Quiz 3- Cơ bản về mật mã

Homework due Jul 1, 2025 07:00 +07 ***Completed***

Question #b5fcd

1/1 point (graded)

Câu 1. Mật mã dịch vòng sử dụng (những) toán tử nào?

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

✔

Submit

Question #a4cdd

1/1 point (graded)

Câu 2. Theo nguyên lý Kerckhoff, cần giữ mật thông tin gì trong hệ mật mã?

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

✔

Submit

Question #c862c

1/1 point (graded)

Câu 3. (Những) Phát biểu nào sau đầy là đúng về hệ mật hoàn hảo là gì?

- [ ] Hệ mật hoàn hảo chỉ tồn tại trên lý thuyết, không thể thiết kế một hệ mật hoàn hảo mà có thể sử dụng trên thực tế
- [x] Trước mọi thuật toán tấn công hiệu quả(có độ phức tạp đa thức), hệ mật hoàn hảo luôn an toàn
- [x] Trong hệ mật hoàn hảo, xác suất xuất hiện của mọi giá trị khóa là như nhau
- [x] Trong hệ mật hoàn hảo, khóa phải có kích thước tối thiểu bằng kích thước bản tin gốc
- [ ] Khi thiết kế được một hệ mật hoàn hảo, khóa có thể dùng lại mà không ảnh hưởng đến tính an toàn

✔

Submit

Question #cf6f6

1/1 point (graded)

Câu 4. Để giảm độ rủi ro hệ thống mật mã bị tấn công vét cạn, (những) phương pháp nào sau đây được sử dụng?

- [ ] Đảo ngược nội dung bản tin trước khi mã hóa
- [x] Sử dụng khóa có kích thước lớn hơn
- [x] Tạo sinh khóa hoàn toàn ngẫu nhiên
- [ ] Nén bản tin gốc trước khi mã hóa

✔

Submit

Question #2ba32

1/1 point (graded)

Câu 5. 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?

25 ✔

Submit

Question #5bda7

1/1 point (graded)

Câu 6. 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 2^{-60}?

126 ✔

Submit

Question #6e229

1/1 point (graded)

Câu 7. 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.

146 ✔

146

Submit