MBA Post-Graduate Studies on Cybersecurity Management

Cyber Security Systems

Prof. Alessandro Armando

December 7, 2019

Attenzione: Si risponda alle domande utilizzando lo spazio apposito.

Name, Surname: _____

---

1. ***Digital Signatures***

   Which of the following sentences are true?

   A. *A public key certificate is states the correspondence between a public key and an entity (person, legal entity, device) and a*

   B. *A smartcard used for digital signatures stores the private key of the owner.*

   C. *Smartcards play a crucial role in the validation of digital signatures*

   D. *Smartcards play a crucial role in the generation of digital signatures*

   E. *Smartcards play a crucial role in the storage of digital signatures*

2. ***Cryptography***

Alice must send a large file M to Bob (for example, a video) in such a way that Bob can check both the integrity and the confidentiality of the confidentiality of M.

Which of the following procedure are adequate to the task?

Justify your answers.

1. *Alice encodes M with her own private key and sends the resulting ciphertext to Bob.*

2. *Alice guesses a secret key K and sends to Bob:*
   - *the ciphertext obtained by encrypting the hashcode of M with her own private key,*
   - *the ciphertext obtained by encrypting M with K,*
   - *the ciphertext obtained by encrypting K with Bob's public key.*

3. *Alice sends Bob:*
   - *the ciphertext obtained by encrypting the hashcode of M with her own private key,*
   - *the ciphertext obtained by encrypting M with Bob's public key,*

4. *Alice sends Bob*
   - *the ciphertext obtained by encrypting the hashcode of M with her own public key,*
   - *the ciphertext obtained by encrypting M with Bob's private key*