

1. 【单选题】 In the Vigenere cipher, let the plaintext $M = \text{finaltest}$, key $K = \text{dec}$, what is the ciphertext C ?

- A. ompdpvhvw
- B. hmpdpvhvw
- C. imppdvhwv
- D. impdpvhvw

答案: D

难易程度: 中

答案解析: 置换密码

知识点: Encryption (PPT 题目) → Polyalphabetic cipher (章节题目)

2. 【多选题】 Which of the following statements about PGP are correct?

- A. PGP employs a trusted server to verify public key certificate.
- B. The UI design of security software should consider some special principles.
- C. The usability evaluation is always difficult because of security's special properties.
- D. PGP is used to grant access to system visitors.

答案: BC

难易程度: 难

答案解析: PGP 的介绍及可用性分析

知识点: Encryption (PPT 题目) → Web of trust、Usability study of PGP 5.0 (章节题目)

3. 【多选题】 Which of the following statements about PGP are NOT correct?

- A. The metaphor of sign has a correct design.
- B. The information for the keys is appropriate.
- C. The key server has ambiguous definition.
- D. The key size can reveal the strength of security.

答案: AB

难易程度: 难

答案解析: PGP 可用性分析

知识点: Encryption (PPT 题目) → Key type analysis、Key server (章节题目)

4. 【多选题】 Which of the followings are the requirements for usable encryption?

- A. Persistent
- B. Share with anyone
- C. Positive control
- D. Visibility and audit

答案: ABCD

难易程度: 中

答案解析: 实用加密的原则

知识点: Encryption (PPT 题目) → Four principles of usable encryption (阅读材料 2)

5. 【多选题】 Privacy is the individual and organization's decision of ____ information is communicated to others.

- A. When
- B. Where
- C. How
- D. To what extent

答案：ACD

难易程度：中

答案解析：隐私的定义

知识点：Privacy-I（PPT 题目）→What is privacy（章节题目）

6. 【单选题】Why awareness is important for CSCW?

- A. Because it is required.
- B. Because many people use it.
- C. Because CSCW supports cooperative work.
- D. Because the privacy protection is well settled in CSCW.

答案：C

难易程度：易

答案解析：CSCW 中的隐私

知识点：Privacy-I（PPT 题目）→ Privacy in CSCW（章节题目）

7. 【多选题】What should be done in providing informed consent?

- A. Authorization
- B. Disclosure
- C. Competence
- D. Minimal distraction

答案：BCD

难易程度：中

答案解析：知情同意

知识点：Privacy-II（PPT 题目）→ Six components（章节题目）

8. 【单选题】Evidence to avoid the pitfall in obscuring potential information flow include:

- A. Turn on the cookies.
- B. When user logs into e-mail address, give user clear illustration.
- C. Use jargons in privacy policy.
- D. Privacy settings in windows.

答案：B

难易程度：中

答案解析：隐私设计的五个陷阱

知识点：Privacy-II（PPT 题目）→Obscuring potential information flow（章节题目）

9. 【多选题】Which of the following is provided in 4G/5G mobile communication?

- A. IMEI
- B. IMSI

C. Location

D. SMS

答案：ABCD

难易程度：中

答案解析：实用隐私技术

知识点：Privacy-II（PPT 题目）→ Privacy assets（章节题目）

10. 【单选题】 Which of the following is not included in a P3P format?

A. Access

B. Consequence

C. Purpose

D. Algorithm description

答案：D

难易程度：中

答案解析：P3P

知识点：Privacy-III（PPT 题目）→ P3P format（章节题目）