Quiz 5 - Mật mã đối xứng (2)

Tổng điểm 8/8

Các câu hỏi lựa chọn đáp án có thể có nhiều hơn 1 đáp án.

MSSV *

20200497

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

- [ ] Tấn công chọn trước bản rõ(CPA)
- [ ] Tấn công chọn trước bản mật(CCA)
- [ ] Tấn công biết trước bản rõ(KPA)
- [x] Không chống được loại tấn công nào đã liệt kê

Câu 2. Hạn chế của chế độ mã ECB so với CBC là gì? 1/1

- [ ] Tốc độ thực hiện chậm hơn
- [x] 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

Câu 3. Ưu điểm của chế độ mã CTR so với CBC là gì? 1/1

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

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? 1/1

8

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? 1/1

07070707070707

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? 1/1

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

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? 1/1

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

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? 1/1

24