Exercise 8

Question 1

$Y_A = x_A G$

- Bob picks k
- Bob sends Alice $C_1 = k \cdot G$
- Alice sends Bob M and $S = M - x_A C_1$
- Bob verifies $M = S + k Y_A$

a) Alice sends: $S = M - x_A C_1 \iff M = S + x_A C_1$

Bob knows $C_1 = kG$, $Y_A = x_A G$ $\Rightarrow k Y_A = k(x_A G) = x_A \cdot C_1$ $\Rightarrow$

$\Rightarrow M = S + x_A C_1 = S + k Y_A$

In conclusion, the verification equation is correct when the signature is valid.

b) The attacker must produce a S where:

$M = S + k Y_A \Rightarrow S = M - k Y_A$

We think that the attacker does not know k. So to forge "S" the attacker needs to know $k Y_A$. But the attacker might know that $C_1 = kG$ which is sent by Alice.

To compute $k Y_A$ we would need to know k or $S = M - k Y_A$

In conclusion, forging a valid signature would require solving the elliptic curve discret logarithm problem, which is believed to be very hard.

Question 2

1. $A \rightarrow B : A, N_A$
2. $B \rightarrow A : E(K_{AB}, [N_A, K'_{AB}])$
3. $A \rightarrow B : E(K'_{AB}, N_A)$

a)

- Why A believes they share K'_{AB}:

A receives $E_{K_{AB}}$ which only B could have encrypted. The message contains her own nonce N_A so A knows it's not a replay. So it concludes that the message is fresh and from B → K'_{AB} must be the new session key from B.

- Why B believes they share K'_{AB}:

B generated K'_{AB} and sent it to A securely. B receives $E_{K_{AB}}$ which shows that A received the new key and could decrypt and re-encrypt the nonce. Since only someone with K_{AB} could and that, B believes A has the same key.

- Why they both believe it's fresh:

The nonce N_A ensure freshness: It was generated by A and sent in step 1. A sees it returned in step 2 → confirms B saw it. B sees it and returned in step 3 → confirms A used it to finally agreed key.

In conclusion: Both A and B believe they are communicating directly with each other and that the session key is fresh and secret.

Question 3

a) Description:

1. A and B want to establish a shared key K_{AB}
2. T is a trusted server that helps sharing the key.
3. A and B share a long-term symmetric key with T: K_{AT} and K_{BT}

Step 1: A -> B
Step 2: B -> T
Step 3: T -> B
Step 4: B -> A

b) We will check for ~~audi~~ confidentiality first:

- Only A and T know K_{AT}
- Only B ant T know K_{BT}
- key K_{AB} is encrypted
- Only A and B can obtain K_{AB} by decrypting the messages.
- An attacker can not decrypt K_{AB}

=> Confidentiality is provided.

We will now check for freshness:

- A includes a fresh nonce N_A
- B includes a a fresh nonce N_B
- T does not return both N_A and N_B to both parts
  <=> A receives N_A but doesn't see N_B
  <=> B recieves N_B but doesn't see N_A after step 1
- A can only verify possession if it remembers all previous steps

=> A has no proof that K_{AB} wasn't generated early

=> In conclusion freshness is not provided.