Congratulations! You passed!

TO PASS 80% or higher

Keep Learning

GRADE
100%

Cryptography Applications

TOTAL POINTS 3

1. What information does a digital certificate contain? Check all that apply. **1 / 1 point**

- [x] Identifying information of the certificate owner

Correct
Great job! A digital certificate contains the public key information, along with a digital signature from a CA. It also includes information about the certificate, like the entity that the certificate was issued to.

- [x] Digital signature

Correct
Great job! A digital certificate contains the public key information, along with a digital signature from a CA. It also includes information about the certificate, like the entity that the certificate was issued to.

- [ ] Private key data
- [x] Public key data

Correct
Great job! A digital certificate contains the public key information, along with a digital signature from a CA. It also includes information about the certificate, like the entity that the certificate was issued to.

2. Which type of encryption does SSL/TLS use? **1 / 1 point**

- ( ) Asymmetric encryption
- ( ) Symmetric encryption
- ( ) Neither
- (•) Both

Correct
Wohoo! SSL/TLS use asymmetric algorithms to securely exchange information used to derive a symmetric encryption key.

3. What are some of the functions that a Trusted Platform Module can perform? Check all that apply. **1 / 1 point**

- [ ] Malware detection
- [ ] Secure user authentication
- [x] Data binding and sealing

Correct
You nailed it! A TPM can be used for remote attestation, ensuring that a host is a known good state and hasn't been modified or tampered (from a hardware and a software perspective). TPMs can also seal and bind data to them, encrypting data against the TPM. This also allows it to be decrypted by the TPM, only if the machine is in a good and trusted state.

- [x] Remote attestation

Correct
You nailed it! A TPM can be used for remote attestation, ensuring that a host is a known good state and hasn't been modified or tampered (from a hardware and a software perspective). TPMs can also seal and bind data to them, encrypting data against the TPM. This also allows it to be decrypted by the TPM, only if the machine is in a good and trusted state.