Quiz 7. Mã xác thực thông điệp(MAC)

Tổng điểm 6/6

Các câu hỏi lựa chọn có thể có nhiều hơn 1 đáp án. Cần phải lựa chọn tất cả đáp án đúng.

MSSV *

20200497

Câu 1. Một hệ thống bán hàng cung cấp tính năng cho phép người dùng tính giá trị MAC cho đơn hàng với khóa bí mật chỉ do người dùng biết. Người sử dụng lưu lại giá trị MAC và khóa này. Sử dụng mã MAC trong trường hợp này có tác dụng gì với người dùng? 1/1

- [x] Khẳng định đơn hàng do chính người dùng tạo ra
- [ ] Nội dung đơn hàng là bí mật
- [ ] Khi dữ liệu trên máy chủ bị mất, người dùng có thể cung cấp lại nội dung đơn hàng
- [x] Khẳng định đơn hàng không bị người khác sửa đổi

Câu 2. Trong các hệ thống truyền tin, tại sao sử dụng hàm MAC không mang lại khả năng chống từ chối? 1/1

- ○ Tất cả các lý do trên
- ○ Có thể tìm ra các bản tin có cùng giá trị MAC
- ◉ Các bên cùng biết khóa để tạo giá trị MAC
- ○ Không thể xác định được nội dung bản tin gốc từ giá trị MAC

Câu 3. Tại sao hàm MAC phải được thiết kế để rất khó tìm ra hai bản tin có mã MAC giống nhau? 1/1

- ☐ Kẻ tấn công không thể xác định được nội dung bản tin gốc
- ☑ Kẻ tấn công không thể thay thế nội dung được bản tin gốc
- ☐ Để kích thước đầu ra là không đổi với mọi bản tin
- ☐ Giảm chi phí tính toán

Câu 4. Ký hiệu E là hàm mã hóa, D là hàm giải mã, S là hàm tính giá trị MAC, V là hàm kiểm tra MAC. Nếu nhận được bản tin có cấu trúc E(k1, m) || t, trong đó t = S(k2, E(k1, m)) thì xử lý bản tin này như thế nào? 1/1

- ○ Giải mã D(k1, E(m) || t), sau đó kiểm tra V(k2, m, t)
- ○ Giải mã D(k1, E(m)), sau đó kiểm tra V(k2, m, t)
- ◉ Kiểm tra V(k2, E(k1, m), t), sau đó giải mã D(k1, E(m)) nếu V = true

Câu 5. Giả sử E là hàm mã hóa ở chế độ CBC, S là hàm tính giá trị MAC. Sơ đồ mật mã nào sau đây luôn chống lại được tấn công CCA? 1/1

- ☑ E(k1, m) || S(k2, E(k1, m))
- ☐ E(k1, m) || S(k1, E(k1, m))
- ☐ E(k1, m) || S(k2, m)
- ☐ E(k1, m || S(k2, m))

Câu 6. Giả sử bản tin m có kích thước là 2 khối, m1 và m2. Alice mã hóa bản tin m ở chế độ ECB thành bản tin c có 2 khối, c1 và c2. Sau đó Alice tạo mã xác thực t = F(k, c) và gửi c || t cho Bob. Hàm F() nào sau đây cho phép Bob phát hiện bản tin nhận được đã bị sửa đổi bởi kẻ tấn công? Trong đó hàm S là hàm MAC an toàn. 1/1

- [x] F(k, c) = S(k, c2 || c1)
- [ ] F(k, c) = S(k, S(k, c1))
- [ ] F(k, c) = S(k, c1 XOR c2)
- [ ] F(k, c) = S(k, c1) || S(k, c2)
- [x] F(k, c) = S(k, c1 || c2)