



20225261

bao.kv225261@sis.hust.edu.vn

1

2

3

4

5

6

7

8

Quiz 5 - Các chế độ của mật mã khóa đối xứng

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

Question #6207f

1/1 point (graded)

Câu 1. Chế độ mã ECB chống lại được (những) dạng tấn công nào dưới đây?

- ☐ 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



Submit

Question #ca71c

1/1 point (graded)

Câu 2. Hạn chế của chế độ mã ECB so với CBC là gì?

- ☐ 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



Submit

Question #3dea2

1/1 point (graded)

Câu 3. Ưu điểm của chế độ mã CTR so với CBC là gì?

- ☒ Tốc độ mã hóa nhanh hơn
- ☒ Không cần thêm phần đệm
- ☐ An toàn hơn trước tấn công CCA
- ☐ Không cần giữ mật giá trị IV



Submit

### Question #ea633

1/1 point (graded)

Câu 4. Sử dụng mật mã 3DES ở chế độ CBC cho bản tin có kích thước 200 byte. Phần đệm có kích thước bao nhiêu byte?



Submit

### Question #29de1

1/1 point (graded)

Câu 5. Sử dụng mật mã AES ở chế độ CBC cho bản tin có kích thước 201 byte. Nếu dùng chuẩn PKCS#7, giá trị phần đệm viết dưới dạng hexa là bao nhiêu?



Submit

### Question #208d2

1/1 point (graded)

Câu 6. Giả sử khi sử dụng chế độ CBC và CTR, giá trị IV là giá trị thời gian hiện tại của hệ thống. Phát biểu nào sau đây là đúng?

- ☒ Cả 2 chế độ mã không an toàn trước tấn công CPA
- ☐ Cả 2 chế độ mã là an toàn trước tấn công CPA
- ☐ Mã ở chế độ CBC là không an toàn trước tấn công CPA, còn CTR vẫn an toàn
- ☐ Mã ở chế độ CBC là an toàn trước tấn công CPA, còn CTR thì không



Submit

### Question #0107f

1/1 point (graded)

Câu 7. Giả sử khi sử dụng chế độ CBC và CTR, giá trị IV được xác định bằng cách mã hóa giá trị thời gian hiện tại của hệ thống. Phát biểu nào sau đây là đúng?

- ☐ Mã ở chế độ CBC là không an toàn trước tấn công CPA, còn CTR vẫn an toàn
- ☐ Cả 2 chế độ mã không an toàn trước tấn công CPA
- ☒ Cả 2 chế độ mã là an toàn trước tấn công CPA
- ☐ Mã ở chế độ CBC là an toàn trước tấn công CPA, còn CTR thì không



Submit

### Question #c4707

1/1 point (graded)

Câu 8. Nếu sử dụng mật mã AES ở chế độ CBC, để xác suất tấn công CPA là không đáng kể thì sau khi mã hóa  $2^x$  khối phải đổi khóa. Giá trị  $x$  là bao nhiêu?



Submit