Quiz 5 - Mật mã đối xứng(2) và mật mã bất đối xứng

Tổng điểm 13/13

MSSV *

20204974

✓ Câu 1. Ưu điểm của chế độ mã CTR so với CBC là gì?(Chọn 2 đáp án) 1/1

- [x] Tốc độ mã hóa nhanh hơn ✓
- [x] Không cần thêm phần đệm ✓
- [ ] An toàn hơn trước tấn công CCA
- [ ] Không cần giữ mật giá trị IV

✓ Câu 2. Sử dụng mật mã 3DES ở chế độ CBC cho bản tin có kích thước 200 byte. Phần đệm có kích thước bao nhiêu byte? 1/1

8 ✓

✓ Câu 3. Sử dụng mật mã AES ở chế độ CBC cho bản tin có kích thước 201 byte. Nếu dùng chuẩn PKCS#7, giá trị phần đệm viết dưới dạng hexa là bao nhiêu? 1/1

07070707070707 ✓

✓ Câu 4. Giả sử khi sử dụng chế độ CBC và CTR, giá trị IV là giá trị thời gian hiện tại của hệ thống. Phát biểu nào sau đây là đúng? 1/1

- ( ) Cả 2 chế độ mã là an toàn trước tấn công CPA
- ( ) Cả 2 chế độ mã không an toàn trước tấn công CPA
- (•) Mã ở chế độ CBC là không an toàn trước tấn công CPA, còn CTR vẫn an toàn ✓
- ( ) Mã ở chế độ CBC là an toàn trước tấn công CPA, còn CTR thì không

✓ Câu 5. Giả sử khi sử dụng chế độ CBC và CTR, giá trị IV được xác định bằng cách mã hóa giá trị thời gian hiện tại của hệ thống. Phát biểu nào sau đây là đúng? 1/1

- (•) Cả 2 chế độ mã là an toàn trước tấn công CPA ✓
- ( ) Cả 2 chế độ mã không an toàn trước tấn công CPA
- ( ) Mã ở chế độ CBC là không an toàn trước tấn công CPA, còn CTR vẫn an toàn
- ( ) Mã ở chế độ CBC là an toàn trước tấn công CPA, còn CTR thì không

✓ Câu 6. Nếu sử dụng mật mã AES ở chế độ CBC, để xác suất tấn công CPA là không đáng kể thì sau khi mã hóa 2^x khối phải đổi khóa. Giá trị x là bao 1/1

nhiêu?

24 ✓

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

- [ ] {9, 35}
- [x] {11, 35} ✓
- [x] {13, 35} ✓
- [ ] {15, 35}
- [x] {17, 35} ✓

✓ Câu 8. Trong hệ mật RSA, giả sử giá trị khóa công khai là {37, 77}. Giá trị d của khóa cá nhân là bao nhiêu? 1/1

13 ✓

✓ Câu 9. 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? 1/1

2 ✓

✓ Câu 10. 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 11. Để chống lại các hành vi nghe lén trong quá trình truyền tin tới phia nhận, phia gửi có thể thực hiện bằng một trong những cách nào sau đây?(Chọn tất cả đáp án đúng) 1/1

- [x] Mã hóa bằng thuật toán AES với khóa đã chia sẻ trước ✓
- [ ] 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
- [x] 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

✓ Câu 12. Hệ mật mã nào sau đây sử dụng khóa mã hóa và giải mã khác nhau? 1/1

- ( ) 3DES
- (•) RSA ✓
- ( ) AES

- ○ DES

✓ Câu 13. 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