TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN, ĐHQG-HCM

ĐỀ THI KẾT THÚC HỌC PHẦN
Học kỳ II – Năm học 2020-2021

MÃ LƯU TRỮ
(do phòng KT-ĐBCL ghi)

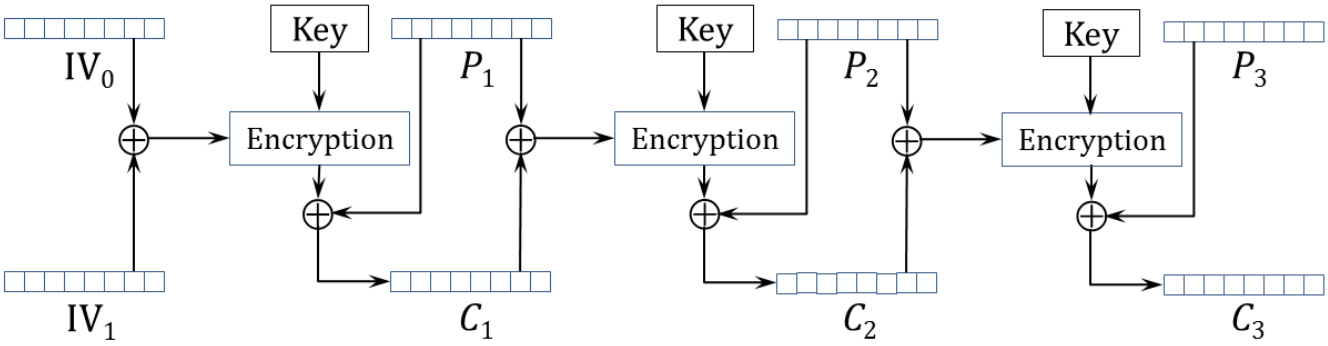
Tên học phần: **Mã hóa thông tin và Ứng dụng** **Mã HP:** _____

Thời gian làm bài: **120 phút** Ngày thi: _____

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:



Ghi chú:

Plaintext (P_i): nội dung trước khi mã hóa $\boldsymbol{P_0 = IV_0, C_0 = IV_1}$

Ciphertext (C_i): nội dung sau khi mã hóa $\boldsymbol{C_i = P_i \oplus E_K(P_{i-1} \oplus C_{i-1})}$

IV_0 và IV_1: initialization vector

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

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

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

Câu 2. Nhà thông minh **(2.0 điểm)**

Trong một căn nhà thông minh có nhiều ***thiết bị*** khác nhau, ví dụ như TV, máy giặt, cửa sổ, tủ lạnh, máy lạnh… Người sử dụng (hợp lệ) có thể dùng ***điện thoại/đồng hồ thông minh*** của mình để điều khiển các thiết bị trong gia đình.

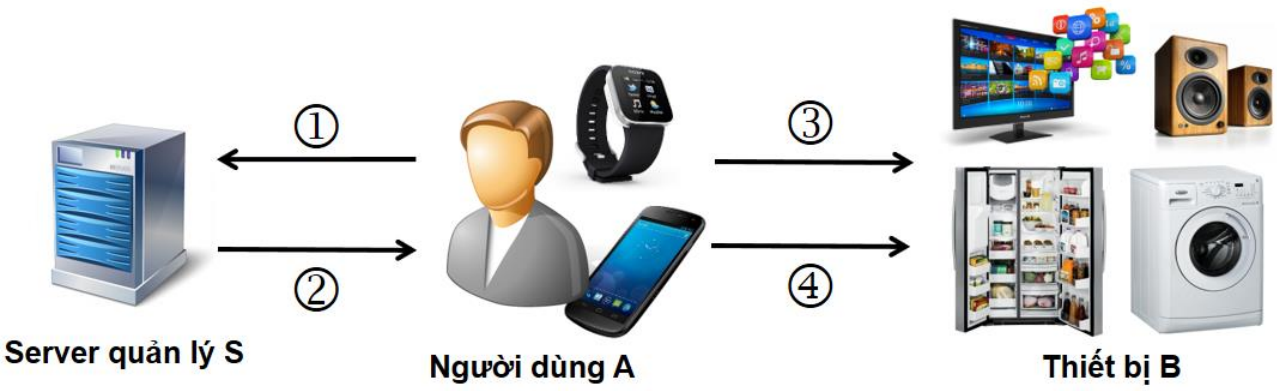
Họ tên người ra đề-MSCB: Chữ ký: ..... [Trang 1-5]

Họ tên người duyệt đề: Chữ ký:.....

TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN, ĐHQG-HCM

ĐỀ THI KẾT THÚC HỌC PHẦN
Học kỳ II – Năm học 2020-2021

MÃ LƯU TRỮ (*do phòng KT-ĐBCL ghi*)



Mô hình hoạt động của căn nhà thông minh như sau:

- Khi **người dùng A** muốn sử dụng hay điều khiển **thiết bị B**, **người dùng** sẽ dùng **điện thoại/đồng hồ thông minh** của mình để gửi cho **server quản lý S** thông điệp ① bao gồm các thông tin: Tên đăng nhập của mình, ID_B của **thiết bị B** mà mình muốn sử dụng.
- **Server quản lý S** tìm trong cơ sở dữ liệu của mình để xác định **khóa bí mật** (secret key) $\mathbf{K_A}$ của **người dùng A** và **khóa bí mật** $\mathbf{K_B}$ của **thiết bị thông minh B**.
- **Server (S)** phát sinh **khóa phiên** (session key) $\mathbf{K_T}$, sau đó gửi lại điện thoại/đồng hồ thông minh của **người dùng A** thông điệp ② bao gồm 2 phần:
  - ***Phần 2a***: Khóa phiên (session key) $\mathbf{K_T}$
  - ***Phần 2b***: Khóa phiên (session key) $\mathbf{K_T}$, tên đăng nhập của **A**, thời gian time-out của phiên làm việc này. Sau thời gian này, **người dùng A** không được phép sử dụng **thiết bị B**. Toàn bộ thông điệp 2b được **mã hóa** bằng **khóa bí mật** $\mathbf{K_B}$ của **thiết bị B**.
- Toàn bộ thông điệp 2 được mã hóa bằng **khóa bí mật** $\mathbf{K_A}$ của **người dùng A.**
- **Người dùng A** dùng điện thoại/đồng hồ thông minh để giải mã thông điệp②, sau đó gửi cho **thiết bị B** thông điệp ③ chính là ***phần 2b*** của thông điệp ②.
- **Thiết bị B** sẽ giải mã thông điệp ③. Dựa vào tên đăng nhập của **người dùng A**, **thiết bị B** sẵn sàng phục vụ theo yêu cầu/điều khiển của **người dùng A**.
- **Người dùng A** dùng điện thoại/đồng hồ thông minh của mình để gửi lệnh điều khiển ④ đến **thiết bị B**. Thông điệp ④ bao gồm tên đăng nhập của A (không được mã hóa) và mã lệnh điều khiển thiết bị (được mã hóa **bằng khóa phiên** $\mathbf{K_T}$).

Họ tên người ra đề-MSCB: Chữ ký: ..... [Trang 2-5]
Họ tên người duyệt đề: Chữ ký:.....

Yêu cầu:

a) Trong giao thức trên, **người dùng A** ***chỉ gửi*** cho **server quản lý S** ***tên đăng nhập*** của mình mà ***không*** gửi kèm theo ***bất kỳ thông tin nào để chứng minh là mình thật sự là người dùng*** **A**. Hãy giải thích vì sao **thiết bị B** có thể tin tưởng để cung cấp chức năng cho **người dùng A**. *(1.0đ)*

b) Trong giao thức trên, nếu **phần 2b của thông điệp** ② **<u>không</u> được** mã hóa **bằng** khóa bí mật K_B **của thiết bị B** thì có thể dẫn đến nguy cơ gì? Trình bày và giải thích nguy cơ này. *(1.0đ)*

Câu 3. Hệ thống TV-on-demand (3.0 điểm)

Dịch vụ TV-on-demand cho phép người dùng có thể chọn xem các chương trình truyền hình theo ý thích của mình vào bất kỳ thời điểm nào. Người dùng được công ty dịch vụ TV-on-demand lắp đặt một **bộ giải mã** (set top box) tại nhà để giúp ***giải mã tín hiệu truyền hình***, đồng thời quản lý việc ***chứng thực*** và ***truy cập dịch vụ***.

Vấn đề an toàn thông tin trong hệ thống dịch vụ TV-on-demand là yếu tố quan trọng:

- **Server** (B) tại trung tâm dịch vụ cần kiểm tra **bộ giải mã** (A) đang muốn kết nối để nhận tín hiệu chương trình truyền hình có phải là một trong những bộ giải mã thật sự trong hệ thống hay không.
- **Bộ giải mã** (A) cần phải kiểm tra có phải đang thật sự kết nối với **Server** (B) tại Trung tâm truyền hình hay không.
- Sau khi thiết lập kênh liên lạc an toàn, mọi thông tin truyền/nhận giữa **Server** (B) và **Bộ giải mã** (A) 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 A và B.

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

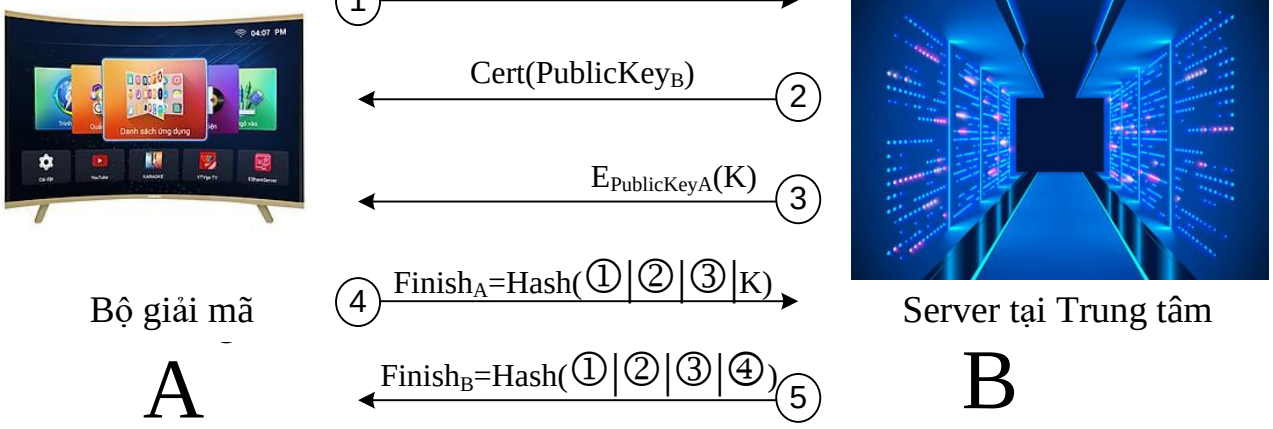
- **Server** tại trung tâm dịch vụ cũng như mỗi **Bộ giải mã** trong hệ thống ***đều có một cặp khóa bất đối xứng của riêng mình*** (đã ***đăng ký cấp chứng nhận số*** tại CA chung).
- Mỗi **Bộ giải mã** trong hệ thống đều có ***ID riêng***.
- **Server** tại trung tâm dịch vụ có toàn bộ ***thông tin ID*** và ***public key*** của **mỗi bộ giải mã** trong hệ thống**.**

TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN, ĐHQG-HCM

ĐỀ THI KẾT THÚC HỌC PHẦN
Học kỳ II – Năm học 2020-2021

MÃ LƯU TRỮ (do phòng KT-ĐBCL ghi)

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



Thông điệp	Ý nghĩa
①	A gửi cho B thông điệp yêu cầu liên lạc, số ngẫu nhiên **Random$_A$**, ID của mình (**ID$_A$**)
②	B gửi cho A chứng nhận khóa công của B (Cert(**PublicKey$_B$**))
③	B phát sinh ngẫu nhiên một khóa bí mật **K** (dùng trong việc mã hóa đối xứng). B tìm trong cơ sở dữ liệu của mình khóa công khai (**PublicKey$_A$**) tương ứng với ID$_A$. Sau đó, B mã hóa nội dung khóa **K** bằng khóa công khai của A (**PublicKey$_A$**) và gửi thông tin khóa **K** (sau khi đã mã hóa) cho A
④	A sử dụng khóa riêng của mình (**PrivateKeyA**) để giải mã nội dung khóa **K**. Sau đó, A gửi thông điệp **Finish$_A$** là thông điệp rút gọn (digest message) của tất cả thông điệp đã trao đổi giữa A và B (gồm thông điệp ①②③) và nội dung khóa **K**
⑤	B gửi thông điệp **Finish$_B$** là thông điệp rút gọn (digest message) của tất cả những thông điệp đã trao đổi giữa A và B (gồm thông điệp ①②③④)

Họ tên người ra đề-MSCB: Chữ ký: ..... [Trang 4-5]

Họ tên người duyệt đề: Chữ ký:.....

a) Trong giao thức, **B** không phát sinh và gửi cho **A** bất kỳ giá trị ngẫu nhiên $\mathbf{Random_B}$ nào. 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 . *(1.0đ)*

b) Trong giao thức, bộ giải mã A có thể kiểm tra được server B ***thật sự sở hữu*** $\mathbf{PublicKey_B}$ và $\mathbf{PrivateKey_B}$ hay không? Vì sao? Nếu không, hãy đề ra 1 giải pháp đơn giản để bộ giải mã A đảm bảo đang thật sự liên lạc với server sở hữu $\mathbf{PublicKey_B}$ và $\mathbf{PrivateKey_B}$. *(1.0đ)*

c) Trong giao thức, server B có thể kiểm tra được bộ giải mã A có phải là **bộ giải mã có ID là $\mathbf{ID_A}$** (một bộ giải mã hợp lệ trong hệ thống) hay không? Vì sao? Nếu không, hãy đề ra 1 giải pháp đơn giản để server B đảm bảo đang thật sự liên lạc với bộ giải mã có ID là $\mathbf{ID_A}$. *(1.0đ)*

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.

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? *(1.0đ)*

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

HẾT