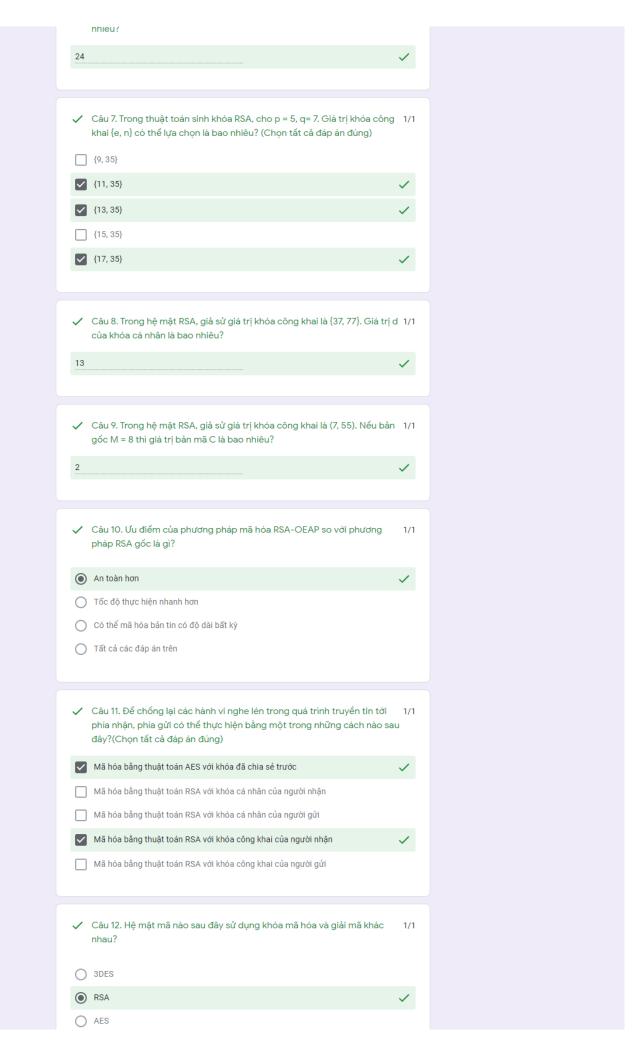
Quiz 5 - Mật mã đối xứng(2) và mật mã bất đối xứng Tổng điểm 13/13 ?

MSSV * 20204974
✓ Câu 1. Ưu điểm của chế độ mã CTR so với CBC là gi?(Chọn 2 đáp án) 1/1
✓ 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
✓ Câu 2. Sử dụng mật mã 3DES ở chế độ CBC cho bản tin có kích thước 1/1 200 byte. Phần đệm có kích thước bao nhiều byte?
8
Câu 3. Sử dụng mật mã AES ở chế độ CBC cho bản tin có kích thước 201 1/1 byte. Nếu dùng chuẩn PKCS#7, giá trị phần đệm viết dưới dạng hexa là bao nhiêu?
07070707070707
Câu 4. Giả sử khi sử dụng chế độ CBC và CTR, giá trị IV là giá trị thời gian 1/1 hiện tại của hệ thống. Phát biểu nào sau đây là đúng?
Cả 2 chế độ mã là an toàn trước tấn công CPA
Cả 2 chế độ mã không 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
Câu 5. Giả sử khi sử dụng chế độ CBC và CTR, giá trị IV được xác định 1/1 bằng cách mã hóa giá trị thời gian hiện tại của hệ thống. Phát biểu nào sau đây là đúng?
Cả 2 chế độ mã là an toàn trước tấn công CPA
Cả 2 chế độ mã không 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

✓ Câu 6. Nếu sử dụng mật mã AES ở chế độ CBC, để xác suất tấn công CPA 1/1 là không đáng kể thì sau khi mã hóa 2^x khối phải đổi khóa. Giá trị x là bao



O DES
✓ Câu 13. Ưu điểm của mật mã khóa công khai so với mật mã khóa đối xứng 1/1 là gì?
Tốc độ nhanh hơn Không thể bị tấn công vét cạn
O An toàn hơn
Biểu mẫu này đã được tạo ra bên trong School of Information & Communication Technology.
C D13 %

Google Biểu mẫu

1