ĐỀ THI GIỮA KỲ 20211
NHẬP MÔN AN TOÀN THÔNG TIN
Thời gian làm bài: 60 phút - Được phép sử dụng mọi tài liệu trên giấy

Câu 1.*(2 điểm)* Nguyên tắc an toàn bảo mật.

a. Khi dịch Covid-19 bùng phát, một siêu thị lớn muốn quản lý tốt hơn khách vào ra nên chỉ để mở 2 cửa, trong đó một cửa chỉ cho khách vào và một cửa chỉ cho khách ra. Nguyên tắc an toàn bảo mật nào đã được áp dụng. Hãy giải thích ngắn gọn để chứng minh?
b. Một hệ thống Web của công ty nọ yêu cầu nhân viên phải sử dụng mật khẩu có độ dài tối thiểu 10 ký tự, chứa các loại ký tự khác nhau. Điều đó khiến cho một số người đã ghi mật khẩu của họ vào tờ giấy ghi chú. Nguyên tắc an toàn bảo mật nào đã bị vi phạm? Hãy giải thích ngắn gọn để chứng minh.

Câu 2.*(2 điểm)* Giả sử Alice sử dụng hệ mật mã AES-128 với khóa ngẫu nhiên 128-bit để mã hóa các bản tin gửi cho Bob. Mallory đã thu thập được một số cặp thông điệp (m, c), trong đó m là bản rõ, c là bản mật. Mallory muốn thực hiện tấn công vét cạn để tìm khóa K mà Alice đang sử dụng.

a. Nếu Mallory có khả năng thử 1 triệu khóa/giây thì mất bao lâu Mallory tìm ra khóa K?
b. Mallory có một hệ thống gồm 1 triệu máy chủ, mỗi máy chủ có tốc độ thử 10 tỷ khóa/giây. Thời gian Mallory tìm ra khóa là bao lâu?
c. Mallory có một hệ thống máy tính lượng tử với khả năng cài đặt các thuật toán có độ phức tạp $O(\sqrt{n})$ thay cho các thuật toán có độ phức tạp $O(n)$ trên máy tính thông thường. Thời gian mà Mallory tấn công giảm đi bao nhiêu lần?
d. Nếu Alice sử dụng khóa 256-bit thì thời gian tấn công của Mallory tăng lên bao nhiêu lần?

Câu 3.*(3 điểm)* Giả sử server cần gửi thông điệp tới tất cả client C_1, C_2, .., C_n. Mỗi client khi nhận được thông điệp này cần xác minh được rằng thông điệp do chính server gửi. Giả sử rằng đã có một kênh an toàn được sử dụng để phân phối khóa giữa các bên.

a. Giả sử server và tất cả client chia sẻ một khóa đối xứng ngẫu nhiên cho từng phiên quảng bá. Server sử dụng khóa này để tạo mã MAC và gắn vào mỗi bản tin được gửi đi. Client có thể tin tưởng rằng thông điệp nhận được là do server gửi và nội dung thông điệp toàn vẹn hay không? Giải thích.

b. Giả sử server đã chia sẻ một khóa ngẫu nhiên với mỗi client cho từng phiên quảng bá. Server sử dụng khóa này để tạo mã MAC và gắn vào mỗi bản tin được gửi đi. Client có thể tin tưởng rằng thông điệp nhận được là do server gửi hay không? Giải thích.

c. Giả sử client nhận được một thông điệp từ server có chứa phần mềm độc hại. Client có thể khởi kiện server hay không? Giải thích.

Câu 4. *(3 điểm).* Giả sử Alice muốn gửi bản tin m cho Bob với các yêu cầu sau:

(1) Bí mật: Nội dung bản tin là bí mật với bên thứ 3 đối phương
(2) Xác thực: Bob xác định được ai là người gửi
(3) Toàn vẹn: Bob xác định được nội dung bản tin là nguyên gốc
(4) Chống từ chối: Alice không thể phủ nhận việc đã tạo ra bản tin

Trong các mô tả sau đây:

- k_S: Khóa bí mật đã được chia sẻ giữa Alice và Bob, thay đổi sau mỗi phiên
- (k_{UA}, k_{RA}): Cặp khóa công khai, khóa cá nhân của Alice
- (k_{UB}, k_{RB}): Cặp khóa công khai, khóa cá nhân của Bob
- E: Hàm mã hóa an toàn trước tấn công CPA
- H: Hàm băm an toàn

Tất cả các khóa đã được phân phối và bảo vệ an toàn. Trong mỗi cách thức gửi tin dưới đây, Bob có đọc được nội dung bản tin m không và quá trình truyền tin đạt được những yêu cầu nào đã đề cập ở trên? Giải thích ngắn gọn câu trả lời.

a. Alice gửi $E(k_{UA}, m) \,||\, H(m)$
b. Alice gửi $E(k_S, m) \,||\, H(m)$
c. Alice gửi $E(k_{UB}, m \,||\, E(k_{RA}, H(m)))$

---------- HẾT ----------