

Quiz 4 - Mật mã khóa đối xứng (1)

Tổng điểm 13/13 ?

MSSV *

20200497

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

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

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

25



Câu 3. Giả sử kẻ tấn công thực hiện tấn công sử dụng phương pháp tấn công vét1/1 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 suất thành công của kẻ tấn công nhỏ hơn $1/2^{60}$.

126

Câu 4. Giả sử kẻ tấn công thực hiện tấn công sử dụng phương pháp tấn công vét1/1 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 16×10^6 GHz. Khóa cần phải có kích thước tối thiểu là bao nhiêu bit để trong thời gian tấn công 100 năm thì xác suất thành công của kẻ tấn công nhỏ hơn $1/2^{60}$.

146



Câu 5. 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
- ☒ Không an toàn trước tất cả các dạng tấn công

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

01100010

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

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? 1/1

- ☒ $E(K1) - D(K2) - E(K1)$
- ☒ $E(K1) - D(K2) - E(K3)$
- ☐ $E(K1) - E(K2) - D(K3)$
- ☐ $E(K1) - E(K2) - D(K1)$



Câu 11. Mật mã AES sử dụng khóa có kích thước bao nhiêu?

1/1

- ☒ 256
- ☐ 64
- ☒ 128
- ☒ 192

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

1/1

128

Câu 13. Phương pháp mật mã nào sau đây còn an toàn để sử dụng?

1/1

- ☐ 2DES
- ☐ DES
- ☒ 3DES
- ☒ AES

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



Google Biểu mẫu



