points)**

Eve is an eavesdropper listening to an insecure channel between Alice and Bob.

1. Alice and Bob each seed a PRNG with different random inputs.
2. Alice and Bob each use their PRNG to generate some pseudorandom output.
3. Eve learns both Alice's and Bob's pseudorandom outputs from step 2.
4. Alice, without reseeding, uses her PRNG from the previous steps to generate a, and Bob, without reseeding, uses his PRNG from the previous steps to generate b.
5. Alice and Bob perform a Diffie-Hellman key exchange using their generated secrets (a and b). Recall that, in Diffie-Hellman, neither a nor b are directly sent over the channel.

For each choice of PRNG constructions, select the minimum number of PRNGs Eve needs to compromise (learn the internal state of) in order to learn the Diffie-Hellman shared secret $g^{ab} \bmod p$. Assume that Eve always learns the internal state of a PRNG between steps 3 and 4.

Q2.1 Alice and Bob both use a PRNG that outputs the same number each time.

◯ (A) Neither PRNG ◯ (C) Both PRNGs ◯ (E) ——

◯ (B) One PRNG ◯ (D) Eve can't learn the secret ◯ (F) ——

Q2.2 Alice uses a secure, rollback-resistant PRNG. Bob uses a PRNG that outputs the same number each time.

◯ (G) Neither PRNG ◯ (I) Both PRNGs ◯ (K) ——

◯ (H) One PRNG ◯ (J) Eve can't learn the secret ◯ (L) ——

Q2.3 Alice and Bob both use a secure, rollback-resistant PRNG.

◯ (A) Neither PRNG ◯ (C) Both PRNGs ◯ (E) ——

◯ (B) One PRNG ◯ (D) Eve can't learn the secret ◯ (F) ——

For the rest of the question, consider a different sequence of steps:

1. Alice and Bob each seed a PRNG with different random inputs.
2. Alice uses her PRNG from the previous step to generate a, and Bob uses his PRNG from the previous step to generate b.
3. Alice and Bob perform a Diffie-Hellman key exchange using their generated secrets (a and b).
4. Alice and Bob, without reseeding, each use their PRNG to generate some pseudorandom output.
5. Eve learns both Alice's and Bob's pseudorandom outputs from step 2.

As before, assume that Eve always learns the internal state of a PRNG between steps 3 and 4.

Q2.4 Alice and Bob both use a secure, but not rollback-resistant PRNG.

- ◯ (G) Neither PRNG
- ◯ (H) One PRNG
- ◯ (I) Both PRNGs
- ◯ (J) Eve can't learn the secret
- ◯ (K) ——
- ◯ (L) ——

Q2.5 Alice and Bob both use a secure, rollback-resistant PRNG.

- ◯ (A) Neither PRNG
- ◯ (B) One PRNG
- ◯ (C) Both PRNGs
- ◯ (D) Eve can't learn the secret
- ◯ (E) ——
- ◯ (F) ——

Q3 *To Believe or Not To Believe* **(0 points)**

You are a detective at the Universal Conflict-resolution Bureau (UCB). You have been presented with a new case: Alice claims that Bob agreed to pay her \$100. As evidence, she has a message from Bob, "I, Bob, owe Alice \$100," along with some cryptography applied to the message.

Decide whether each piece of cryptographic evidence below is sufficient to believe her claim that this message is from Bob.

- m is the message from Bob.
- PK, SK is a public-private key pair.
- MAC is a cryptographically secure message authentication code function.
- k_1 and k_2 is a secret key shared between Alice and Bob.
- H is a cryptographically secure hash function.
- $\mathsf{Sign}(\mathsf{SK}, m)$ is a digital signature algorithm signing a message m with secret key SK.
- $\mathsf{Enc}, \mathsf{Dec}$ is an IND-CPA secure symmetric encryption scheme.

Q3.1 Alice presents you with $\mathsf{Sign}(\mathsf{SK}, m)$ and PK.

You obtain $\mathsf{Sign}(\mathsf{SK}_{CA}, \text{"Bob's public key is } \mathsf{PK}\text{"})$ from a certificate authority you trust. SK_{CA} is the secret key of the CA, and you know the corresponding public key.

◯ (A) m must be from Bob.

◯ (B) m is not necessarily from Bob.

◯ (C) ——

◯ (D) ——

◯ (E) ——

◯ (F) ——

Q3.2 Alice presents you with $\mathsf{H}(m)$.

◯ (G) m must be from Bob.

◯ (H) m is not necessarily from Bob.

◯ (I) ——

◯ (J) ——

◯ (K) ——

◯ (L) ——

Q3.3 Alice presents you with $\mathsf{MAC}(k_1, m)$ and the secret key k_1.

◯ (A) m must be from Bob.

◯ (B) m is not necessarily from Bob.

◯ (C) ——

◯ (D) ——

◯ (E) ——

◯ (F) ——

Q3.4 Alice presents you with $\mathsf{MAC}(k_1, \mathsf{Enc}(k_2, m))$ and the secret keys k_1 and k_2.

◯ (G) m must be from Bob.

◯ (H) m is not necessarily from Bob.

◯ (I) —

◯ (J) —

◯ (K) —

◯ (L) —

Q3.5 Alice presents you with $\mathsf{Sign}(\mathsf{SK}, m)$, PK.

Additionally, Alice generates a certificate with her public key, $\mathsf{Sign}(\mathsf{SK}_{\text{Alice}}, \text{“Bob's public key is PK”})$ and presents you with the certificate and her public key $\mathsf{PK}_{\text{Alice}}$.

◯ (A) m must be from Bob.

◯ (B) m is not necessarily from Bob.

◯ (C) —

◯ (D) —

◯ (E) —

◯ (F) —