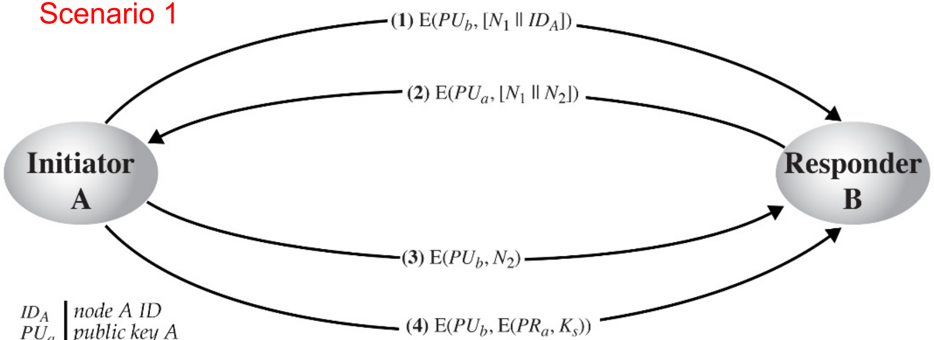
Question 3:

We have the following two Public-Key Encryption scenarios for establishing a Session Key:

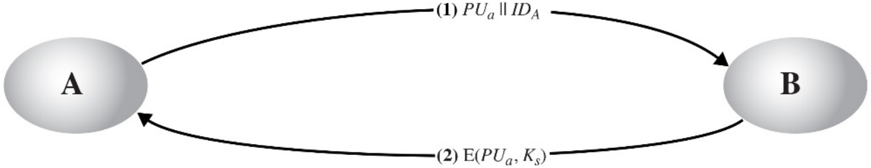
Scenario 1



(1) $E(PU_b, [N_1 \| ID_A])$
(2) $E(PU_a, [N_1 \| N_2])$
Initiator A
Responder B
(3) $E(PU_b, N_2)$
(4) $E(PU_b, E(PR_a, K_s))$

ID_A	node A ID
PU_a	public key A
PR_a	private key A
PU_b	public key B
N_1	nonce 1
N_2	nonce 2
K_s	session key

Scenario 2



Question 3:

- **A)** Is scenario 2, safe against **man-in-the-middle** attacks? Why?
- **B)** In scenario 1, is each side confident about the authenticity of the other side? Why?
- **C)** In scenario 1, assume that in step 2 only **nonce 2** is being transmitted (and not **nonce 1**). In the end of step 4, which side is ensured about the identity of the other side? Why?