Quiz 4 - Mật mã đối xứng (1)

Tổng điểm 15/15

MSSV *

20204974

✓ Câu 1. Để giảm độ rủi ro hệ thống mật mã bị tấn công vét cạn, phương pháp nào sau đây được sử dụng?(Chọn tất cả đáp án đúng) 1/1

- [ ] Thêm giá trị ngẫu nhiên vào bản tin trước khi mã hóa
- [ ] Đảo ngược nội dung bản tin trước khi mã hóa
- [x] Sử dụng khóa có kích thước dài hơn ✓
- [x] Sinh giá trị khóa một cách ngẫu nhiên ✓

✓ Câu 2. Giả sử trung bình kẻ tấn công mất 100 năm để bẻ khóa được hệ mật mã bằng phương pháp vét cạn. Nếu hắn biết được chắc chắn giá trị của 2 bit khóa thì thời gian tấn công là bao nhiêu năm? 1/1

25 ✓

✓ Câu 3. Giả sử kẻ tấn công thực hiện tấn công sử dụng phương pháp tấn công vét cạn với tốc độ thử mỗi khóa mất 1 chu kỳ CPU. Tốc độ CPU ước tính trên máy tính kẻ tấn công sử dụng là 16 GHz. Khóa cần phải có kích thước tối thiểu là bao nhiêu bit để trong thời gian tấn công 100 năm thì xác xuất thành công của kẻ tấn công nhỏ hơn 1/2^60. 1/1

126 ✓

✓ Câu 4. Giả sử kẻ tấn công thực hiện tấn công sử dụng phương pháp tấn công vét cạn với tốc độ thử mỗi khóa mất 1 chu kỳ CPU. Tốc độ CPU ước tính trên máy tính kẻ tấn công sử dụng là 16x10^6 GHz. Khóa cần phải có kích thước tối thiểu là bao nhiêu bit để trong thời gian tấn công 100 năm thì xác xuất thành công của kẻ tấn công nhỏ hơn 1/2^60. 1/1

146 ✓

✓ Câu 5. Mật mã dịch vòng(Shift cipher) là an toàn trước dạng tấn công nào? 1/1

- ( ) Tấn công chọn trước bản rõ
- ( ) Tấn công chỉ biết bản mật
- (•) Không an toàn trước tất cả các dạng tấn công trên ✓
- ( ) Tấn công chọn trước bản mật
- ( ) Tấn công biết trước bản rõ

✓ Câu 6. Khi sử dụng mật mã one-time-pad, nếu chuỗi bit mã là c = 01010011 và khóa k = 00110001 thì kết quả giải mã là gì? 1/1

01100010

✓ Câu 7. Khi sử dụng mật mã one-time-pad, nếu chuỗi bit bản rõ m = 11101000 và bản mã c = 01010011 thì khóa k bằng bao nhiêu? 1/1

10111011 ✓

✓ Câu 8. Hệ mật DES sử dụng khóa có kích thước bao nhiêu bit?(Câu trả lời chỉ chứa giá trị số) 1/1

56 ✓

✓ Câu 9. Kích thước khối dữ liệu trong mật mã DES là bao nhiêu bit?(Chỉ viết đáp án là số) 1/1

64 ✓

✓ Câu 10. Nếu ký hiệu E(K) là phép mã hóa DES, D(K) là phép giải mã DES thì trình tự mã hóa theo 3DES có thể là gì?(Chọn 2 đáp án) 1/1

- [ ] E(K1) - E(K2) - D(K3)
- [x] E(K1) - D(K2) - E(K1) ✓
- [ ] E(K1) - E(K2) - D(K1)
- [x] E(K1) - D(K2) - E(K3) ✓

✓ Câu 11. Mật mã AES sử dụng khóa có kích thước bao nhiêu?(Chọn tất cả đáp án) 1/1

- [ ] 64
- [x] 128 ✓
- [x] 192 ✓
- [x] 256 ✓

✓ Câu 12. Kích thước khối dữ liệu của mật mã AES là bao nhiêu bit?(Chỉ viết đáp án là số) 1/1

128 ✓

✓ Câu 13. Phương pháp mật mã nào sau đây còn an toàn để sử dụng?(Chọn tất cả đáp án đúng) 1/1

- [ ] DES
- [ ] 2DES
- [x] 3DES ✓
- [x] AES ✓

✓ Câu 14. Chế độ mã ECB chống lại được dạng tấn công nào dưới đây? 1/1

- ○ Tấn công chọn trước bản rõ(CPA)
- ○ Tấn công chọn trước bản mật(CCA)
- ○ Tấn công biết trước bản rõ(KPA)
- ◉ Không chống được loại tấn công nào đã liệt kê ✓

✓ Câu 15. Hạn chế của chế độ mã ECB so với CBC là gì? 1/1

- ○ Tốc độ thực hiện chậm hơn
- ◉ Không an toàn để sử dụng ✓
- ○ Không có cơ chế kiểm tra toàn vẹn
- ○ Kích thước bản gốc phải chia hết cho kích thước của khối