Quiz 3 - Khái niệm cơ bản về mật mã học và mật mã đối xứng (1)

Tổng điểm 18/18

MSSV *

20215041

Câu 1. Mật mã dịch vòng sử dụng cách thức nào? 1/1

- [ ] Phép toán XOR
- [ ] Hoán vị các ký tự
- [x] Thay thế ký tự

Câu 2. Để giảm độ rủi ro hệ thống mật mã bị tấn công vét cạn, phương pháp nào sau đây được sử dụng? 1/1

- [ ] Sử dụng giá trị khóa khó đoán hơn
- [x] Sử dụng khóa có kích thước dài hơn
- [ ] Đảo ngược nội dung bản tin trước khi mã hóa

Câu 3. Theo nguyên lý Kerckhoff, cần giữ mật thông tin gì trong hệ mật mã? 1/1

- [ ] Thuật toán mã hóa
- [x] Giá trị khóa
- [ ] Thuật toán giải mã
- [ ] Khuôn dạng bản tin gốc
- [ ] Thuật toán tạo khóa

Câu 4. Kết quả mã hóa bản tin "SECURITY" bằng mật mã dịch vòng với giá trị khóa k = 10 là gì?(Viết hoa toàn bộ) 1/1

COMEBSDI

Câu 5. Nếu sử dụng mật mã dịch vòng mã hóa bản gốc là "HELLO" thành bản mật là "BYFFI" thì giá trị khóa đã sử dụng là bao nhiêu? 1/1

20

Câu 6. Nếu sử dụng bản chữ cái tiếng Anh, số lượng giá trị khóa khả dụng của mã dịch vòng là bao nhiêu? 1/1

25

Câu 7. 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 8. 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 9. 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 10. Mật mã dịch vòng(Shift cipher) là an toàn trước dạng tấn công nào? 1/1

- [ ] Tấn công chỉ biết bản mật
- [ ] Tấn công biết trước bản rõ
- [ ] Tấn công chọn trước bản rõ
- [ ] Tấn công chọn trước bản mật
- [x] Không an toàn trước tất cả các dạng tấn công

Câu 11. 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 12. 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 13. Hệ mật DES sử dụng khóa có kích thước bao nhiêu bit?(Câu trả lời chỉ chứa giá trị số) 1/1

56

Câu 14. Kích thước khối dữ liệu trong mật mã DES là bao nhiêu bít?(Chỉ viết đáp án là số) 1/1

64

Câu 15. 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? 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 16. Mật mã AES sử dụng khóa có kích thước bao nhiêu? 1/1

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

Câu 17. Kích thước khối dữ liệu của mật mã AES là bao nhiêu bit?(Chỉ viết đáp án số) 1/1

128

Câu .18 Phương pháp mật mã nào sau đây còn an toàn để sử dụng? 1/1

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