

1. In the “ISO two-pass unilateral authentication protocol using a Cryptographic Check Function (CCF)”, what is used to provide authentication?

- A. One-way hash function
- B. Signature
- C. Symmetric encryption
- D. Private key

答案：A

难易程度：中

答案解析：几种认证方式的 ISO 标准

知识点：Authentication-I (PPT 题目) → ISO Standardization of Authentication II (章节题目)

2. Which of the following method could be used to provide the freshness of message and liveness of principle?

- A. Timestamp
- B. Password
- C. Nonce
- D. Sequence number

答案：ACD

难易程度：难

答案解析：认证实现消息新鲜性和主体活现性的技术

知识点：Authentication-I (PPT 题目) → Message Freshness and Principle Liveness, Authentication based on Timestamp, ISO Timestamp Mechanism I (章节题目)

3. Which of the following statement is correct?

- A. Timestamp-based authentication is easy to maintain.
- B. Challenge-response mechanism is used to protect the secrecy of message.
- C. Signature is the only way to realize authentication.
- D. Mutual authentication is not a direct addition of two one-directional authentications.

答案：D

难易程度：难

答案解析：认证实现技术

知识点：Authentication-I (PPT 题目) → Authentication based on Timestamp, Challenge-Response Authentication, Authentication Mechanism II, Mutual Authentication (章节题目)

4. A two-factor authentication provides an extra layer of security, but the usability is poor.

答案：对

难易程度：易

答案解析：双因子认证

知识点：Authentication-II (PPT 题目) → Security and Usability of TFA (章节题目)

5. Given a one-way hash function $y=f(x)$, it is easy to compute x knowing y .

答案：错

难易程度：易

答案解析：哈希函数

知识点: Authentication-I (PPT 题目) → One-Way Hash Function (章节题目)

6. What deficiency categories are used to describe authentication mechanism when choosing a suitable form of password for on-line bank?

- A. Accessibility
- B. Memorability
- C. Security
- D. Cost

答案: ABCD

难易程度: 难

答案解析: 口令的可用性分析方法

知识点: Authentication-II (PPT 题目) → Quality Criteria (章节题目)

7. Which of the following are the international organizations that work exclusively on standardization?

- A. IEEE
- B. NIST
- C. ISO
- D. IEC

答案: CD

难易程度: 中

答案解析: 挑战-应答认证方法

知识点: Authentication-I (PPT 题目) → Standardization (章节题目)

8. Which of the following is type of biometric authentication?

- A. Voice print
- B. Facial recognition
- C. PIN code
- D. Finger prints

答案: ABD

难易程度: 易

答案解析: 基于生物认证的常用方法

知识点: Authentication-II (PPT 题目) → Biometrics (章节题目)

9. What type of attack is the quickest if a user uses the password "orange"?

- A. Brute force
- B. Common word
- C. Dictionary attack
- D. None of above

答案: B

难易程度: 中

答案解析: 可用性口令实现方法

知识点: Authentication-II (PPT 题目) → Some Real Examples (章节题目)

10. Which of the following password is the most secure?

A. As34df

B. sometimes extra student clever

C. abc123

D. d0gz&c4Ts

答案： B

难易程度： 中

答案解析： 可用性口令实现方法

知识点： Authentication-II（PPT 题目） → Usable and Secure Password（章节题目）