

## **Quiz - Cryptography and Compliance Pitfalls**

1. True or False: A whole branch of hacking - Reverse Engineering - is devoted to discovering hidden algorithms and data.  
☒ True  
☐ False
  
2. Which is not a key takeaway of best practices of cryptography?  
☐ Do encrypt all sensitive data, at rest, in use, and in transit.  
☐ Do rely on proven algorithms.  
☒ Do rely on your own encryption algorithms.  
☐ Do use hard to guess keys and store them correctly.
  
4. What is the recommendation to avoid the encrypting data at rest pitfall "Using hardcoded/easily guessed keys"?  
☐ Use a new random initialization vectors every time.  
☒ Select cryptographically-random keys, do not reuse keys for different installs.  
☐ Phase them out  
☐ Store keys in secure keystores.

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

- ☐ Hashing makes data easy to reconstruct.
- ☒ Hashing provides integrity.
- ☒ Maps data of arbitrary size to data of a fixed size.