TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN, ĐHQG-HCM

ĐỀ THI KẾT THÚC HỌC PHẦN
Học kỳ II – Năm học 2021-2022

MÃ LƯU TRỮ
(do phòng KT-ĐBCL ghi)

Tên học phần: Mã hóa Ứng dụng **Mã HP:** CSC15003

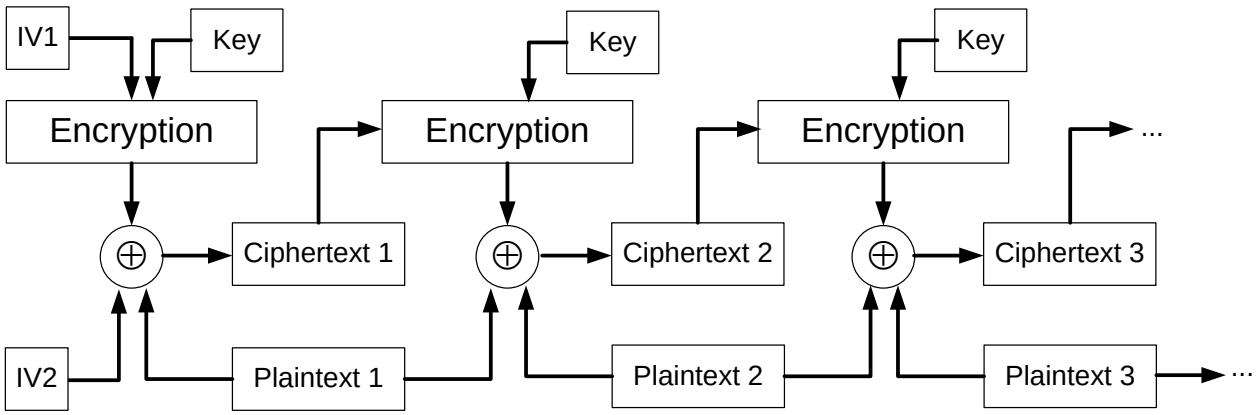
Thời gian làm bài: **120 phút** Ngày thi: **10/07/2022**

Ghi chú: *Sinh viên* [☐ *được phép* - ☑ *không được phép*] *sử dụng tài liệu khi làm bài.*

Câu 1. Chế độ mã hóa (3.0 điểm)

Xét chế độ mã hóa (mode of operation) sau:

$C_0 = \mathbf{IV1}, P_0 = \mathbf{IV2}, C_i = P_{i-1} \oplus P_i \oplus E_K(C_{i-1})$



Ghi chú: **IV** : initialization vector **Plaintext** (P_i) : nội dung trước khi mã hóa

Key : khóa **Ciphertext** (C_i) : nội dung sau khi mã hóa

a) Hãy trình bày quy trình giải mã dữ liệu (*gợi ý: vẽ sơ đồ giải mã dữ liệu*) *(1.0 điểm)*

b) Hãy nhận xét về khả năng xử lý song song khi mã hóa và khi giải mã thông tin *(1.0 điểm)*

c) Giả sử trong quá trình truyền dữ liệu (*đã mã hóa*), ***bit thứ i trong khối 1 (C_1) bị sai và bit thứ j trong khối 2 (C_2) bị sai***. Hãy nhận xét về việc lan truyền lỗi khi giải mã toàn bộ thông điệp nhận được. *(1.0 điểm)*

✍ ***Gợi ý***: Anh/Chị nên xét hai trường hợp : $i = j$ và $i \neq j$

Câu 2. Một số kiến thức cơ bản (2.0 điểm)

a) **Mật khẩu đăng nhập hệ thống**: *(1.0 điểm)*

Trong các hệ thống dịch vụ trực tuyến, tên đăng nhập và mật khẩu thường được dùng để chứng thực người dùng. Giải pháp đơn giản là lưu trữ tên đăng nhập và mật khẩu của người dùng vào cơ sở dữ liệu của hệ thống dịch vụ trực tuyến. Đây có phải là giải pháp an toàn và nên sử dụng hay không? Nếu không, hãy trình bày một giải pháp để lưu trữ thông tin mật khẩu đăng nhập của người dùng trong hệ thống dịch vụ trực tuyến.

Họ tên người ra đề-MSCB: Chữ ký: ..... [Trang 1-4]

Họ tên người duyệt đề: Chữ ký:.....

b) **Mã hóa đối xứng**: *(1.0 điểm)*

Giả sử Anh/Chị cần xây dựng chương trình cho phép mã hóa tập tin bằng thuật toán mã hóa đối xứng theo khối (block cipher). Khi cần mã hóa tập tin nào, chương trình sẽ yêu cầu người dùng nhập một đoạn mật khẩu (passphrase) *có độ dài tùy ý*. Chương trình sử dụng passphrase này để phát sinh ra khóa dùng để mã hóa nội dung tập tin được chọn.

Khi cần giải mã tập tin, người dùng lại nhập passphrase (đã dùng khi mã hóa tập tin này). Nếu passphrase chính xác, chương trình sẽ giải mã toàn bộ tập tin, nếu không, chương trình thông báo lỗi.

(b1) Anh/Chị hãy đề xuất một phương án để tạo ra khóa (có kích thước cố định) để mã hóa từ passphrase (có độ dài tùy ý) do người dùng nhập vào *(0.5 điểm)*

(b2) Anh/Chị hãy đề xuất một phương án để có thể kiểm tra tính hợp lệ của passphrase khi giải mã tập tin. *(0.5 điểm)*

Câu 3. Hệ thống hỗ trợ mua hàng trong siêu thị (3.0 điểm)

SmartMarket là hệ thống các siêu thị được triển khai ở nhiều thành phố và nhiều quốc gia trên thế giới. SmartMarket cung cấp tiện ích trên thiết bị di động giúp khách hàng có thể ***tìm thấy các thông tin liên quan đến sản phẩm dựa vào mã vạch của sản phẩm***, ví dụ như thông tin khuyến mãi, ý kiến nhận xét của người mua về sản phẩm. Ngoài ra, tiện ích này còn cho phép người dùng ***chọn sản phẩm và đặt mua hàng qua thiết bị di động***.

Khi bước chân vào siêu thị, thiết bị di động của bạn (C) sẽ tự động kết nối vào máy chủ (S) của siêu thị. Bạn có thể dùng thiết bị di động ***chụp lại mã vạch*** để nhận biết số hiệu sản phẩm. Sau đó, bạn có thể chọn chức năng trên thiết bị di động để ***gửi số hiệu sản phẩm*** lên máy chủ (S) của siêu thị và ***nhận về các thông tin liên quan*** đến sản phẩm này. Ngoài ra, bạn có thể ***đặt mua sản phẩm sản phẩm*** trực tiếp trên thiết bị di động.

Dưới đây là một số vấn đề an toàn thông tin trong hệ thống hỗ trợ mua hàng:

- Do SmartMarket có nhiều siêu thị nên mỗi khi vào một siêu thị cụ thể của SmartMarket, thiết bị di động (C) cần phải đảm bảo mình kết nối đúng với máy chủ (S) của siêu thị này, tránh tình trạng kết nối nhầm vào máy chủ khác (với mục đích cung cấp cho khách hàng những thông tin sai lệch về sản phẩm).
- Máy chủ (S) của mỗi siêu thị cần kiểm tra người dùng có phải là một người dùng hợp lệ đã đăng ký hay không.

- Sau khi thiết lập kết nối và kênh liên lạc an toàn giữa thiết bị di động (C) và máy chủ (S) của siêu thị, mọi thông tin truyền/nhận giữa thiết bị di động (C) và máy chủ (S) đều được bảo mật bằng cách mã hóa (bằng phương pháp mã hóa đối xứng được quy ước sẵn) sử dụng khóa bí mật K được phát sinh và thống nhất sử dụng giữa S và C.

Giải pháp bảo vệ an toàn thông tin trong hệ thống được đề xuất như sau:

- ***Server tại mỗi siêu thị*** có một ***cặp khóa bất đối xứng*** riêng (đã đăng ký cấp chứng nhận số tại CA chung).
- ***Mỗi người dùng*** đều có ***ID riêng*** và một ***khóa bí mật*** K_c đã đăng ký với máy chủ trung tâm của SmartMarket. Khóa bí mật K_C được lưu trữ sẵn trên thiết bị di động (C) của người dùng.
- Server tại mỗi siêu thị có thể tự động kết nối với máy chủ trung tâm của SmartMarket để lấy toàn bộ ***thông tin ID*** và ***khóa bí mật*** K_C của tất cả người dùng đã đăng ký***.***

Giả sử giao thức dùng để khởi tạo kênh liên lạc an toàn như sau:

Bước 1: Máy chủ (S) định kỳ gửi (dạng ***broadcast***) thông điệp ① cho ***tất cả các thiết bị di động*** trong phạm vi của siêu thị.

① = Mời kết nối, Cert(SName, $PublicKey_S$)

Thông điệp ① gồm: ***lời mời kết nối*** và ***giấy chứng nhận còn hợp lệ của máy chủ*** (S). Trong giấy chứng nhận ghi rõ tên của siêu thị và khóa công khai **$PublicKey_S$** của máy chủ (S) tại siêu thị này.

Bước 2: Thiết bị di động (C) khi nhận được thông điệp ① sẽ kiểm tra tính hợp lệ của giấy chứng nhận. Nếu đây là chứng nhận còn hợp lệ, thiết bị di động (C) sẽ gửi thông điệp ② cho máy chủ (S).

② = $E_{PublicKeyS}(ID_C)$

Nội dung thông điệp ② chính là ***định danh*** **ID_C** của người dùng được ***mã hóa bất đối xứng*** bằng ***khóa công khai*** **$PublicKey_S$** của máy chủ (S).

Bước 3: Máy chủ (S) ***kết nối với máy chủ trung tâm*** của hệ thống siêu thị SmartMarket trên ***kênh truyền an toàn*** để kiểm tra ***tính hợp lệ*** của ID_C và nhận về ***khóa bí mật*** **K_C** của người dùng. Sau đó, máy chủ (S) gửi thông điệp ③ về cho thiết bị di động (C)

③ = Hash(①|②|ID_C)

Thông điệp ③ là thông điệp rút gọn (digest message) của thông điệp ①, ② và định danh **ID_C**.

Bước 4: Thiết bị di động (C) gửi thông điệp ④ cho máy chủ (S)

④= Hash(①|②|③)

Thông điệp ④ là thông điệp rút gọn (digest message) thông điệp ①, ② và ③.

Sau khi kết thúc bước 4, toàn bộ thông điệp liên lạc giữa thiết bị di động (C) với máy chủ (S) đều được mã hóa bằng khóa bí mật $\mathbf{K_C}$.

a) Trong giao thức, thiết bị di động (C) không gửi bất kỳ giá trị ngẫu nhiên $\mathbf{Random_C}$ nào cho máy chủ (S). Theo Anh/Chị, điều này có thể dẫn đến nguy cơ làm mất an toàn hệ thống hay không? Nếu có, hãy nêu ra một tình huống có *ý nghĩa thực tế* có thể làm mất an toàn hệ thống . *(1.0 điểm)*

b) Trong giao thức, thiết bị di động (C) có chắc chắn được máy chủ (S) thật sự là chủ sở hữu $\mathbf{PublicKey_S}$ hay không? Vì sao? Nếu không, hãy đề ra 1 giải pháp đơn giản để thiết bị di động (C) kiểm tra được máy chủ (S) thật sự sở hữu $\mathbf{PublicKey_S}$ *(1.0 điểm)*

c) Trong giao thức, máy chủ (S) có thể kiểm tra được thiết bị di động (C) thật sự có định danh là $\mathbf{ID_C}$ hay không? Nếu không, hãy đề ra 1 giải pháp đơn giản để máy chủ (S) đảm bảo đang thật sự liên lạc với thiết bị di động có lưu thông tin định danh $\mathbf{ID_C}$. *(1.0 điểm)*

Câu 4. An toàn thông tin **(2.0+ điểm)**

a) Hãy tự chọn và trình bày 1 vấn đề thực tế trong lĩnh vực an toàn thông tin cho một hệ thống ứng dụng thực tế. Nên chọn một vấn đề mà anh/chị cảm thấy thích thú và tâm đắc nhất và trình bày chi tiết về vấn đề này: ngữ cảnh của vấn đề, những nguy cơ khi vấn đề này xảy ra.

a) Vấn đề anh/chị vừa nêu thuộc về (những) nhóm nào trong những nhóm bài toán sau đây: giữ bí mật nội dung (secrecy), tính toàn vẹn (integrity), xác thực/chứng thực (authentication), chống thoái thác trách nhiệm (non-repudiation), tính riêng tư (privacy), hay nhóm khác?

(1.0 điểm)

b) Hãy trình bày *1 giải pháp khả thi* cho vấn đề mà anh/chị đã chọn. *(1.0 điểm)*

ꕥ HẾT ꕥ