

Quiz 5 - Mật mã bất đối xứng

Tổng điểm 7/7 ?

Các câu hỏi lựa chọn đáp án có thể có nhiều hơn 1 đáp án.

MSSV *

20215041

Câu 1. Trong thuật toán sinh khóa RSA, cho $p = 5$, $q = 7$. Giá trị khóa công khai $\{e, 1/n\}$ có thể lựa chọn là bao nhiêu? (Chọn tất cả đáp án đúng)

- ☐ {9, 35}
- ☒ {11, 35}
- ☒ {13, 35}
- ☐ {15, 35}
- ☒ {17, 35}

Câu 2. Trong hệ mật RSA, giả sử giá trị khóa công khai là $\{37, 77\}$. Giá trị d của khóa cá nhân là bao nhiêu?

13

Câu 3. Trong hệ mật RSA, giả sử giá trị khóa công khai là $(7, 55)$. Nếu bản gốc $M = 8$ thì giá trị bản mã C là bao nhiêu?

2



Câu 4. Ưu điểm của phương pháp mã hóa RSA-OEAP so với phương pháp RSA gốc là gì? 1/1

- ☒ An toàn hơn
- ☐ Tốc độ thực hiện nhanh hơn
- ☐ Có thể mã hóa bản tin có độ dài bất kỳ
- ☐ Tất cả các đáp án trên

Câu 5. Để chống lại các hành vi nghe lén trong quá trình truyền tin tới phía nhận, 1/1 phía gửi có thể thực hiện bằng một trong những cách nào sau đây?(Chọn tất cả đáp án đúng)

- ☐ Mã hóa bằng thuật toán RSA với khóa cá nhân của người nhận
- ☐ Mã hóa bằng thuật toán RSA với khóa cá nhân của người gửi
- ☒ Mã hóa bằng thuật toán RSA với khóa công khai của người nhận
- ☐ Mã hóa bằng thuật toán RSA với khóa công khai của người gửi
- ☒ Mã hóa bằng thuật toán AES với khóa đã chia sẻ trước

Câu 6. Hệ mật mã nào sau đây sử dụng khóa mã hóa và giải mã khác nhau? 1/1

- ☒ RSA
- ☐ AES
- ☐ 3DES
- ☐ DES



Câu 7. Ưu điểm của mật mã khóa công khai so với mật mã khóa đối xứng là gì? 1/1

- ☐ Tốc độ nhanh hơn
- ☐ Không thể bị tấn công vét cạn
- ☒ Không cần kênh bí mật để trao đổi khóa mã hóa
- ☐ An toàn hơn

Biểu mẫu này đã được tạo ra bên trong School of Information & Communication Technology.

Google Biểu mẫu

