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 use hard to guess keys and store them correctly.
- (•) Do rely on your own encryption algorithms.
- ( ) Do rely on proven algorithms.

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

- [x] Ensures authentication, non-repudiation, and integrity
- [x] Uses public key encryption
- [ ] Uses symmetric key encryption
- [x] Uses hashing

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

- (•) Select cryptographically-random keys, do not reuse keys for different installs.
- ( ) Store keys in secure keystores.
- ( ) Phase them out
- ( ) Use a new random initialization vectors every time.

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

- [x] Hashing provides integrity.
- [x] Maps data of arbitrary size to data of a fixed size.
- [ ] Hashing makes data easy to reconstruct.

6. You are using the command line in Kali Linux. An encrypted file named `confidential.cpt` is in your present working directory, and you used `ccrypt` to encrypt this file. You just learned that the file's encryption key is compromised, so you should change it for security purposes. Which command can you use to change the file's encryption key? **1 point**

- ( ) `ccrypt -x confidential.cpt`
- ( ) `ccrypt -c confidential.cpt`
- (•) `ccrypt -u confidential.cpt`
- ( ) `ccrypt -K confidential.cpt`

7. You need to send your coworker an encrypted message through email. For encryption, you will both use an OpenPGP-compliant program such as Mailvelope. Which key must you use to encrypt the message? **1 point**

- ( ) Your private key
- ( ) Your public key
- ( ) Your coworker's private key
- (•) Your coworker's public key

Coursera Honor Code Learn more

[x] I, **Giang Pham**, understand that submitting work that isn't my own may result in permanent failure of this course or deactivation of my Coursera account.

Submit Save draft