20225261
bao.kv225261@sis.hust.edu.vn

1 2 3 4 5
6 7 8 9

Quiz 4 - Mật mã khóa đối xứng

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

Question #113f6

1/1 point (graded)

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

COMEBSDI ✔

Submit

Question #6058c

1/1 point (graded)

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?

20 ✔

20

Submit

Question #e042b

1/1 point (graded)

Khi sử dụng mật mã Vernam (one-time-pad), nếu chuỗi bit mã là c = 01010011 và khóa k = 00110001 thì kết quả giải mã là gì?

01100010 ✔

01100010

Submit

Question #899be

1/1 point (graded)

Khi sử dụng mật mã Vernam (one-time-pad), nếu chuỗi bit bản rõ m = 11101000 và bản mã c = 01010011 thì khóa k bằng bao nhiêu?

10111011 ✔

10111011

Submit

Question #89487

1/1 point (graded)

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

64 ✔

Submit

Question #70173

1/1 point (graded)

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?

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

✔

Submit

Question #60044

1/1 point (graded)

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

128 ✔

128

Submit

Question #b39f0

1/1 point (graded)

Trong kỹ thuật thám mã nào sau đây, kẻ tấn công có nhiều quyền truy cập nhất trong hệ thống?

- ○ Tấn công biết trước bản rõ
- ○ Tấn công chọn trước bản rõ
- ◉ Tấn công chọn trước bản mật
- ○ Tấn công chỉ biết bản mật

✔

Submit

Question #794ee

1/1 point (graded)

Bob muốn triển khai mật mã Vernam (one-time-pad) nhưng sử dụng khóa có kích thước cố định n bit để mã hóa khối dữ liệu có kích thước n bit. Với bản tin kích thước 2n bit, Bob thực hiện mã hóa E(k, m1 || m2) = OTP-Enc(k, m1) || OTP-Enc(k, m2). Cách thức mã hóa này của Bob an toàn trước (những) kỹ thuật thám mã nào?

- [ ] Tấn công biết trước bản rõ
- [ ] Tấn công chọn trước bản rõ
- [ ] Tấn công chọn trước bản mật
- [x] Không an toàn trước dạng tấn công nào