Cryptography and Compliance Pitfalls

TOTAL POINTS 5

1. True or False: A whole branch of hacking - Reverse Engineering - is devoted to discovering hidden algorithms and data. `1 point`

    ⦿ True

    ◯ False

2. Which is not a key takeaway of best practices of cryptography? `1 point`

    ◯ Do encrypt all sensitive data, at rest, in use, and in transit.

    ◯ Do rely on proven algorithms.

    ◯ Do use hard to guess keys and store them correctly.

    ⦿ Do rely on your own encryption algorithms.

3. Which three (3) are true of digital signatures? `1 point`

    ☑ Uses hashing

    ☑ Uses public key encryption

    ☐ uses symmetric key encryption

    ☑ ensures authentication, non-reputation, and integrity

4. What is the recommendation to avoid the encrypting data at rest pitfall "Using hardcoded/easily guessed keys"? `1 point`

    ◯ Phase them out

    ◯ Store keys in secure keystores.

    ◯ Use a new random initialization vectors every time.

    ⦿ Select cryptographically-random keys, do not reuse keys for different installs.

5. Which two (2) statements are true of the Hash function? `1 point`

    ☑ Maps data of arbitrary size to data of a fixed size.

    ☐ Hashing makes data easy to reconstruct.

    ☑ Hashing provides integrity.

☑ I, **Adarsh Kumar**, understand that submitting work that isn't my own may result in permanent failure of this course or deactivation of my Coursera account.
Learn more about Coursera's Honor Code

👍 💬 🏳

Save   Submit