Key Distribution and Management

Marcio Woitek

Problem 1

▷ Alice's private key
▷ Bob's private key

Problem 2

Answer: Nonce

Problem 3

▷ To connect the response to the corresponding communication

Problem 4

Answer: 190

The total number of virtual machines is $n = 5 \cdot 4 = 20$. In this case, there will be one key exchange session for each pair of VMs. Therefore, the number of sessions is given by

$$\binom{n}{2} = \frac{n(n-1)}{2} = \frac{20(20-1)}{2} = 190. \tag{1}$$

Problem 5

Answer: 19900

The total number of applications is $n = 5 \cdot 4 \cdot 10 = 200$. In this case, there will be one key exchange session for each pair of applications. Therefore, the number of sessions is given by

$$\binom{n}{2} = \frac{n(n-1)}{2} = \frac{200(200-1)}{2} = 19900. \tag{2}$$

Problem 6

▷ The public key of the user (the certificate subject)
▷ The private key of CA
▷ The request for the user's certificate

Problem 7

▷ The certificate itself
▷ The public key of CA

Problem 8

- ▷ Digital certificates can be requested before using it to share the public key.
- ▷ Once receiving the digital certificates signed by a Certificate Authority (CA), a user can share it with anybody whom it wants to communicate.

Problem 9

- ▷ Manage certificates
- ▷ Distribute certificates
- ▷ Create certificates
- ▷ Store certificates
- ▷ Revoke certificates