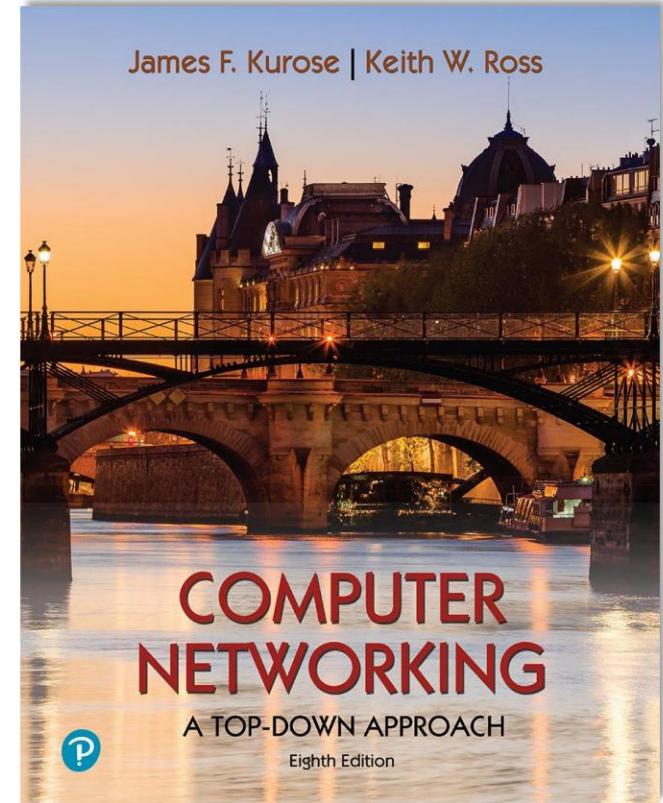


Chương 8

Bảo vệ



Mạng máy tính: A
Cách tiếp cận từ trên xuống
phiên bản thứ 8
Jim KuroseKeith Ross
Pearson, 2020

Bảo mật: tổng quan

Mục tiêu của chương:

hiểu các nguyên tắc của an ninh mạng:

- mã và nhiều công dụng của nó ngoài tính “bảo mật”
- xác thực
- tin nhắn toàn vẹn

an ninh trong thực tế:

- tường lửa và hệ thống phát hiện xâm nhập •

an ninh trong các lớp ứng dụng, truyền tải, mạng, liên kết

đại cương chương 8

An ninh mạng là gì? Nguyên

tắc mật mã Tính toàn vẹn, xác
thực của thông điệp Bảo mật
e-mail Bảo mật kết nối TCP:
TLS Bảo mật lớp mạng: IPsec
Bảo mật trong mạng di động
và không dây Bảo mật vận hành: tường
lửa và IDS



An ninh mạng là gì?

bảo mật: chỉ người gửi, người nhận dự định mới “hiểu” nội dung tin nhắn

- người gửi mã hóa tin nhắn
- người nhận giải mã xác

thực tin nhắn: người gửi, người nhận muốn xác nhận danh tính của nhau khác

tính toàn vẹn của tin nhắn: người gửi, người nhận muốn đảm bảo tin nhắn không bị thay đổi (trong khi truyền hoặc sau đó) mà không bị phát hiện

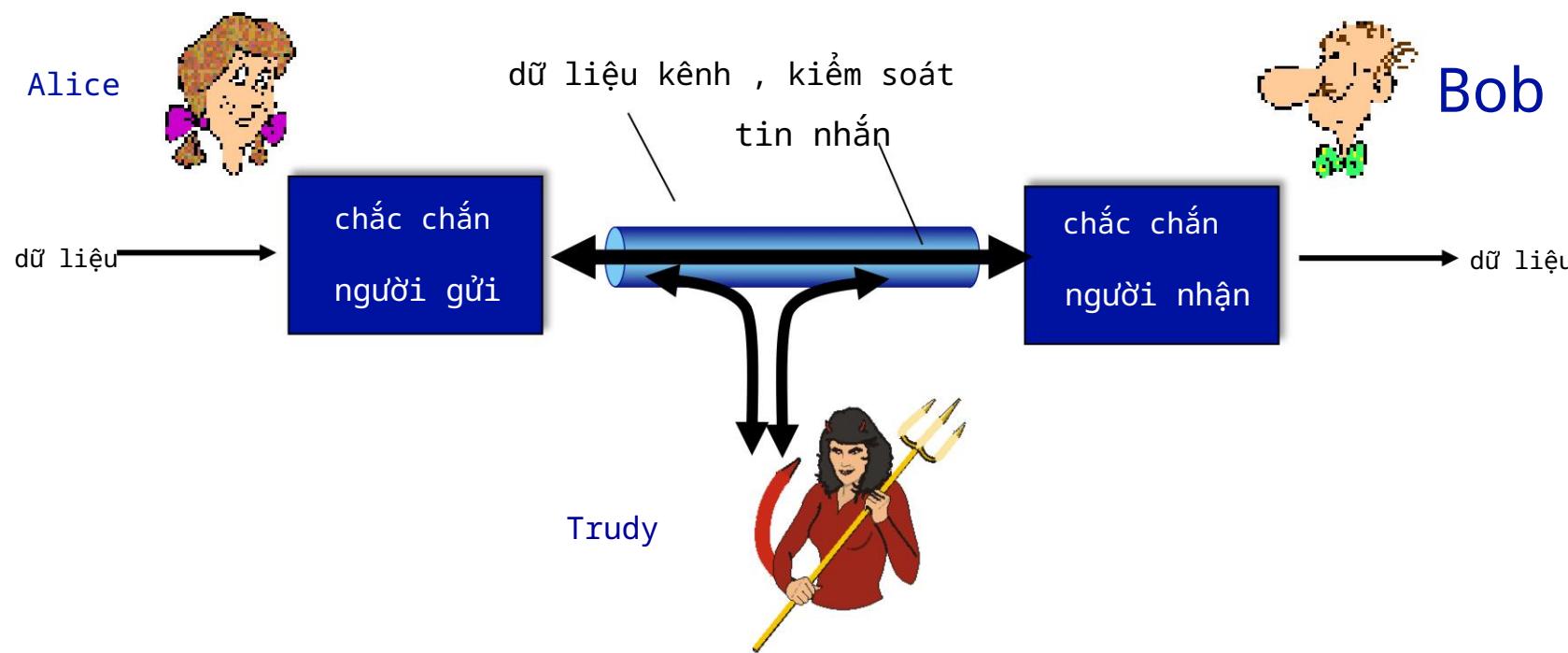
người dùng

Bạn bè và kẻ thù: Alice, Bob, Trudy

nổi tiếng trong giới an ninh mạng

Bob, Alice (đôi tình nhân!) muốn liên lạc “an toàn”

Trudy (kẻ đột nhập) có thể chặn, xóa, thêm tin nhắn



Bạn bè và kẻ thù: Alice, Bob, Trudy

Bob và Alice có thể là ai?

- . chà, Bob và Alice ngoài đời thực !

Trình duyệt web/máy chủ cho các giao dịch điện tử (ví dụ: mua hàng trực tuyến)

Máy khách/máy chủ ngân hàng trực tuyến

Máy chủ DNS

Các bộ định tuyến BGP trao đổi thông tin cập nhật về bảng
định tuyến các ví dụ khác?

Có những kẻ xấu (và cô gái) ngoài kia!

Q: Một "kẻ xấu" có thể làm gì?

Đáp: Rất nhiều! (nhắc lại phần

1.6) • **nghe trộm:** chặn tin nhắn •

chủ động **chèn** tin nhắn vào kết nối • **mạo danh:**

có thể giả mạo (giả mạo) địa chỉ nguồn trong gói (hoặc bất kỳ trường nào
trong gói) • **chiếm quyền điều khiển:** “tiếp quản” kết nối đang diễn ra

bằng cách xóa người gửi hoặc

người nhận, chèn mình vào vị trí

• **từ chối dịch vụ:** ngăn không cho người khác sử dụng dịch vụ (ví dụ: do quá
tải tài nguyên)

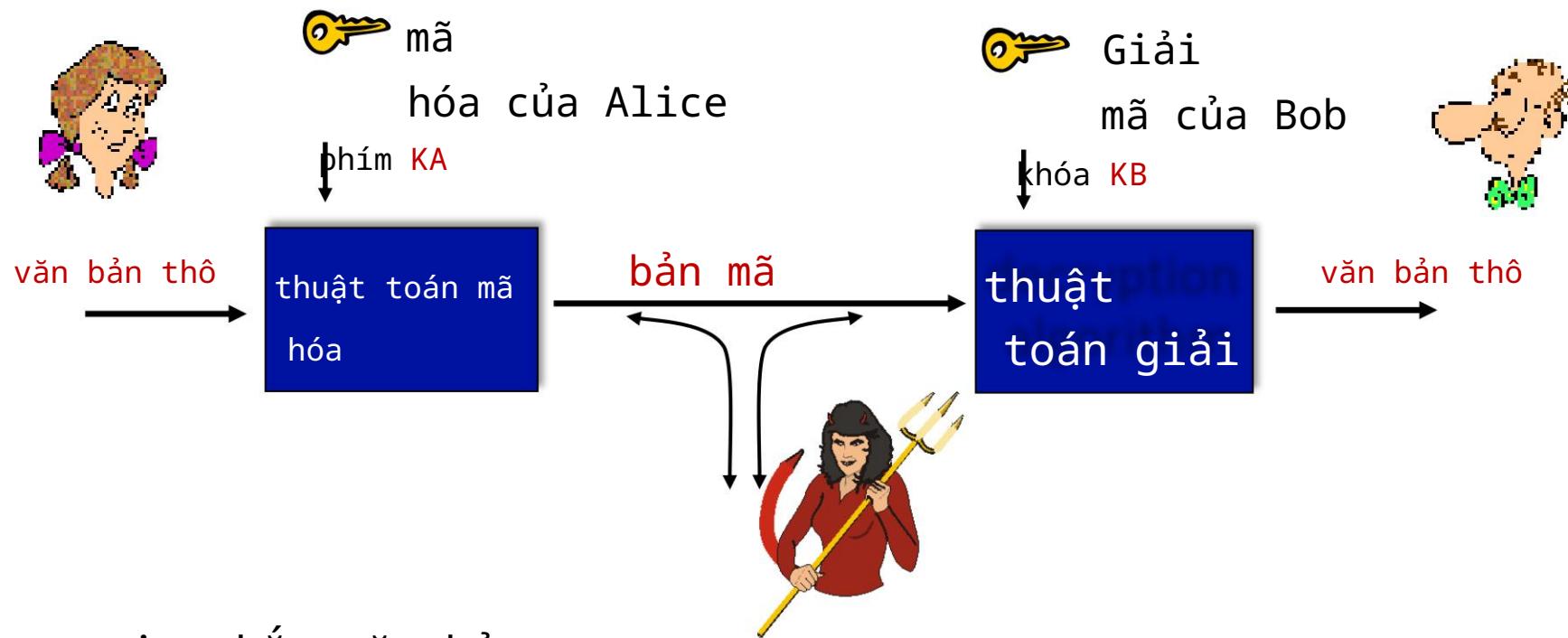
đại cương chương 8

An ninh mạng là gì?

Nguyên tắc mật mã Tính
tòan vẹn, xác thực của thông điệp
Bảo mật e-mail Bảo mật kết
nối TCP: TLS Bảo mật lớp mạng:
IPsec Bảo mật trong mạng di
động và không dây Bảo mật vận hành:
tường lửa và IDS



Ngôn ngữ mật mã



m : tin nhắn văn bản

$KA(m)$: bản mã, được mã hoá bằng khoá KA

$$m = KB(KA(m))$$

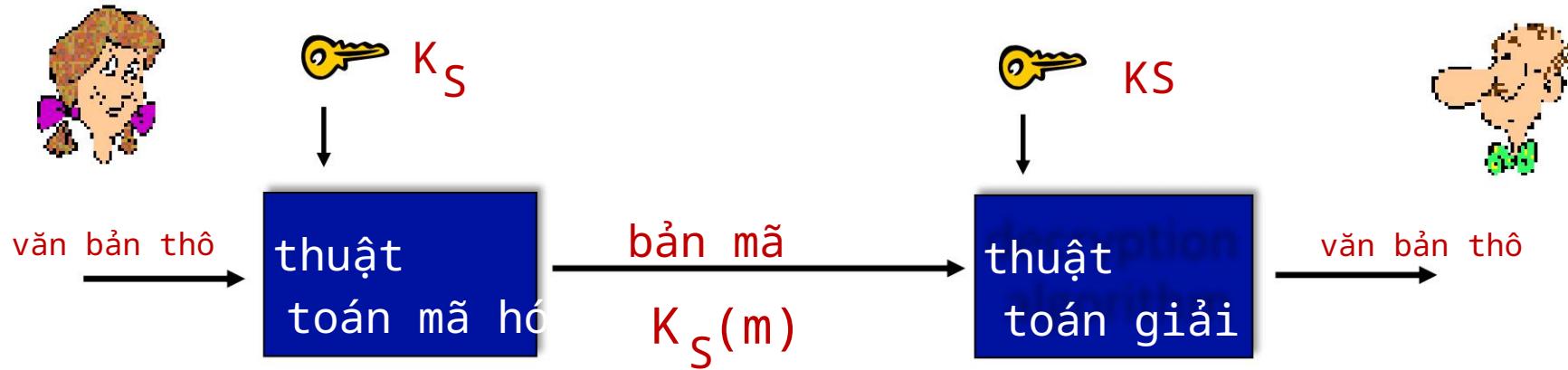
Phá vỡ sơ đồ mã hóa

tấn công chỉ vào văn bản mật mã:
Trudy có bản mã mà cô ấy có thể
phân tích **hai cách tiếp cận:** •

brute force: tìm kiếm qua tất cả
các khóa • phân tích thống kê

tấn công bản rõ đã biết: Trudy
có bản rõ tương ứng với bản mã,
ví dụ: trong mật mã đơn bảng chữ cái,
• Trudy xác định các cặp cho
a,l,i,c,e,b,o, **tấn công bản rõ**
được chọn: Trudy có thể lấy bản mã
cho bản rõ đã chọn

Mật mã khóa đối xứng



mật mã khóa đối xứng: Bob và Alice chia sẻ cùng một khóa (đối xứng): K , ví dụ: khóa biết mẫu thay thế trong mật mã thay thế chữ cái đơn âm

Hỏi: làm thế nào để Bob và Alice đồng ý về giá trị khóa?

Sơ đồ mã hóa đơn giản

mật mã thay thế: thay thế một thứ cho một thứ khác

mật mã một bảng chữ cái: thay thế một chữ cái cho một chữ cái khác

bản rõ: abcdefghijklmnopqrstuvwxyz



bản mã: mnbvcxzasdfghjklpoiuytrewq



ví dụ: Nguyên văn: bob. Tôi mến bạn. bản mã alice :

nkn. s gktc wky. mgsbc



Khóa mã hóa: ánh xạ từ bộ 26 chữ cái sang bộ
26 chữ cái

Một cách tiếp cận mã hóa phức tạp hơn

n mật mã thay thế, M_1, M_2, \dots, M_n Mẫu

quay vòng: ví dụ, $n=4$: M_1, M_3, M_4, M_3, M_2 ;

- M_1, M_3, M_4, M_3, M_2 ; ... Đối với mỗi ký

hiệu văn bản gốc mới, hãy sử dụng mẫu thay thế tiếp theo trong mẫu
tuần hoàn • chó: d từ M_1 , o từ M_3 , g từ M_4

 **Khóa mã hóa:** n mật mã thay thế và mẫu tuần hoàn • khóa
không cần chỉ là mẫu n bit

Mật mã khóa đối xứng: DES

DES: Data Encryption Standard Tiêu chuẩn

mã hóa của Hoa Kỳ [NIST 1993] Khóa đối xứng

56 bit, đầu vào văn bản gốc 64 bit Mật mã khối với
chuỗi khối mật mã DES an toàn đến mức nào?

- Thử thách DES: Giải mã cụm từ được mã hóa bằng khóa 56 bit (brute force) trong vòng chưa đầy một ngày
- không có cuộc tấn công phân tích tốt

nào được biết đến làm cho DES trở nên an

toàn hơn: • 3DES: mã hóa 3 lần bằng 3 khóa khác nhau

AES: Tiêu chuẩn mã hóa nâng cao

Chuẩn NIST khóa đối xứng, thay thế cho DES (tháng 11 năm 2001) xử lý dữ liệu trong các khối 128 bit Khóa 128, 192 hoặc 256 bit Giải mã nhanh (thử từng khóa) mất 1 giây trên DES, mất 149 nghìn tỷ năm đối với AES

Mật mã khóa công khai

mật mã khóa đối xứng: yêu

cầu người gửi, người nhận biết
khóa bí mật dùng chung Hỏi:
làm thế nào để đồng ý về khóa
ngay từ đầu (đặc biệt nếu chưa
bao giờ “gặp mặt”)?

mật mã khóa công khai

cách tiếp cận hoàn toàn khác

[Diffie-Hellman76, RSA78]

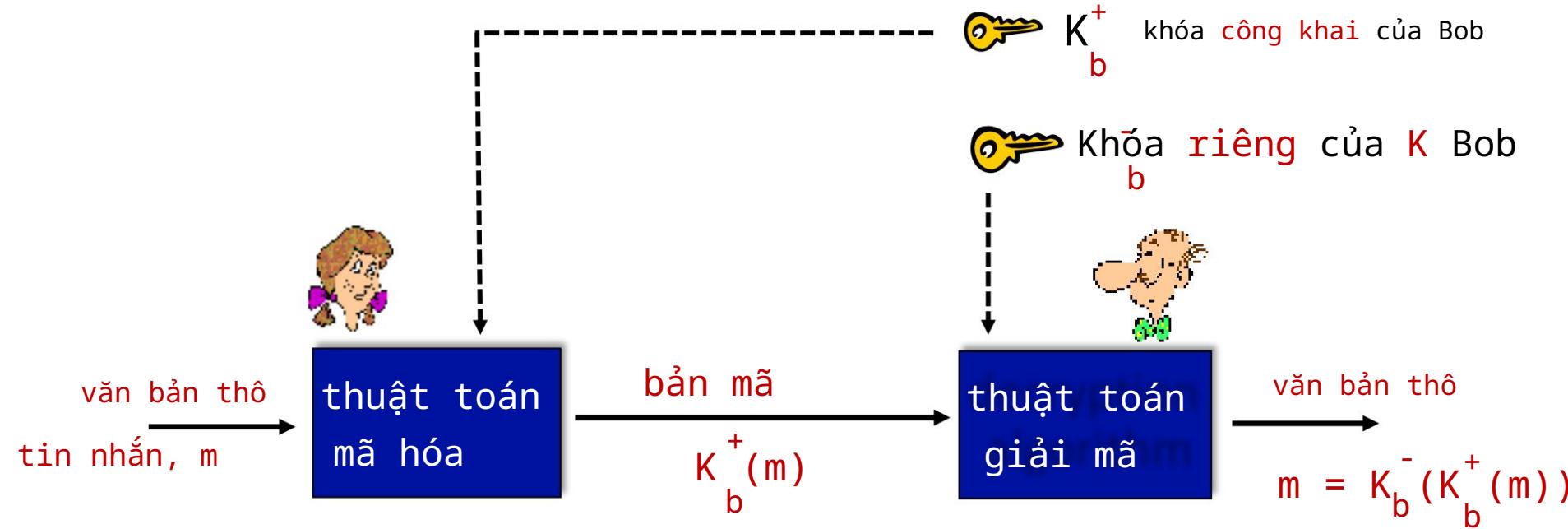
người gửi, người nhận **không**
chia sẻ khóa bí mật

khóa **công khai** mà tất cả mọi người
đều biết

khóa giải mã **riêng** chỉ
người nhận biết



Mật mã khóa công khai



Ồ - mật mã khóa công khai đã cách mạng hóa mật mã 2000 năm tuổi (trước đây chỉ có khóa đối xứng)!

- những ý tưởng tương tự xuất hiện gần như cùng lúc, độc lập ở Hoa Kỳ và Vương quốc Anh (đã được phân loại)

Thuật toán mã hóa khóa công khai

yêu cầu:

1 cần K_b^+ và K_b^- sao cho

$$K_B(K_B(m)) = m$$

2 cung cấp khóa công khai K_b^+ , nó không thể
tính khóa riêng K_b^-

RSA: Thuật toán Rivest, Shamir, Adelson

Điều kiện tiên quyết: số học mô-đun

$x \bmod n$ = phần dư của x khi chia cho n dữ

kiện: $[(a \bmod n) + (b \bmod n)] \bmod n = (a+b) \bmod n$

$[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$

$[(a \bmod n) * (b \bmod n)] \bmod n = (a * b) \bmod n$

do đó

$(a \bmod n)^d \bmod n$ ví dụ: $x=14, d=4 \bmod n$

$n=10, d=2: d \bmod n = 4 \quad 2 \bmod 10$

$6 = 14 \quad 2 = 16$ ($x \bmod n$) $d \bmod 10 =$

$d \times$

RSA: sẵn sàng

thông báo: chỉ là một mô hình nhỏ

mẫu bit có thể được biểu diễn duy nhất bằng một số nguyên do đó, mã hóa một thông điệp tương đương với mã hóa một con số

ví dụ:

$m = 10010001$. Thông báo này được biểu thị duy nhất bằng số thập phân số 145.

để mã hóa m , chúng tôi mã hóa số tương ứng, cho ra một số mới (bản mã).

RSA: Tạo cặp khóa công khai/riêng tư

1. chọn hai số nguyên tố lớn p, q. (ví dụ: 1024 bit mỗi cái)
2. tính $n = pq$, $z = (p-1)(q-1)$
3. Chọn e (với $e < n$) không có ước chung với z (e , z là “nguyên tố cùng nhau”).
4. chọn d sao cho $ed - 1$ chia hết cho z . (nói cách khác: $ed \bmod z = 1$).
5. khóa công khai là $\underbrace{(n, e)}_{\substack{+ \\ KB}}$. khóa riêng là $\underbrace{(n, d)}_{\substack{- \\ KB}}$.

RSA: mã hóa, giải mã

0. đã cho (n, e) và (n, d) như đã tính ở trên

1. để mã hóa tin nhắn $m (< n)$, tính toán

$$e \cdot c = m \bmod n$$

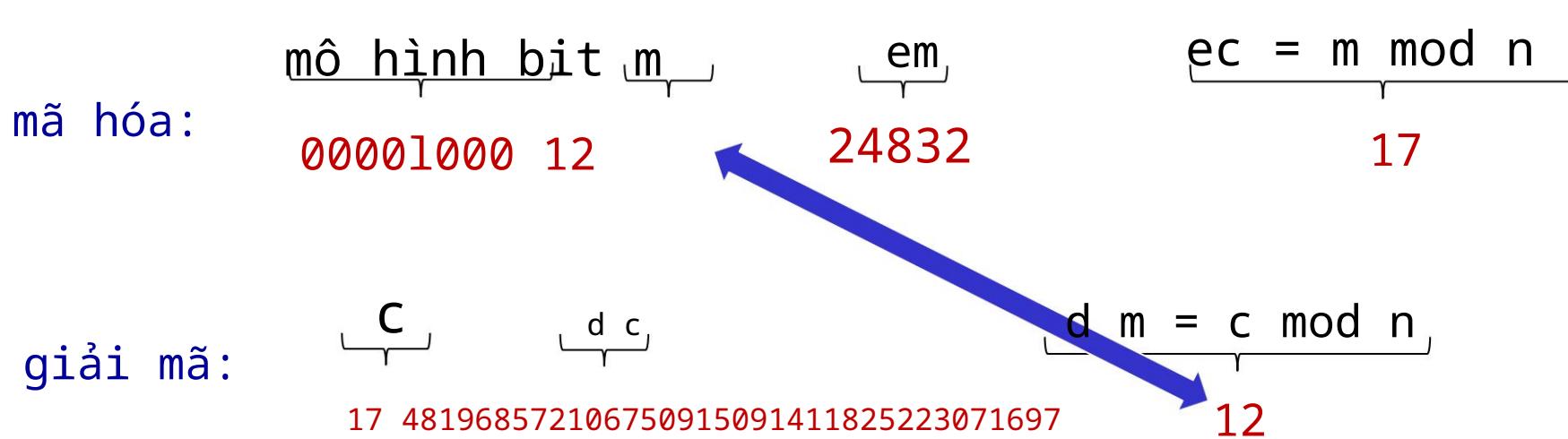
2. để giải mã mẫu bit nhận được, c , tính toán $m = c \bmod n$

Phép thuật xảy ra! $dm = (\underbrace{m^e \bmod n}_c) \bmod n$

Ví dụ RSA:

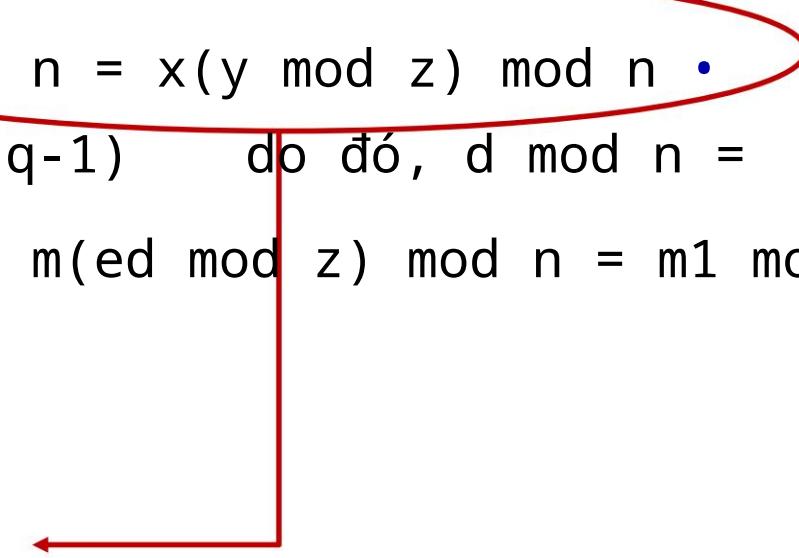
Bob chọn $p=5$, $q=7$. Khi đó $n=35$, $z=24$.

$e=5$ (do đó e , z nguyên tố cùng nhau). $d=29$ (vì vậy $ed-1$ chia hết cho z). Mã hóa tin nhắn 8-bit.



Tại sao RSA hoạt động?

phải chỉ ra rằng $cd \bmod n = m$, trong đó $c = me \bmod n$
thực tế: với mọi x và y : $xy \bmod n = x(y \bmod z) \bmod n$ •
trong đó $n = pq$ và $z = (p-1)(q-1)$ do đó, $d \bmod n =$
 $(me \bmod n)d \bmod n = med \bmod n = m(ed \bmod z) \bmod n = m_1 \bmod$
 c_n



= m

RSA: một thuộc tính quan trọng khác

Thuộc tính sau sẽ rất hữu ích sau này:

$$\underbrace{K^{-}(\overline{k}(m))}_{B\ B} = m = \underbrace{K^{+}(K^{-}(m))}_{BB}$$

sử dụng khóa

chung trước,

sau đó là khóa riêng

sử dụng khóa

riêng trước,

sau đó là khóa chung

kết quả là như nhau!

Tại sao $\bar{K}_B^+(K(m)) = m = K_{BB}^+(K^-(m))$?

theo trực tiếp từ số học mô-đun:

$$\begin{aligned}
 e \bmod n) \quad d \bmod n &= med \bmod n (m \\
 &= mde \bmod n \\
 &= (m d \bmod n) e \bmod n
 \end{aligned}$$

Tại sao RSA lại an toàn?

giả sử bạn biết khóa công khai của Bob (n, e). Làm thế nào là nó khó để xác định d ?

về cơ bản cần tìm thừa số của n mà không cần biết 2 thừa số p và q • thực tế: phân tích số lớn khó

RSA trong thực tế: khóa phiên

phép lũy thừa trong RSA cần nhiều tính toán DES
nhanh hơn RSA ít nhất 100 lần

sử dụng mật mã khóa công khai để thiết lập kết nối an toàn,
sau đó thiết lập khóa thứ hai - khóa phiên đối xứng - để mã
hóa dữ liệu

khóa phiên, KS

Bob và Alice sử dụng RSA để trao đổi khóa phiên đối xứng
KS khi cả hai đều có KS , họ sử dụng mật mã khóa đối xứng

đại cương chương 8

An ninh mạng là gì?

Nguyên tắc mật mã

Xác thực, toàn vẹn thông điệp

Bảo mật e-mail Bảo mật kết nối

TCP: TLS Bảo mật lớp mạng:

IPsec Bảo mật trong mạng di

động và không dây Bảo mật vận hành:

tường lửa và IDS



xác thực

Mục tiêu: Bob muốn Alice “chứng minh” danh tính của mình với
anh ta Giao thức ap1.0: Alice nói “Tôi là Alice”

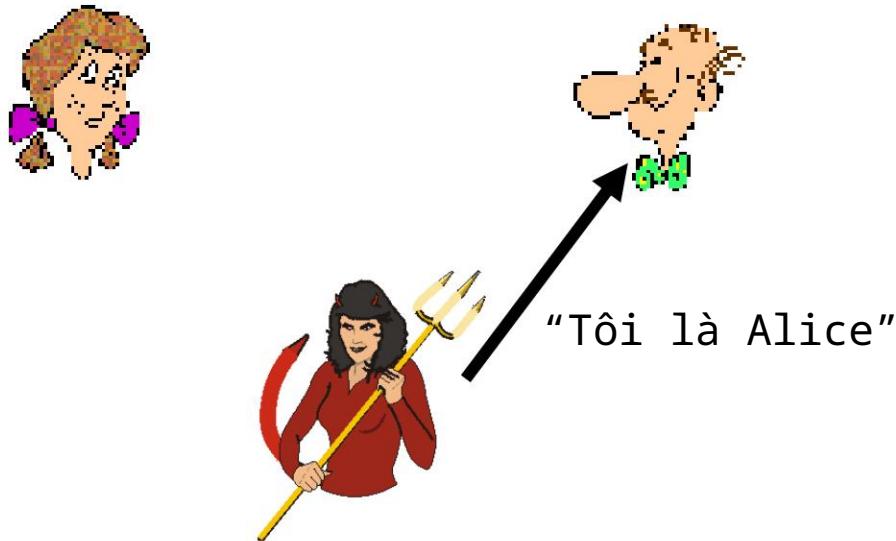


kịch bản thất bại??



xác thực

Mục tiêu: Bob muốn Alice “chứng minh” danh tính của mình với anh ta Giao thức ap1.0: Alice nói “Tôi là Alice”



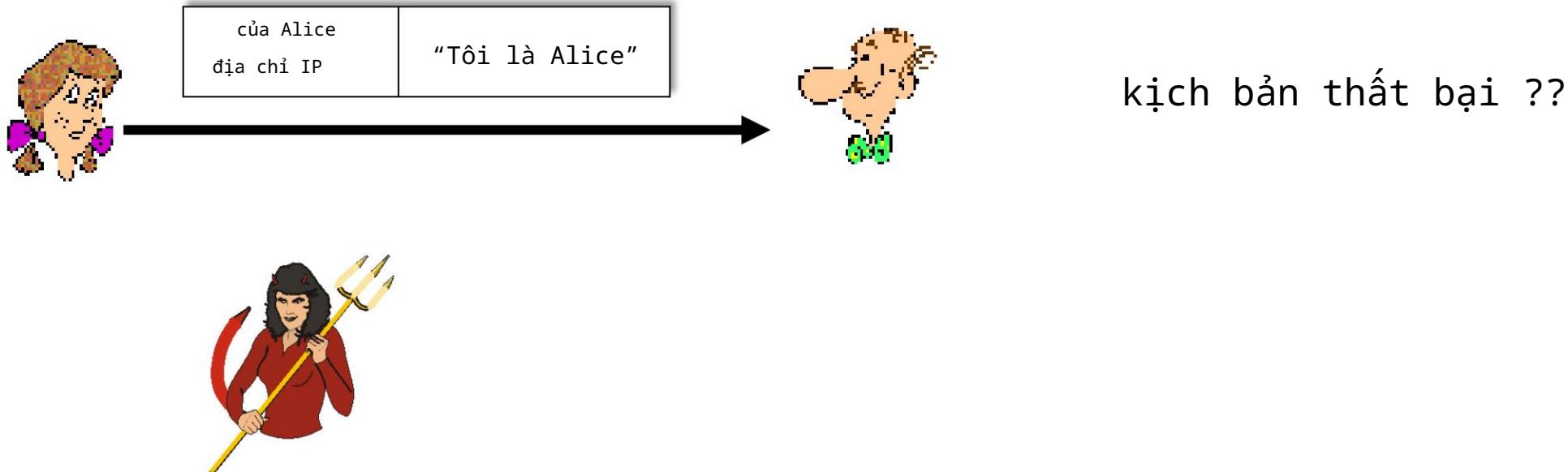
trong một mạng, Bob
không thể “thấy”
Alice, vì vậy
Trudy chỉ đơn
giản tuyên bố mình là Alice



Xác thực: lần thử khác

Mục tiêu: Bob muốn Alice “chứng minh” danh tính của cô ấy với anh ta

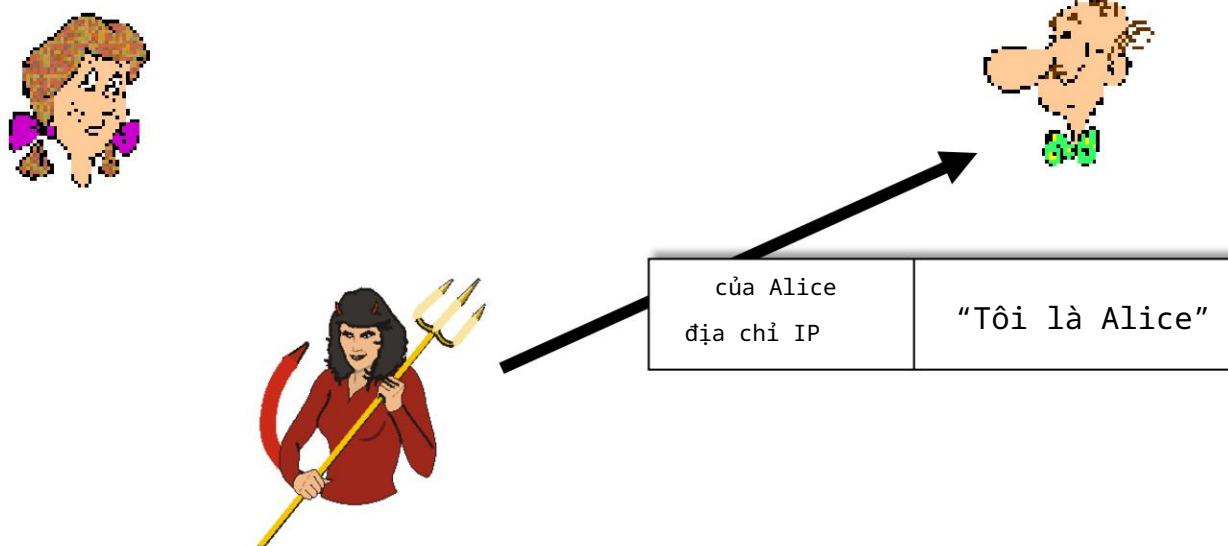
Giao thức ap2.0: Alice nói “Tôi là Alice” trong gói IP chứa địa chỉ IP nguồn của cô ấy



Xác thực: lần thử khác

Mục tiêu: Bob muốn Alice “chứng minh” danh tính của cô ấy với anh ấy

Giao thức ap2.0: Alice nói “Tôi là Alice” trong gói IP chứa địa chỉ IP nguồn của cô ấy

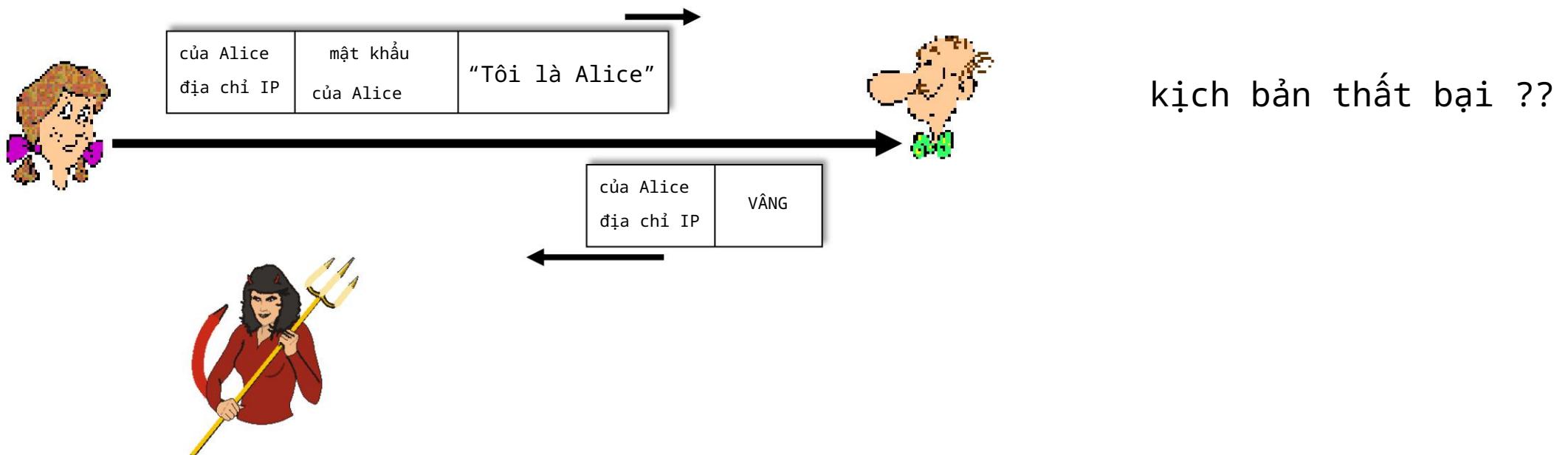


Trudy có thể tạo
một gói “giả mạo”
địa chỉ Alice

Xác thực: lần thử thứ ba

Mục tiêu: Bob muốn Alice “chứng minh” danh tính của cô ấy với anh ta

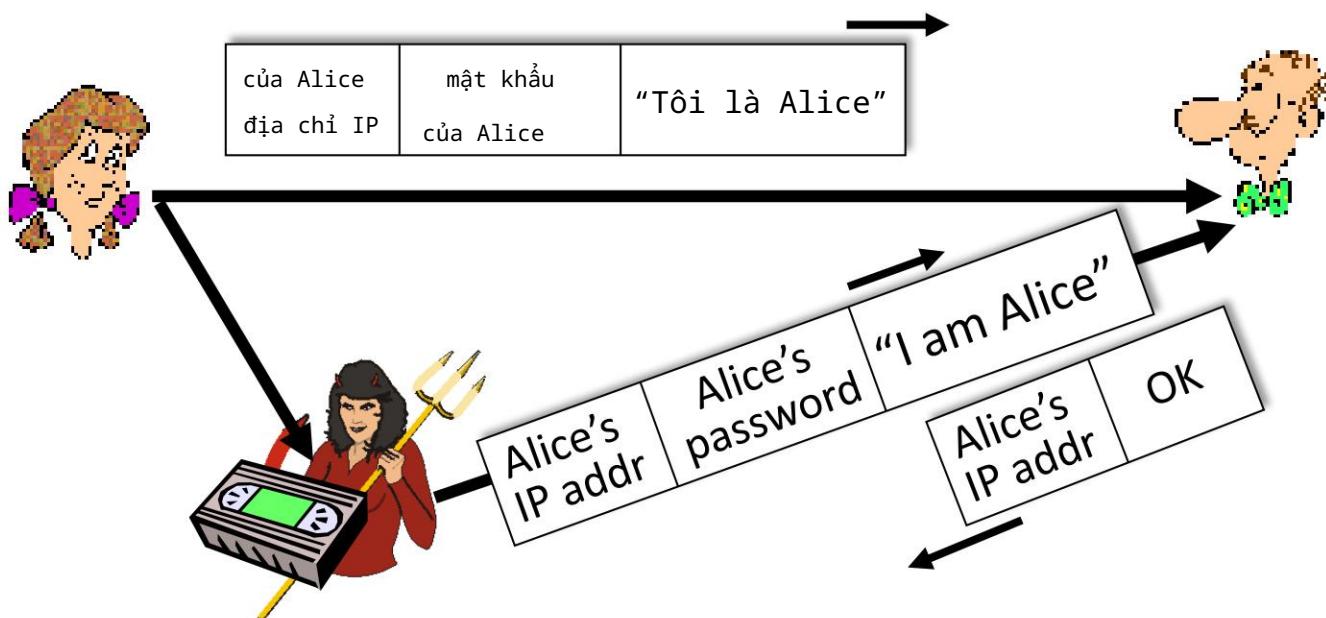
Giao thức ap3.0: Alice nói “Tôi là Alice” Alice nói “Tôi là Alice” và gửi mật khẩu bí mật của mình để “chứng minh” điều đó.



Xác thực: lần thử thứ ba

Mục tiêu: Bob muốn Alice “chứng minh” danh tính của cô ấy với anh ấy

Giao thức ap3.0: Alice nói “Tôi là Alice” Alice nói “Tôi là Alice” và gửi mật khẩu bí mật của mình để “chứng minh” điều đó.

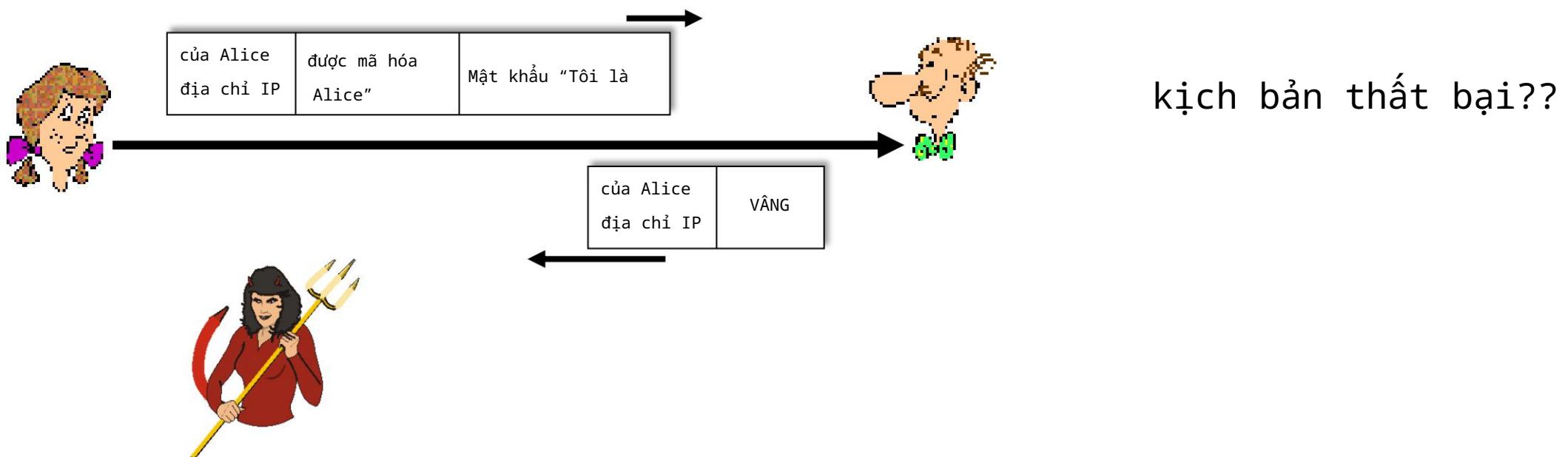


tấn công phát lại:
hồ sơ trudy
Gói của Alice
và sau đó
phát lại cho Bob

Xác thực: lần thử thứ ba đã sửa đổi

Mục tiêu: Bob muốn Alice “chứng minh” danh tính của cô ấy với anh ta

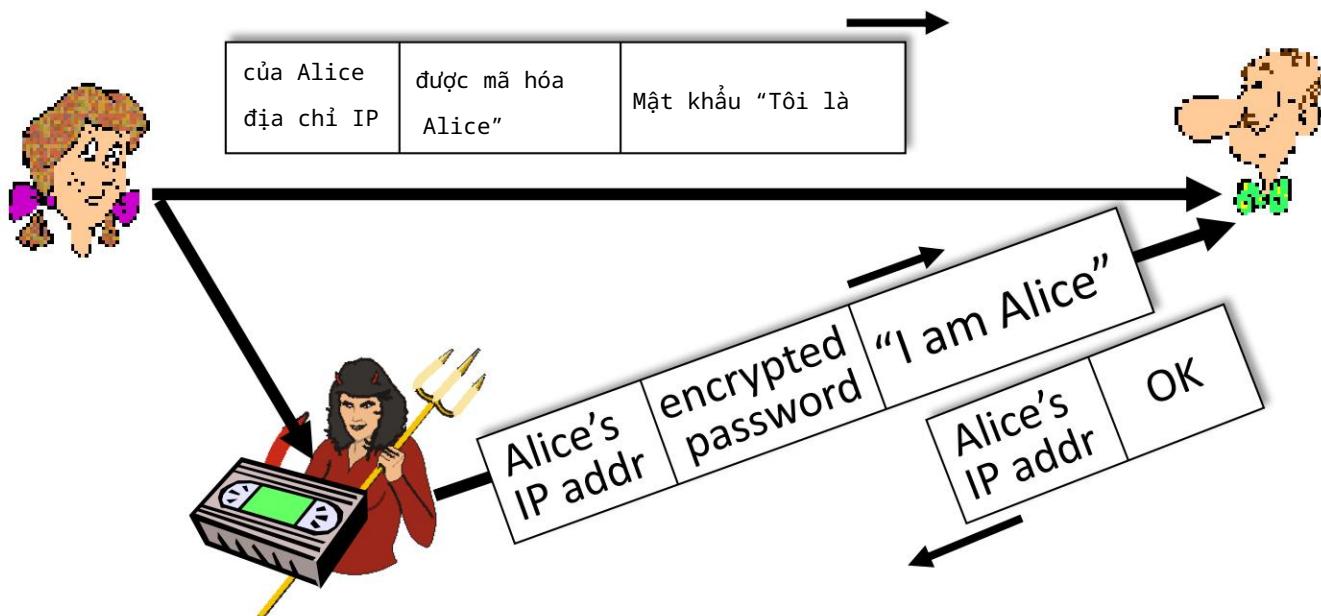
Giao thức ap3.0: Alice nói “Tôi là Alice” Alice nói “Tôi là Alice” và gửi mật khẩu bí mật được mã hóa của cô ấy để “chứng minh” điều đó.



Xác thực: lần thử thứ ba đã sửa đổi

Mục tiêu: Bob muốn Alice “chứng minh” danh tính của cô ấy với anh ấy

Giao thức ap3.0: Alice nói “Tôi là Alice” Alice nói “Tôi là Alice” và gửi mật khẩu bí mật được mã hóa của cô ấy để “chứng minh” điều đó.



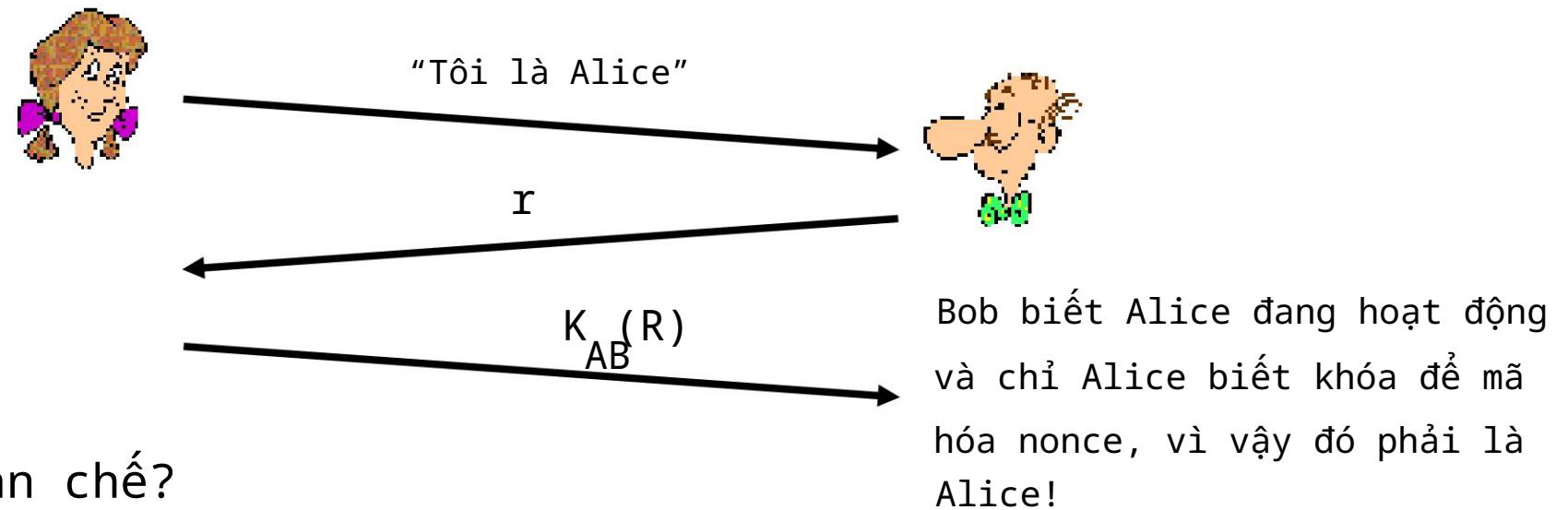
cuộc tấn công phát lại
vấn hoạt động: Hồ sơ Trudy
Gói của Alice
và sau đó phát lại
cho Bob

Xác thực: lần thử thứ tư

Mục tiêu: tránh tấn công phát

lại nonce: số (R) chỉ được sử dụng **một lần trong đời**

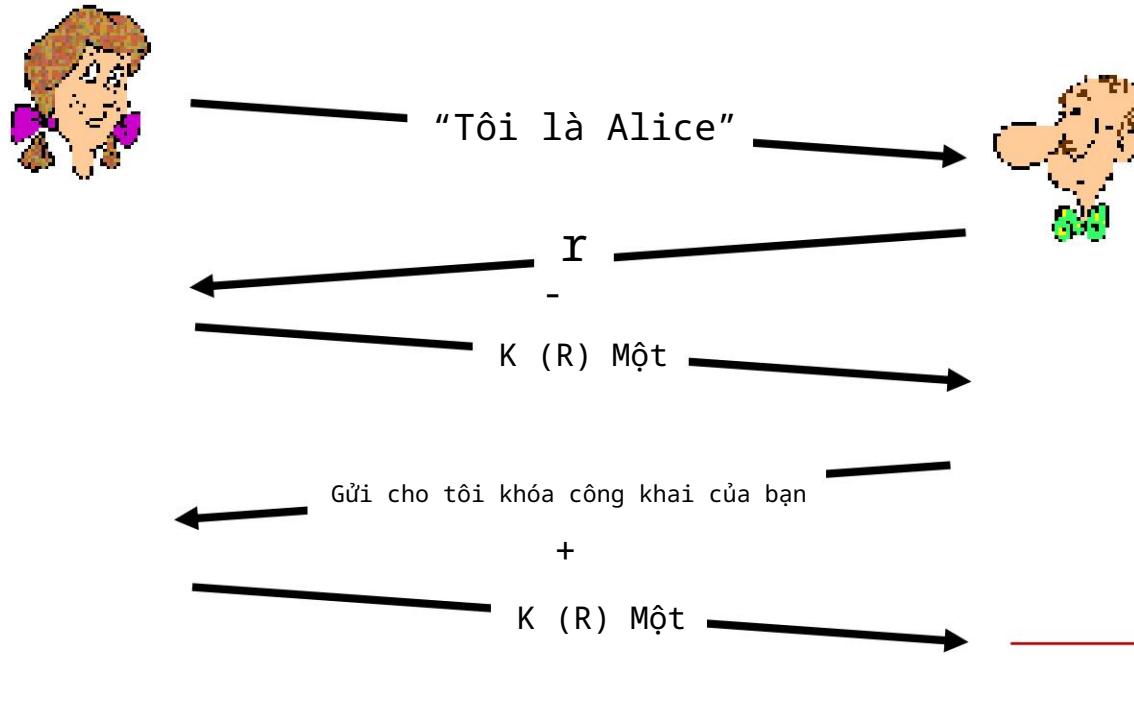
giao thức ap4.0: để chứng minh Alice “sống”, Bob gửi Alice nonce, R
 Alice phải trả lại R, được mã hóa bằng khóa bí mật dùng chung



Xác thực: ap5.0 ap4.0 yêu cầu

khóa đối xứng dùng chung - chúng tôi có thể xác thực bằng các kỹ thuật khóa chung không?

ap5.0: sử dụng nonce, mật mã khóa công khai



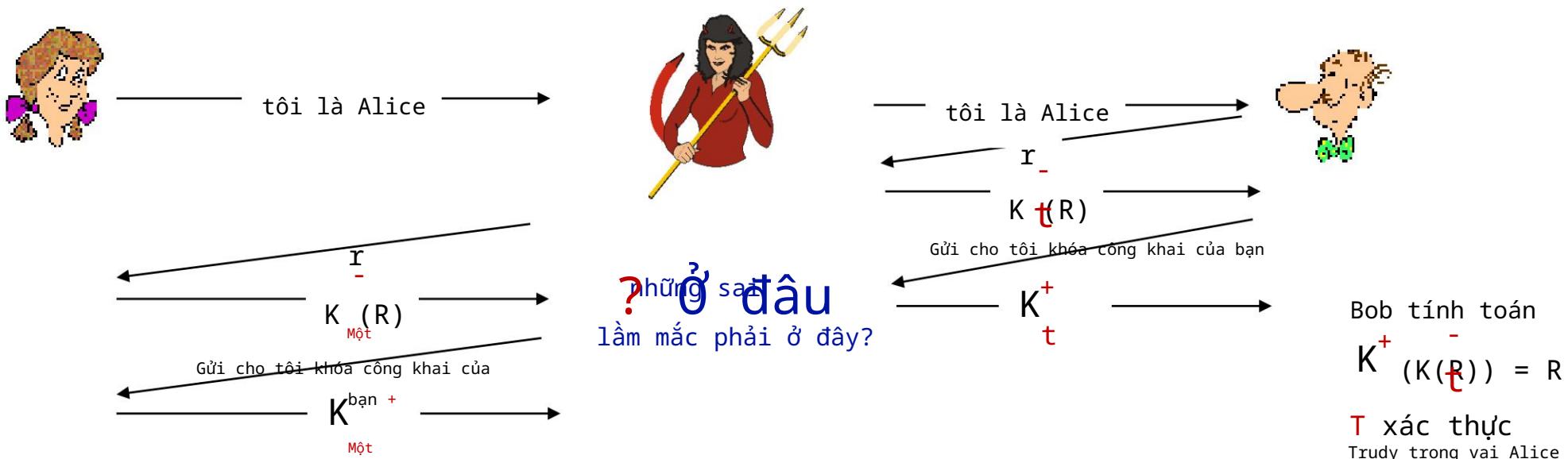
$$\begin{array}{c} \text{Bob tính toán} \\ + \\ K_{\text{Một}} (K(R)) = R \\ \hline \end{array}$$

và biết rằng chỉ Alice mới
có thể có khóa riêng, mã
hóa R đó sao cho

$$\begin{array}{c} + \\ K_{\text{Một}} (K(R)) = R \\ \hline \end{array}$$

Xác thực: ap5.0 - vẫn còn một lỗ hổng!

người đàn ông (hoặc phụ nữ) ở giữa cuộc tấn công: Trudy đóng vai Alice (với Bob) và Bob (với Alice)



Trudy phục hồi m của Bob:

$$m = K_{t}(K_{b}(m)) \xleftarrow{K_{M}(m)}$$

A và cô ấy và Bob gặp nhau
một tuần sau đó và thảo luận
về m , không biết Trudy biết m

Trudy phục hồi m :

$$m = K_{t}(K_{b}(m))$$

T gửi m cho Alice
được mã hóa bằng
Khóa công khai của Alice

$$\xleftarrow{K_{t}(m)}$$

Bob gửi một tin nhắn
cá nhân, m tới Alice

đại cương chương 8

An ninh mạng là gì?

Nguyên tắc mã hóa

Xác thực, toàn vẹn thông điệp

Bảo mật e-mail Bảo mật kết nối

TCP: TLS Bảo mật lớp mạng:

IPsec Bảo mật trong mạng di

động và không dây Bảo mật vận hành:

tường lửa và IDS

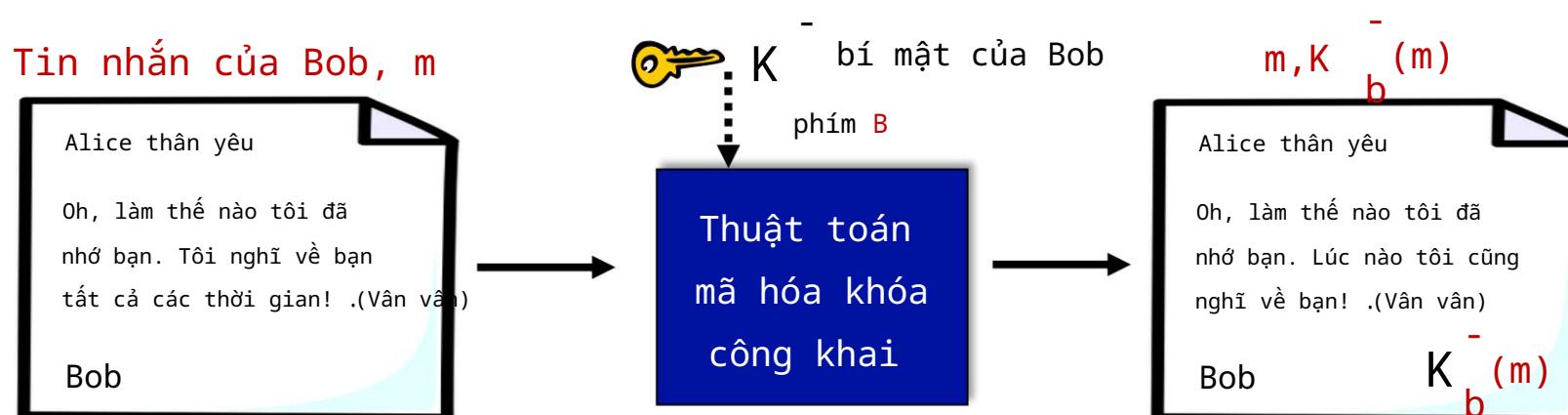


Chữ ký số

kỹ thuật mã tương tự như chữ ký viết tay: người gửi (Bob) ký điện tử vào tài liệu: anh ta là chủ sở hữu/người tạo tài liệu. có thể kiểm chứng, không thể giả mạo: người nhận (Alice) có thể chứng minh với ai đó rằng Bob và không ai khác (kể cả Alice) phải ký vào tài liệu

chữ ký số đơn giản cho tin nhắn m :

Bob ký m bằng cách mã hóa bằng khóa riêng K_B , tạo tin nhắn “đã ký”, $K_B^{-1}(m)$



Chữ ký số

giả sử Alice nhận được tin nhắn m , với chữ ký: $m, KB(m)$

Alice xác minh m được ký bởi Bob bằng cách áp dụng khóa công khai KB của Bob cho $KB(m)$
sau đó kiểm tra $KB(KB(m)) = m$.

Nếu $KB(KB(m)) = m$, người ký m phải sử dụng khóa bí mật của Bob

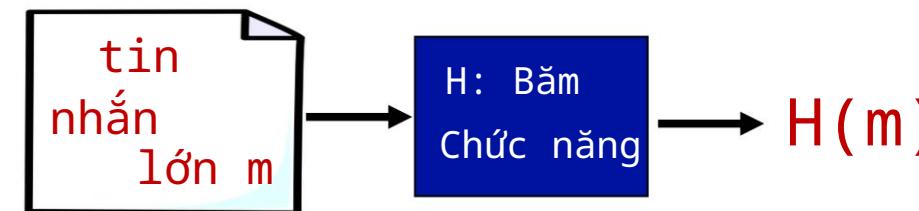
Do đó, Alice xác minh rằng:

Bob đã ký m không ai
khác ký m Bob đã ký m chứ
không phải m' không từ chối:

Alice có thể đưa m và chữ ký $KB(m)$
ra tòa và chứng minh rằng Bob
đã ký m

Thông báo tóm tắt

Đắt về mặt tính toán đối với các thông điệp dài mã hóa bằng khóa công khai **Mục tiêu**: “dấu vân tay” kỹ thuật số có độ dài cố định, dễ tính toán áp dụng hàm băm H cho m , nhận bản tóm tắt thông báo có kích thước cố định, $H(m)$



Các thuộc tính của hàm băm:

nhiều-to-1 tạo thông báo tóm tắt kích thước cố định (dấu vân tay) thông báo tóm tắt x đã cho, không thể tính toán để tìm m sao cho $x = H(m)$

Tổng kiểm tra Internet: hàm băm tiền điện tử kém

Tổng kiểm tra Internet có một số thuộc tính của hàm băm:
 tạo thông báo có độ dài cố định (tổng 16 bit) của thông báo
 là nhiều-một

nhưng thông báo đã cho với giá trị băm đã cho, thật dễ dàng tìm thấy một
 thông báo khác có cùng giá trị băm:

tin nhắn định dạng ASCII

I0U 1 49 4F 5530130 2E .
 39 9 B0B 39 42 D2 42

tin nhắn định dạng ASCII

I0U 9 49 4F 5530930 2E .
 31 9 B0B 39 42 D2 42

B2 C1 D2 AC

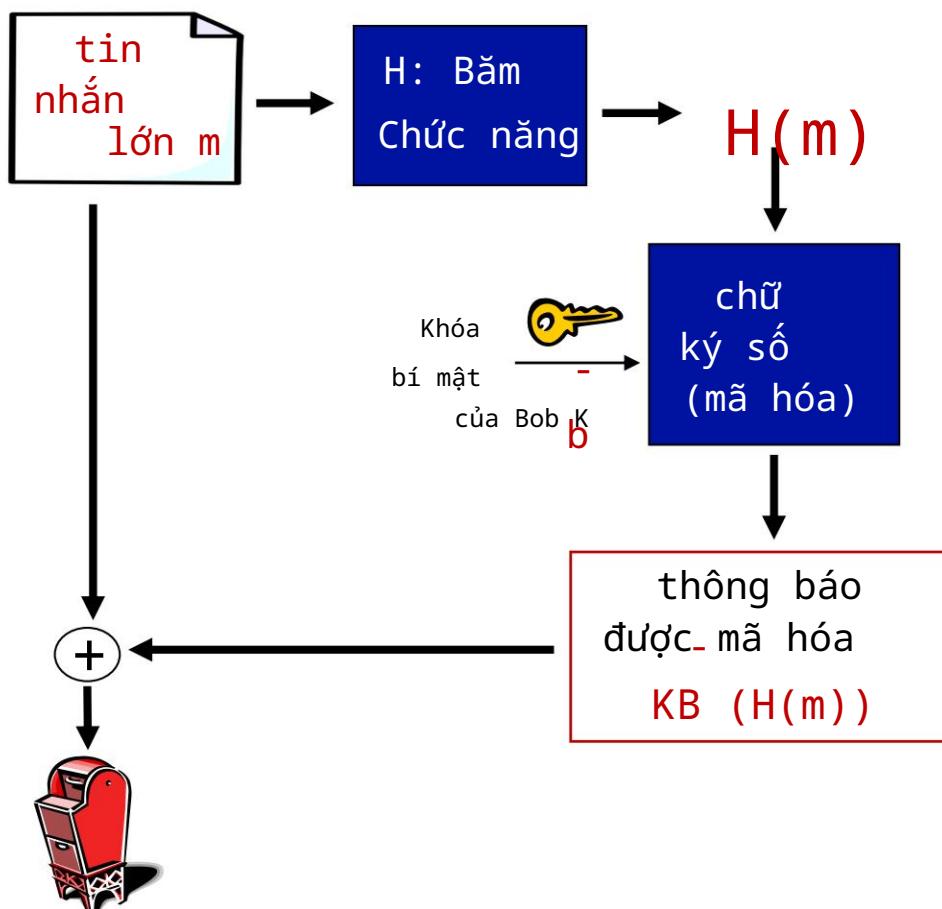
— tin nhắn khác nhau

B2 C1 D2 AC

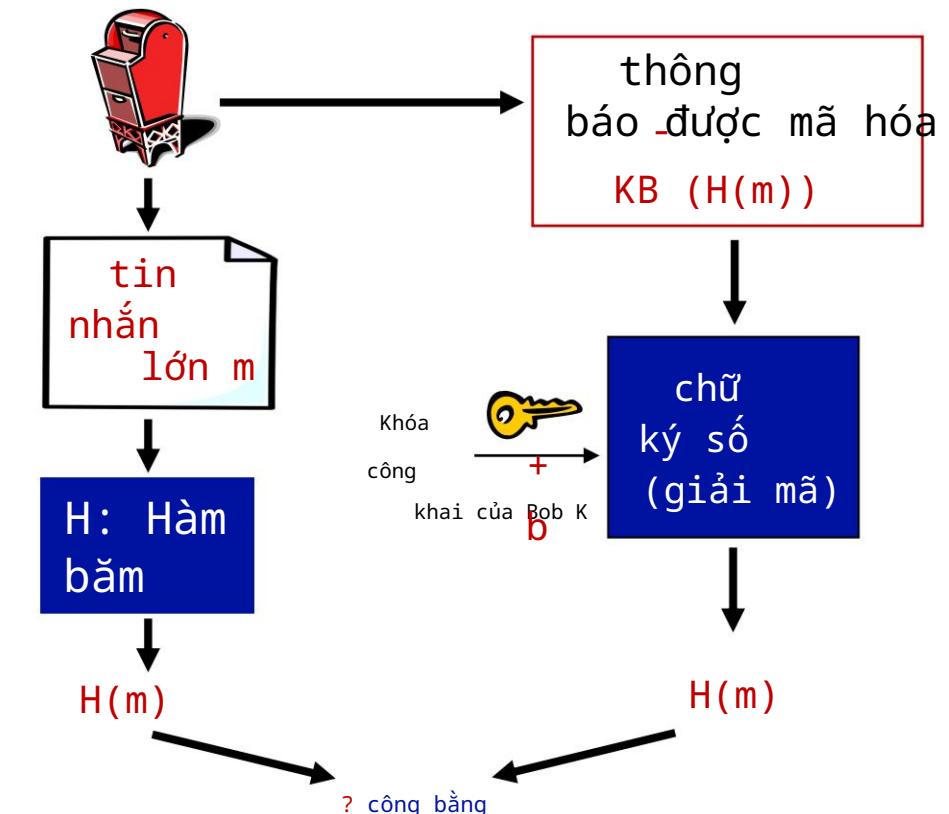
nhưng tổng kiểm tra giống hệt nhau!

Chữ ký số = bản tóm tắt thông báo đã ký

Bob gửi tin nhắn được ký điện tử:



Alice xác minh chữ ký, tính toán vẹn của tin nhắn được ký điện tử:



Thuật toán hàm băm

Hàm băm MD5 được sử dụng rộng rãi (RFC 1321)

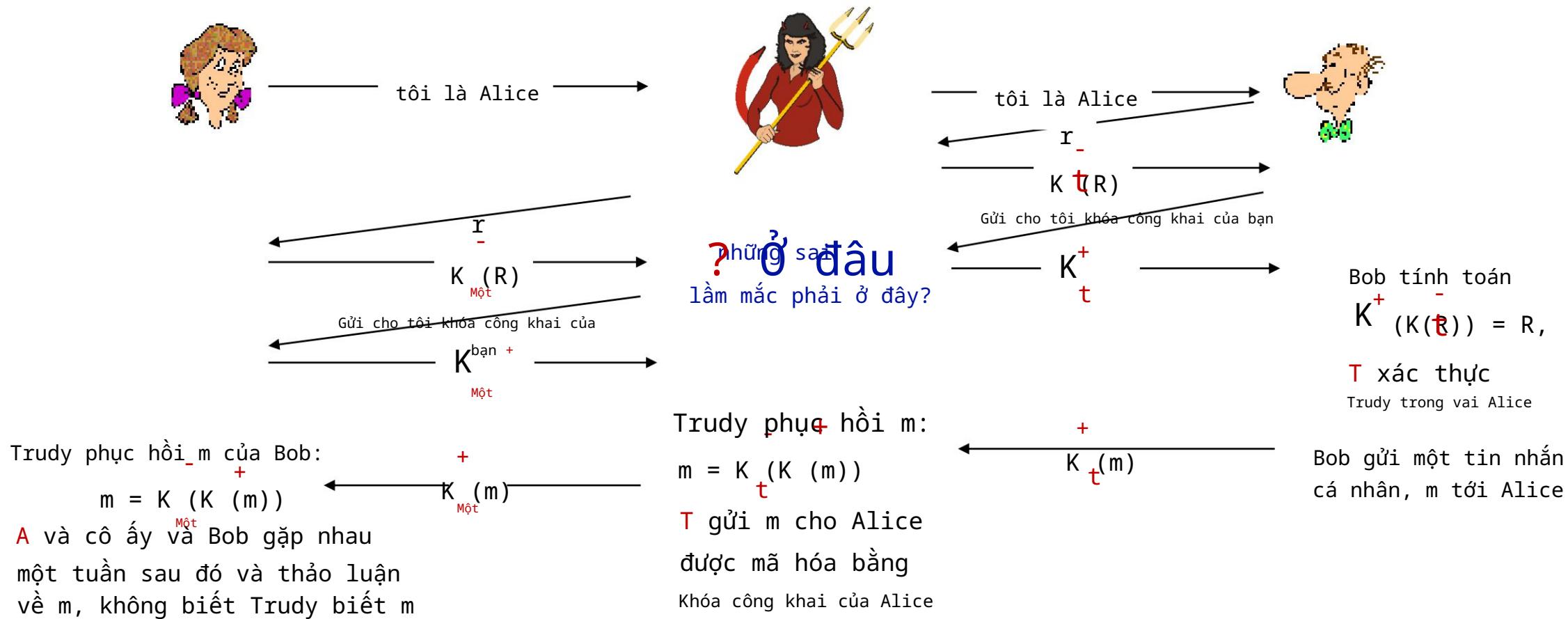
- tính toán thông báo 128-bit thông báo trong quy trình 4 bước.
- chuỗi 128-bit tùy ý x , có vẻ khó xây dựng thông điệp m có hàm băm MD5 bằng x

SHA-1 cũng được sử dụng

- Tiêu chuẩn Hoa Kỳ [NIST, FIPS PUB 180-1]
- Thông báo tóm tắt 160 bit

Xác thực: ap5.0 - hãy sửa nó!!

Nhắc lại vấn đề: Trudy đóng vai Alice (với Bob) và Bob (với Alice)



Cần khóa công khai được chứng nhận

động lực: Trudy chơi khăm Bob chơi pizza

- Trudy tạo đơn đặt hàng qua e-mail:

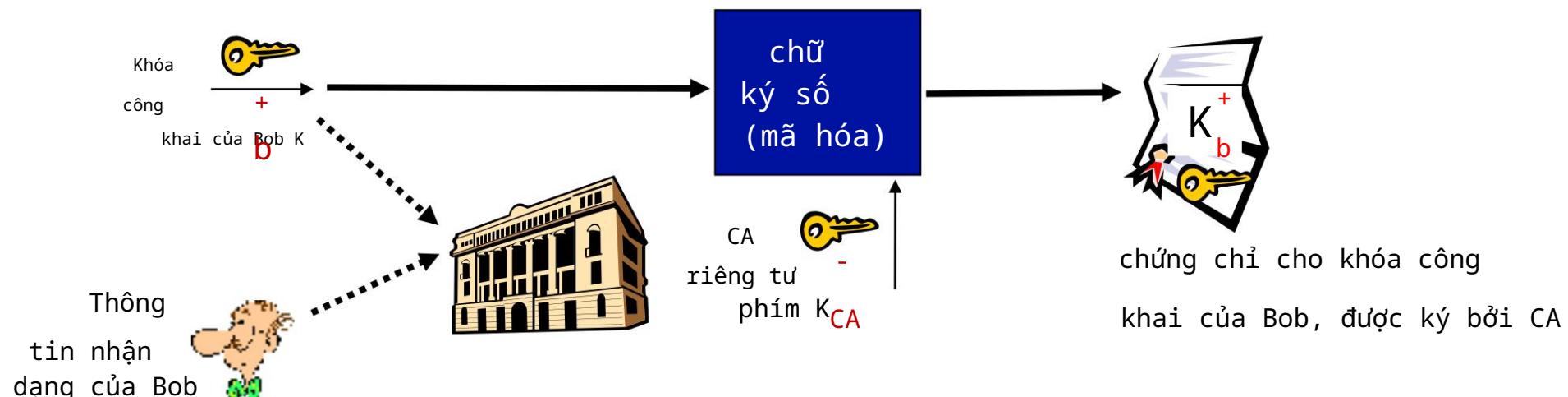
Cửa hàng Pizza thân mến, Vui lòng giao cho tôi
bốn chiếc pizza xúc xích Ý. Cảm ơn bạn, Bob •
Trudy ký đơn đặt hàng bằng khóa riêng của cô ấy •
Trudy gửi đơn đặt hàng đến Cửa hàng Pizza • Trudy
gửi đến Cửa hàng Pizza khóa công khai của cô ấy, nhưng
nói rằng đó là khóa công khai của Bob • Cửa hàng
Pizza xác minh chữ ký; sau đó giao bốn chiếc bánh
pizza pepperoni cho Bob
- Bob thậm chí không thích xúc xích cay



Cơ quan chứng nhận khóa công khai (CA)

cơ quan cấp chứng chỉ (CA): liên kết khóa chung với thực thể cụ thể, E thực thể (người, trang web, bộ định tuyến) đăng ký khóa chung của nó với CE cung cấp “bằng chứng nhận dạng” cho CA • CA tạo chứng chỉ ràng buộc nhận dạng E với khóa chung của E • chứng chỉ chứa khóa công khai của E được ký điện tử bởi CA: CA cho biết “đây là của E

khóa công khai"

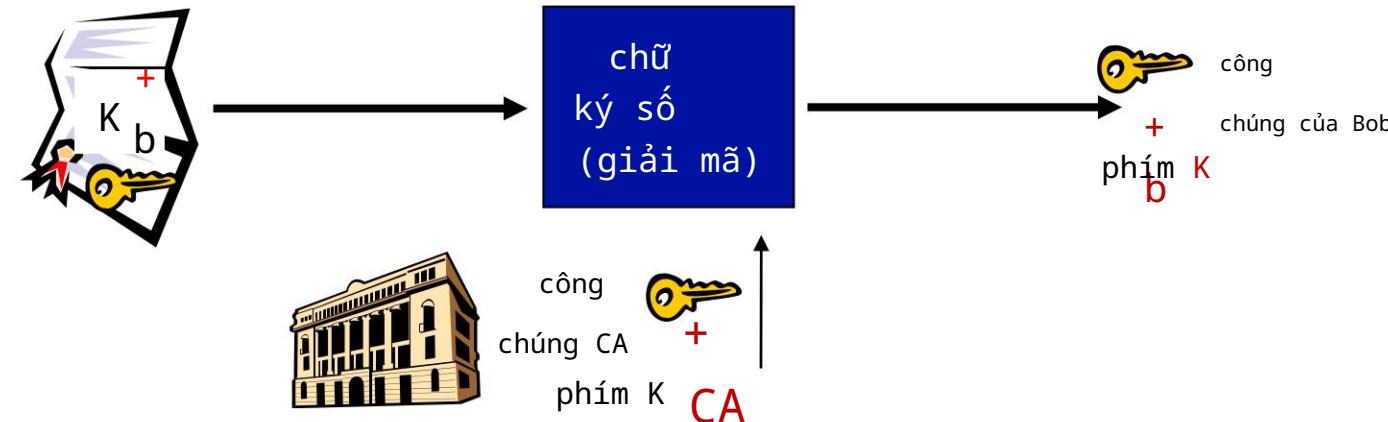


Cơ quan chứng nhận khóa công khai (CA)

khi Alice muốn khóa công khai của Bob:

- lấy chứng chỉ của Bob (Bob hoặc nơi khác) •

áp dụng khóa chung của CA cho chứng chỉ của Bob, lấy khóa chung của Bob



đại cương chương 8

An ninh mạng là gì?

Nguyên tắc mật mã

Xác thực, toàn vẹn thông điệp

Bảo mật e-mail Bảo mật kết nối

TCP: TLS Bảo mật lớp mạng:

IPsec Bảo mật trong mạng di

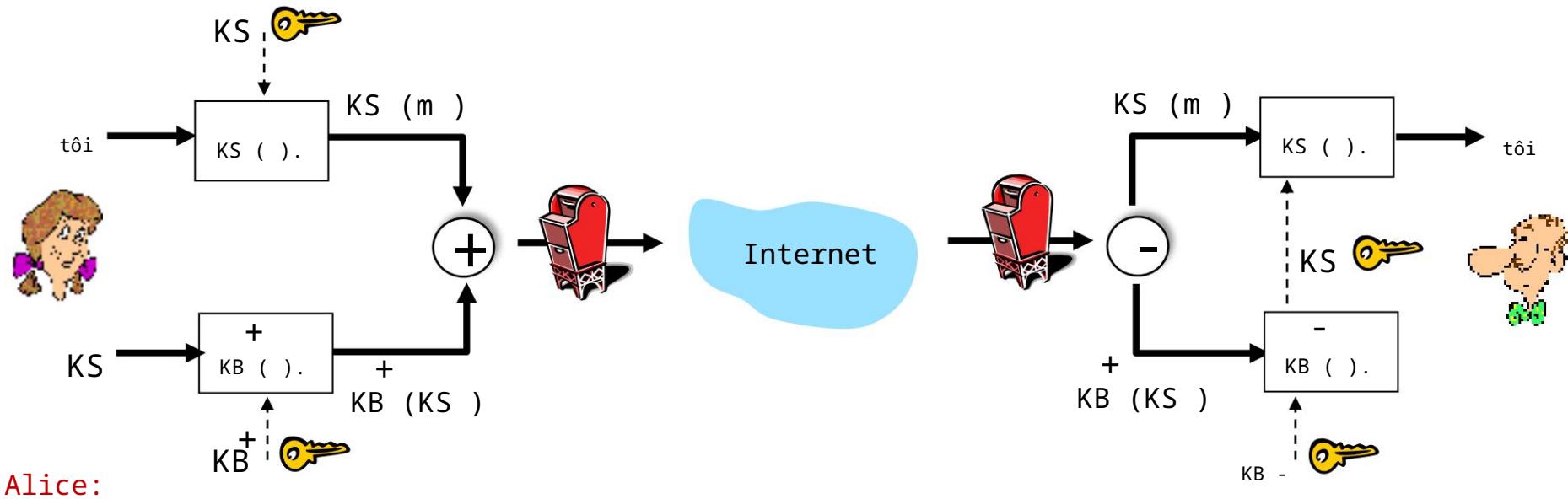
động và không dây Bảo mật vận

hành: tường lửa và IDS



Bảo mật e-mail: bảo mật

Alice muốn gửi e-mail bí mật , m , cho Bob.



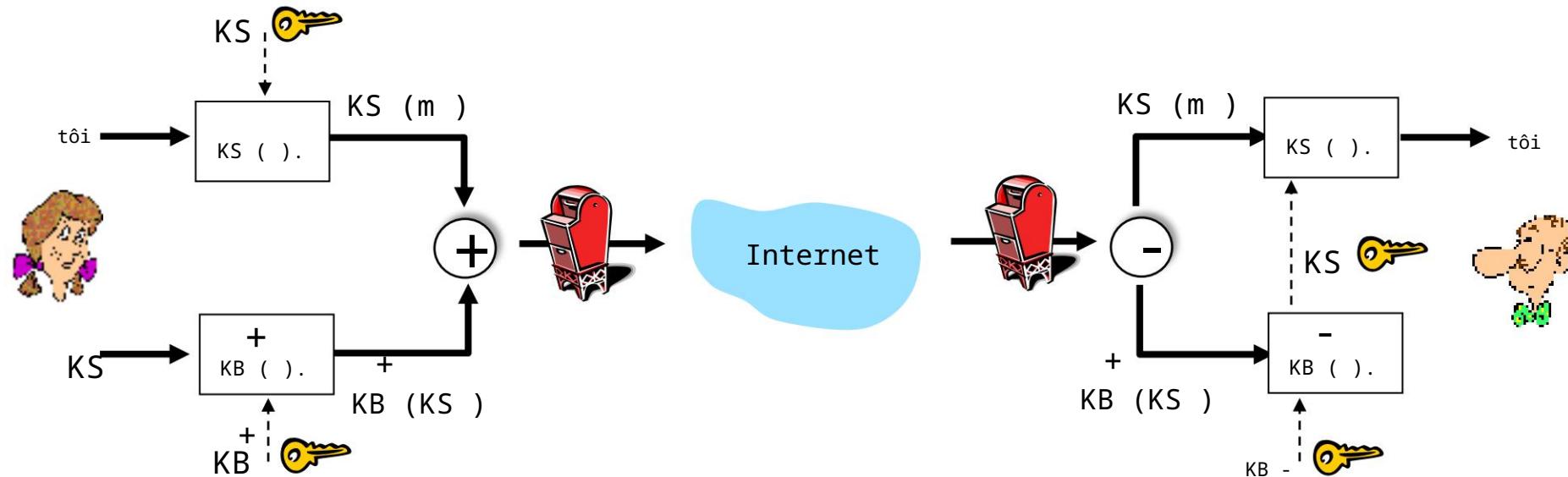
Alice:

tạo khóa riêng đối xứng ngẫu nhiên , KS mã hóa tin
nhắn bằng KS (để đạt hiệu quả) cũng mã hóa KS bằng khóa
chung của Bob gửi cả $KS(m)$ và K^+

$B(KS)$ đến Bob

Bảo mật e-mail: bảo mật (thêm)

Alice muốn gửi e-mail bí mật , m , cho Bob.

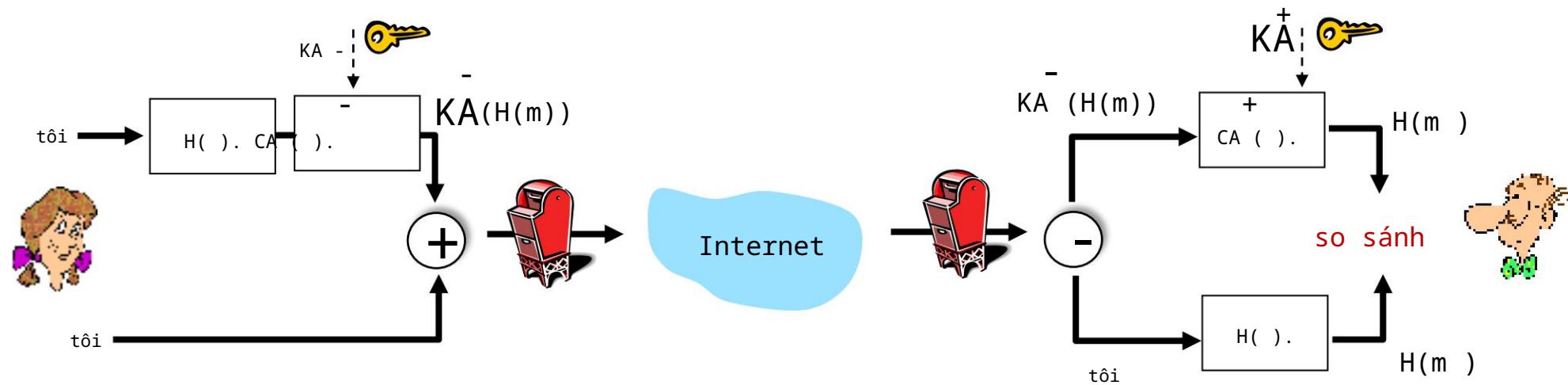


Bob:

sử dụng khóa riêng của mình để giải mã
và khôi phục KS sử dụng KS để giải mã
 $KS(m)$ để khôi phục m

Bảo mật e-mail: toàn vẹn, xác thực

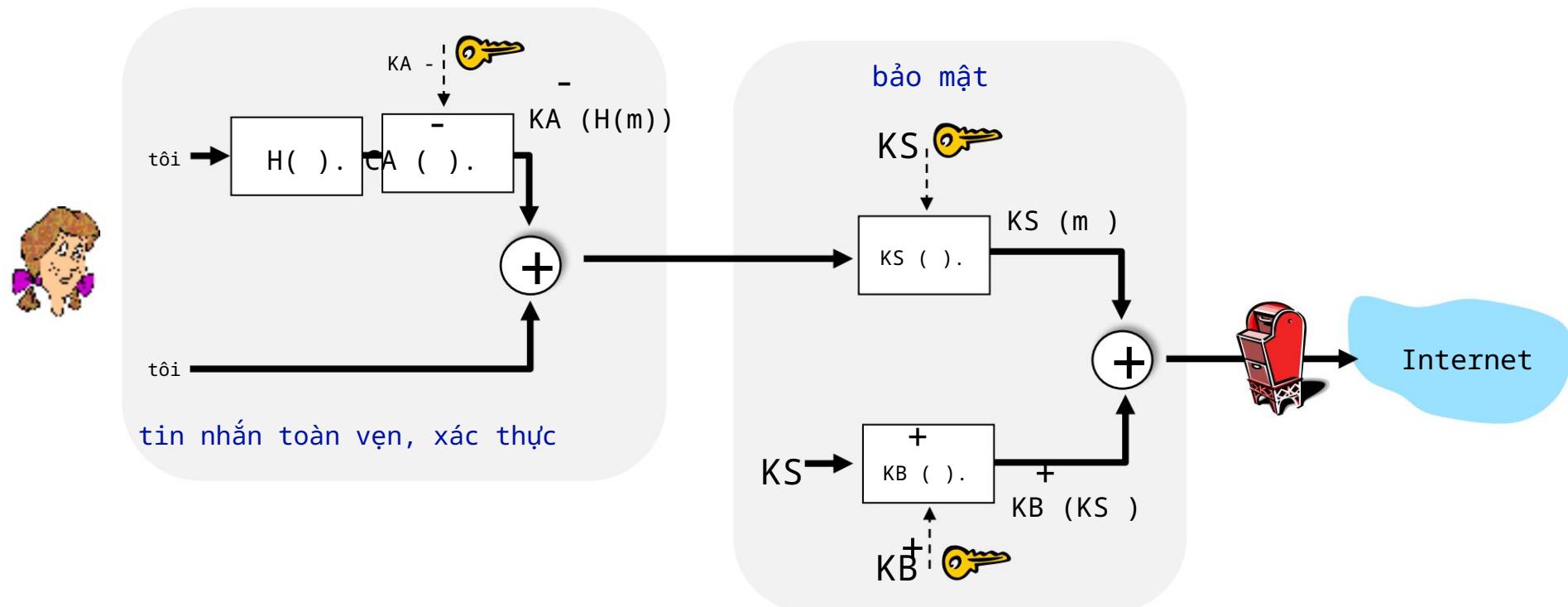
Alice muốn gửi m cho Bob, với tính toàn vẹn của tin nhắn, xác thực



Alice ký điện tử hàm băm của tin nhắn bằng khóa riêng của mình, cung cấp tính toàn vẹn và xác thực
gửi cả tin nhắn (rõ ràng) và chữ ký điện tử

Bảo mật e-mail: toàn vẹn, xác thực

Alice gửi m cho Bob, với tính bảo mật, tính toàn vẹn của tin nhắn, xác thực



Alice sử dụng ba khóa: khóa riêng của cô ấy, khóa chung của Bob, khóa đối xứng mới
hành động bổ sung của Bob là gì?

đại cương chương 8

An ninh mạng là gì?

Nguyên lý mật mã

Xác thực, toàn vẹn thông điệp

Bảo mật thư điện tử

Bảo mật kết nối TCP: TLS Bảo
mật lớp mạng: IPsec Bảo mật
trong mạng di động và không dây
Bảo mật vận hành: tường lửa và IDS



Bảo mật tầng vận chuyển (TLS)

giao thức bảo mật được triển khai rộng rãi phía trên lớp vận chuyển •
được hỗ trợ bởi hầu hết các trình duyệt, máy chủ web: https (cổng 443)
cung cấp: • tính **bảo mật**: thông qua mã hóa đối xứng • **tính toàn vẹn**:
thông qua hàm băm mật mã • **xác thực**: thông qua mật khẩu
lịch sử: • nghiên cứu, triển khai ban đầu: lập trình mạng an toàn, cấm
tất cả các kỹ thuật chung với dữ liệu nghiên cứu
an toàn • lớp cổng bảo mật (SSL) không được dùng nữa [2015] • TLS 1.3:
RFC 8846 [2018]

Bảo mật tầng vận chuyển (TLS)

giao thức bảo mật được triển khai rộng rãi phía trên tầng vận chuyển •
được hỗ trợ bởi hầu hết các trình duyệt, máy chủ web: https (cổng 443)
cung cấp: • tính **bảo mật**: thông qua mã hóa đối xứng • **tính toàn vẹn**:
thông qua hàm băm mật mã • **xác thực**: thông qua mật khẩu
lịch sử: • nghiên cứu, triển khai ban đầu: lập trình mang an toàn
tất cả các kỹ thuật
chung với đã nghiên cứu
• nghiêm cứu, triển khai ban đầu: lập trình mang an toàn
cắm
an toàn • lớp cổng bảo mật (SSL) không được dùng nữa [2015] • TLS 1.3:
RFC 8846 [2018]

Bảo mật tầng vận chuyển: cần những gì?

chúng ta hãy xây dựng một giao thức TLS đồ chơi, t-tls, để xem những gì cần thiết! chúng ta đã thấy “các mảnh ghép” rồi:

bắt tay: Alice, Bob sử dụng chứng chỉ, khóa riêng của họ để xác thực lẫn nhau, trao đổi hoặc tạo bí mật dùng chung **Dẫn**

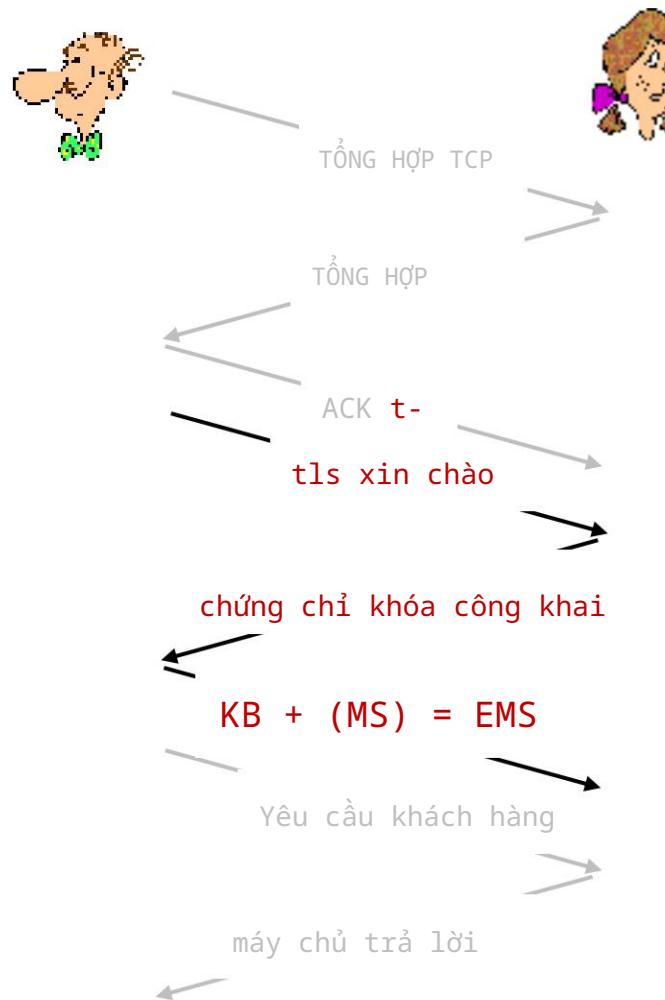
xuất khóa: Alice, Bob sử dụng bí mật dùng chung để lấy bộ khóa

truyền dữ liệu: truyền dữ liệu theo luồng: dữ liệu dưới dạng một loạt các bản ghi

- không chỉ giao dịch một lần

đóng kết nối: thông báo đặc biệt để đóng kết nối an toàn

t-tls: bắt tay ban đầu



giai đoạn bắt tay t-tls:

Bob thiết lập kết nối TCP với Alice

Bob xác minh rằng Alice thực sự
Alice

Bob gửi cho Alice một khóa bí mật
chính (MS), được sử dụng để tạo tất
cả các khóa khác cho phiên TLS

các sự cố tiềm ẩn:

- 3 RTT trước khi máy khách có
thể bắt đầu nhận dữ liệu (bao
gồm bắt tay TCP)

t-tls: khóa mật mã

được coi là không tốt khi sử dụng cùng một khóa cho nhiều hơn một mật mã
chức năng

- các khóa khác nhau cho mã xác thực tin nhắn (MAC) và mã hóa bốn khóa:

 Kc : khóa mã hóa cho dữ liệu được gửi từ máy khách đến máy chủ

 Mc : Khóa MAC cho dữ liệu được gửi từ máy khách đến máy chủ

 Ks : khóa mã hóa cho dữ liệu được gửi từ máy chủ đến máy khách

 Ms : Khóa MAC cho dữ liệu được gửi từ máy chủ đến máy khách

các khóa bắt nguồn từ chức năng dẫn xuất khóa (KDF) • lấy

bí mật chính và (có thể) một số dữ liệu ngẫu nhiên bổ sung để tạo khóa mới

t-tls: mã hóa dữ liệu

thu hồi: TCP cung cấp khả năng trừu tượng hóa luồng byte dữ liệu

Hỏi: chúng tôi có thể mã hóa dữ liệu trong luồng như được ghi vào ổ cắm TCP không?

- A: MAC sẽ đi về đâu? Nếu ở cuối, không có tin nhắn toàn vẹn cho đến khi tất cả dữ liệu đã nhận và kết nối đã đóng!
- giải pháp: ngắt luồng theo chuỗi “bản ghi” •

mỗi bản ghi từ máy khách đến máy chủ mang một MAC, được tạo bằng Mc

- bộ thu có thể tác động lên từng bản ghi khi nó đến

Bản ghi t-tls được mã hóa bằng khóa đối xứng, Kc, được chuyển tới TCP:



t-tls: mã hóa dữ liệu (thêm)

các cuộc tấn công có thể xảy ra trên luồng dữ liệu?

- **sắp xếp lại:** man-in middle chặn các phân đoạn TCP và sắp xếp lại (thao tác các chuỗi # trong tiêu đề TCP không được mã hóa) • **phát lại giải pháp:**
- sử dụng số thứ tự TLS (dữ liệu, TLS-seq# được tích hợp vào MAC)
- sử dụng nonce

t-tls: đóng kết nối

tấn công cắt ngắn:

- kẻ tấn công giả mạo phân đoạn đóng kết nối TCP • một

hoặc cả hai bên nghĩ rằng có ít dữ liệu hơn thực tế

giải pháp: các loại bản ghi, với một loại để đóng

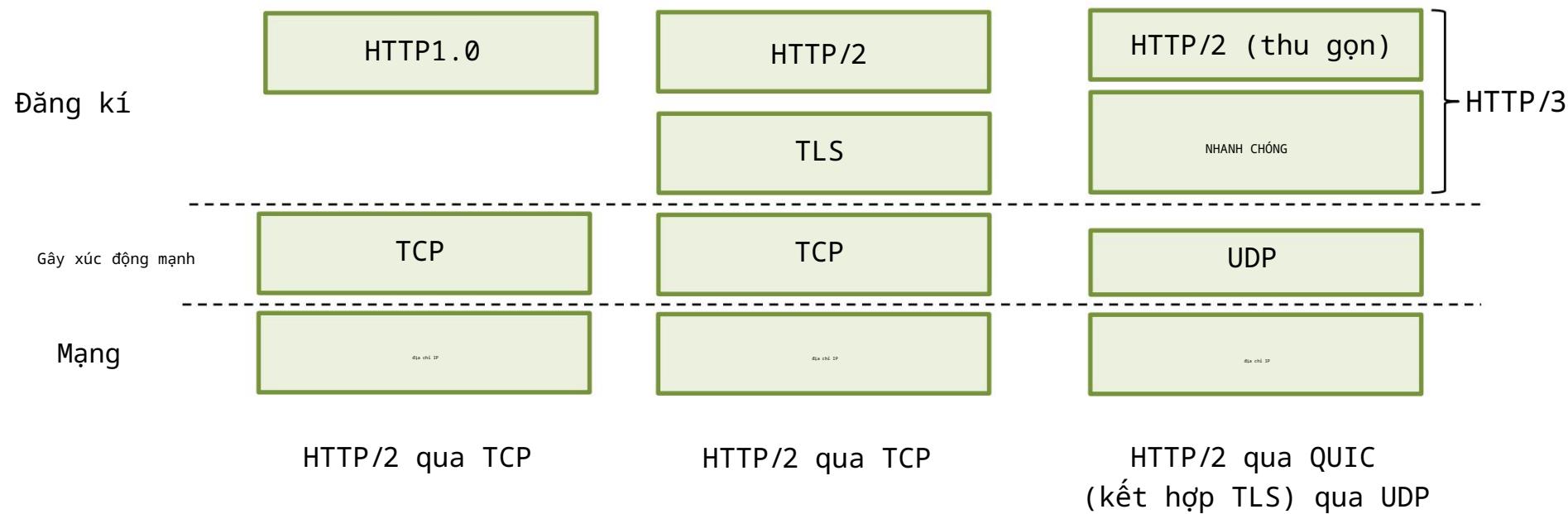
- nhập 0 cho dữ liệu; gõ 1 để đóng

MAC hiện được tính bằng dữ liệu, loại, trình tự #



Bảo mật tầng vận chuyển (TLS)

TLS cung cấp API mà bất kỳ ứng dụng nào cũng có thể sử dụng giao diện HTTP của TLS:



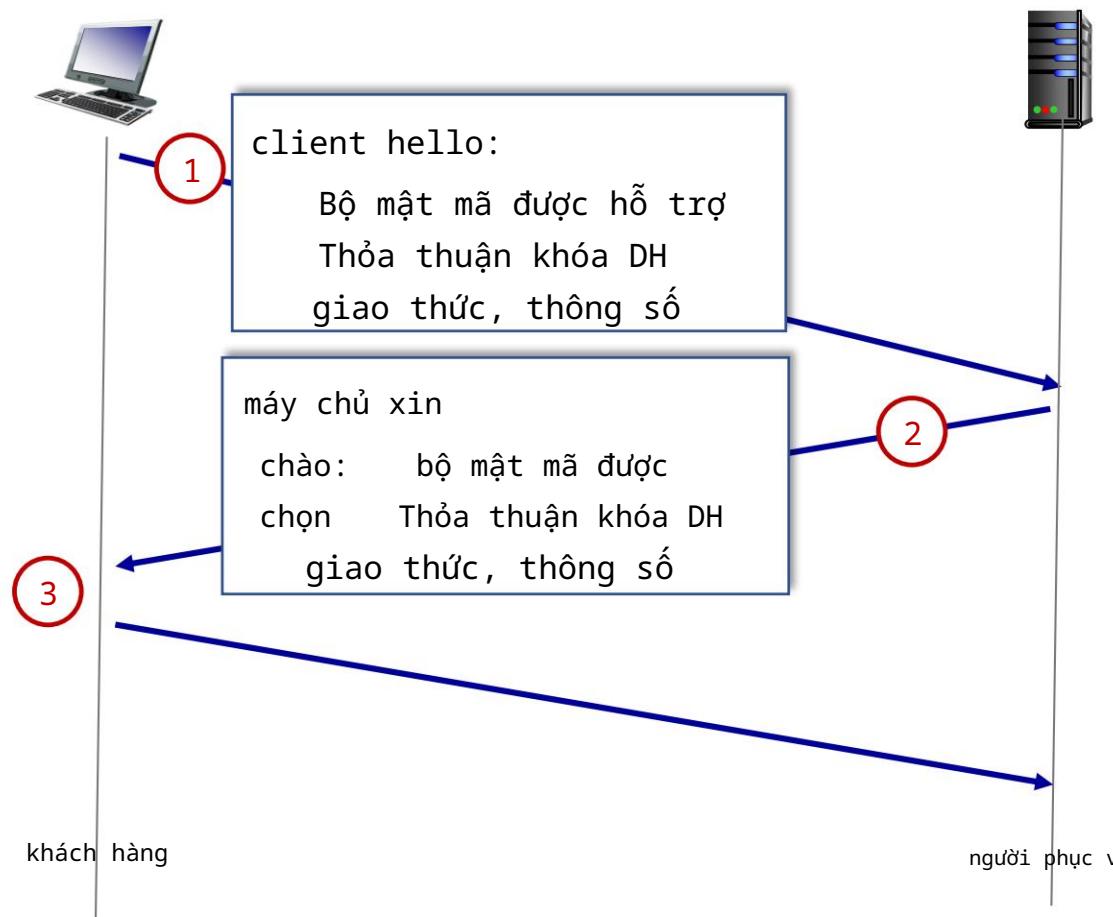
TLS: bộ mật mã 1.3

“bộ mật mã”: các thuật toán có thể được sử dụng để tạo khóa, mã hóa, MAC, chữ ký số

TLS: 1.3 (2018): lựa chọn bộ mật mã hạn chế hơn so với TLS 1.2 (2008)

- chỉ có 5 lựa chọn, thay vì 37 lựa chọn
- yêu cầu Diffie-Hellman (DH) để trao đổi khóa, thay vì DH hoặc RSA
- thuật toán xác thực và mã hóa kết hợp (“mã hóa xác thực”) cho dữ liệu thay vì mã hóa nối tiếp, xác thực • 4 dựa trên AES
- HMAC sử dụng hàm băm mật mã SHA (256 hoặc 284)

Bắt tay TLS 1.3: 1 RTT



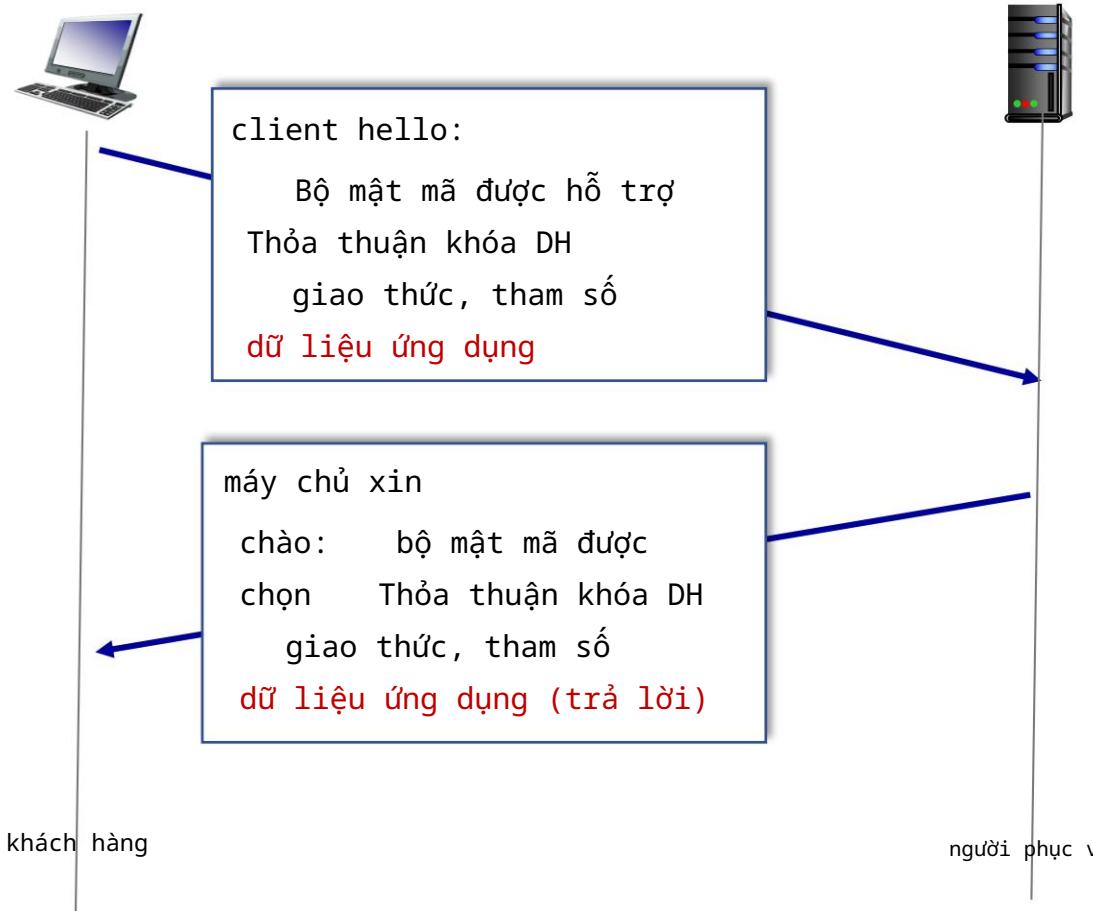
1 client TLS hello msg:

đoán giao thức thỏa thuận
khóa , các tham số chỉ ra
các bộ mật mã mà nó hỗ trợ

2 máy chủ TLS hello msg chọn giao
thức thỏa thuận khóa, tham số bộ
mật mã chứng chỉ do máy chủ ký

3 máy
khách: kiểm tra chứng chỉ máy
chủ tạo khóa hiện có thể
thực hiện yêu cầu ứng dụng (ví dụ:
HTTPS GET)

Bắt tay TLS 1.3: 0 RTT



tin nhắn chào ban đầu chưa dữ liệu ứng dụng được mã hóa! • “tiếp tục” kết nối trước đó giữa máy khách và máy chủ

- dữ liệu ứng dụng được mã hóa bằng cách sử dụng “bí mật tổng thể nối lại” từ kết nối trước đó

dễ bị tấn công lại! • có thể OK để nhận HTTP GET hoặc các yêu cầu máy khách không sửa đổi trạng thái máy chủ

đại cương chương 8

An ninh mạng là gì?

Nguyên tắc mật mã

Xác thực, toàn vẹn thông điệp

Bảo mật e-mail Bảo mật kết nối

TCP: TLS Bảo mật lớp mạng:

IPsec Bảo mật trong mạng di

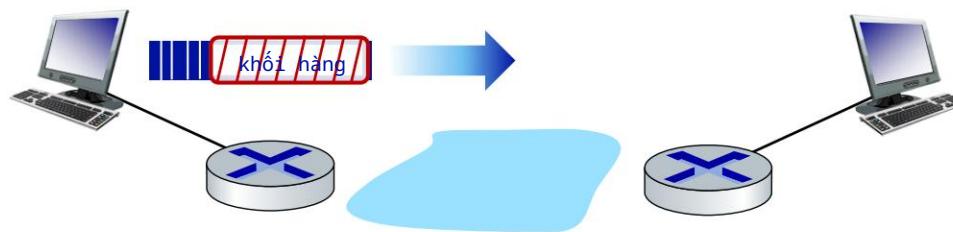
động và không dây Bảo mật vận

hành: tường lửa và IDS



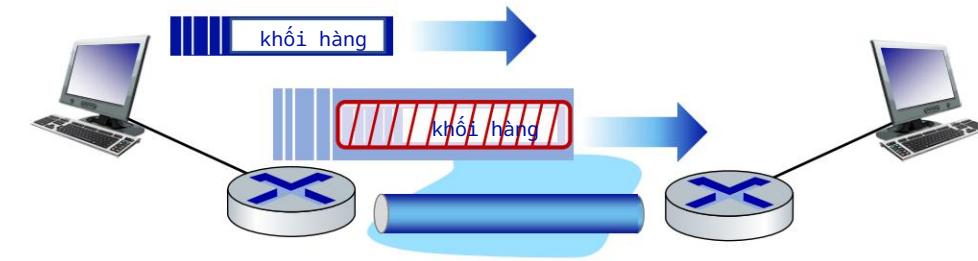
bảo mật IP

cung cấp mã hóa, xác thực, toàn vẹn ở cấp dữ liệu • cho cả lưu lượng người dùng và lưu lượng điều khiển (ví dụ: thông điệp BGP, DNS)
 hai “chế độ”:



chế độ vận chuyển:

chỉ tải dữ liệu datagram
được mã hóa, xác thực



chế độ đường hầm:

toàn bộ datagram được mã hóa, xác thực datagram mã hóa được đóng gói trong datagram mới với tiêu đề IP mới, được tạo đường hầm tới đích

Hai giao thức IPsec

Giao thức Tiêu đề xác thực (AH) [RFC 4302]

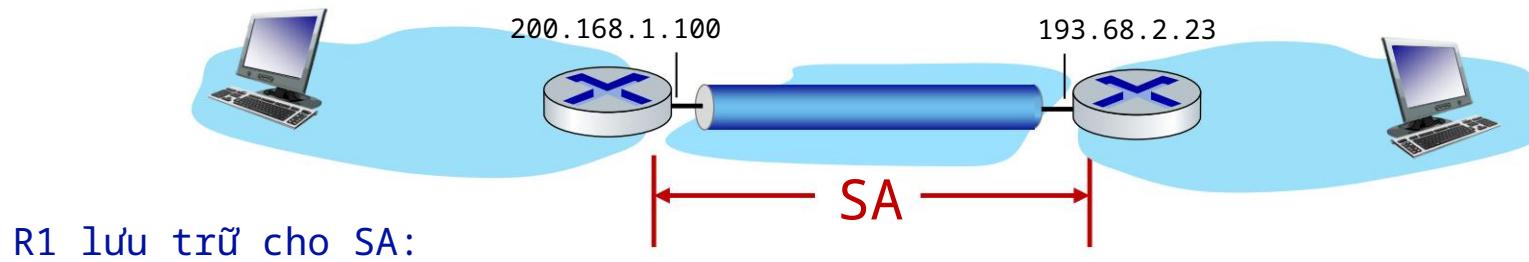
- cung cấp xác thực nguồn & toàn vẹn dữ liệu nhưng không bảo mật

Giao thức bảo mật đóng gói (ESP) [RFC 4303]

- cung cấp xác thực nguồn, tính toàn vẹn dữ liệu và tính bảo mật •
được sử dụng rộng rãi hơn AH

Hiệp hội bảo mật (SA)

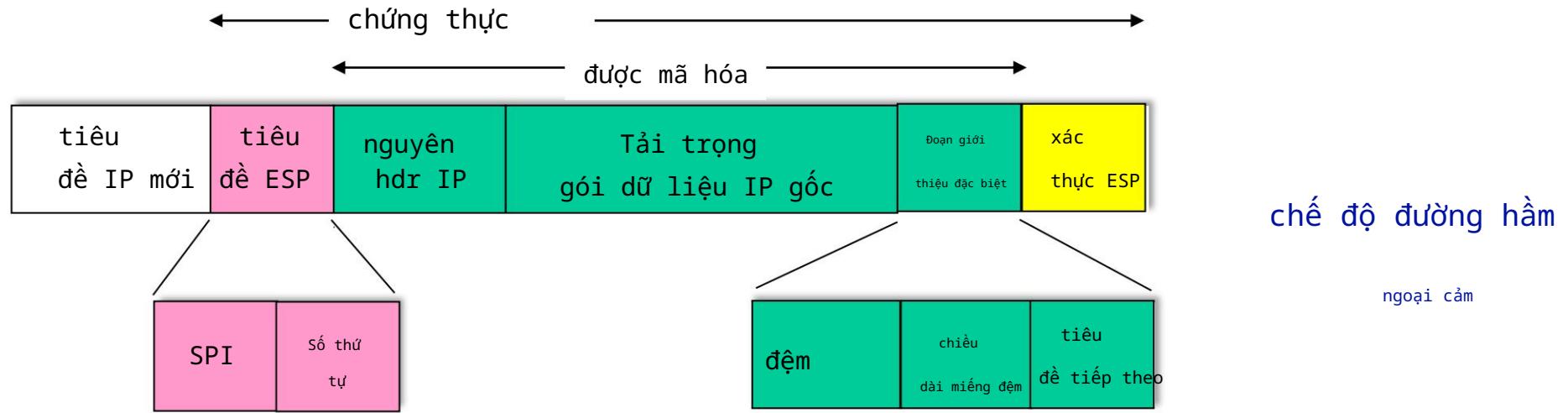
trước khi gửi dữ liệu, **liên kết bảo mật (SA)** được thiết lập từ thực thể gửi đến thực thể nhận (hướng) kết thúc, quyền nhận duy trì thông tin trạng thái về SA • thu hồi: Điểm cuối TCP cũng duy trì thông tin trạng thái • IP không kết nối; IPsec là hướng kết nối!



Mã định danh 32 bit: Chỉ số tham số bảo mật (SPI)

giao diện SA gốc (200.168.1.100) khóa mã hóa giao diện SA
 đích (193.68.2.23) loại kiểm tra tính toàn vẹn lõi được mã hóa được sử dụng
 khóa xác thực

Gói dữ liệu IPsec



Đoạn giới thiệu ESP: đệm cho mật mã khôi Tiêu

đè ESP:

- SPI, để thực thể nhận biết phải làm gì
- số thứ tự, để ngăn chặn các cuộc tấn công lặp lại

MAC trong trường xác thực ESP được tạo bằng khóa bí mật dùng chung

Chế độ đường hầm ESP: hành động

tại R1:

thêm đoạn giới thiệu ESP vào bản gốc datagram (bao gồm các trường tiêu đề ban đầu!) mã hóa kết quả bằng thuật toán & khóa được chỉ định bởi SA

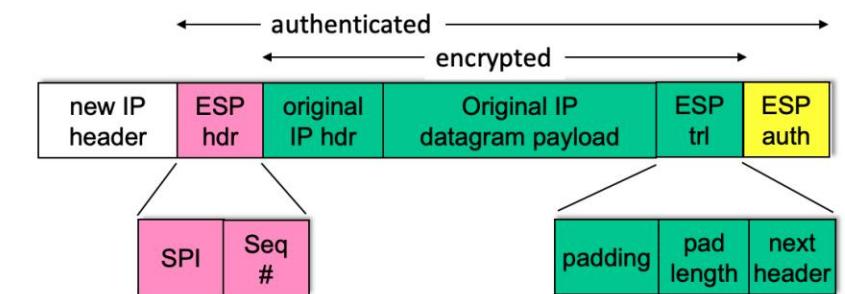
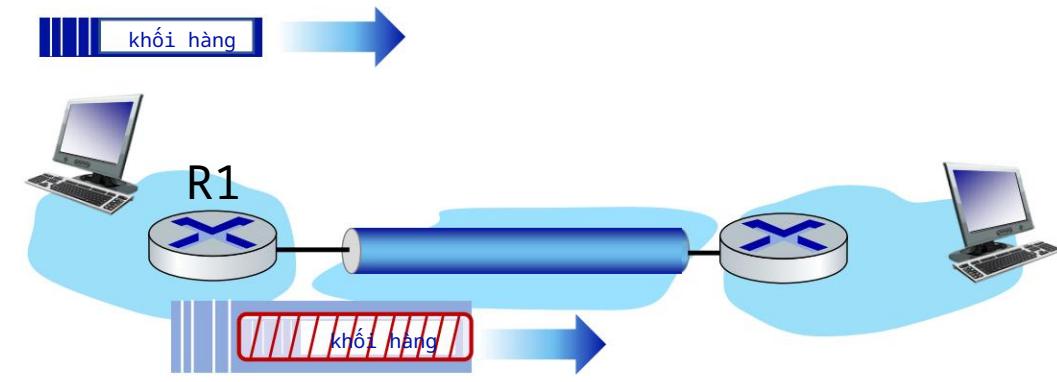
nối thêm tiêu đề ESP vào phía trước này

số lượng được mã hóa

tạo MAC xác thực sử dụng thuật toán và khóa được chỉ định trong SA

nối tải trọng hình thành MAC tạo

tiêu đề IP mới, các trường tiêu đề IP mới, địa chỉ cho điểm cuối đường hầm



Số thứ tự IPsec

đối với SA mới, người gửi khởi tạo seq. # đến 0 mỗi

khi gói dữ liệu được gửi trên SA: • người gửi tăng bộ đếm
seq # • đặt giá trị vào trường seq #

mục

tiêu: • ngăn chặn kẻ tấn công đánh hơi và phát lại một gói • việc

nhận các gói IP đã xác thực, trùng lặp có thể làm gián đoạn dịch vụ

phương pháp:

- đích kiểm tra các bản sao • không

theo dõi tất cả các gói đã nhận; thay vào đó sử dụng một cửa sổ

Cơ sở dữ liệu bảo mật IPsec

Cơ sở dữ liệu chính sách bảo mật (SPD)

chính sách: đối với datagram nhất định, người gửi cần biết liệu nó có nên sử dụng IPsec

chính sách được lưu trữ trong cơ sở dữ liệu
chính sách bảo mật (SPD)

cần biết nên sử dụng SA nào

- có thể sử dụng: địa chỉ IP nguồn và đích ; số giao thức

SAD: “làm thế nào” để làm điều đó

An ninh PGS. Cơ sở dữ liệu (SAD) điểm cuối giữ

trạng thái SA trong cơ sở dữ liệu liên kết **bảo mật (SAD)** khi gửi IPsec datagram, R1 truy cập SAD để xác định cách xử lý datagram khi IPsec datagram đến R2, R2 kiểm tra SPI trong IPsec datagram, lập chỉ mục SAD với SPI , xử lý datagram tương ứng.

SPD: “làm gì”

Tóm tắt: Các dịch vụ IPsec



Trudy ngồi đâu đó giữa R1, R2. cô ấy không biết các phím • Liệu Trudy có thể nhìn thấy nội dung ban đầu của datagram? Làm thế nào về nguồn, địa chỉ IP đích, giao thức truyền tải, cổng ứng dụng? • lật bit mà không phát hiện? • Giả danh R1 bằng cách sử dụng địa chỉ IP của R1? • phát lại một datagram?

IKE: Trao đổi khóa Internet

các ví dụ trước: thiết lập thủ công IPsec SA trong các điểm cuối IPsec:

SA ví dụ:

SPI: 12345

IP nguồn: 200.168.1.100

IP đích: 193.68.2.23

Giao thức: ESP

Thuật toán mã hóa: 3DES-cbc

Thuật toán HMAC: MD5 Khóa mã
hóa: 0x7aeaca.

Khóa HMAC: 0xc0291f.

khóa thủ công là không thực tế đối với VPN có 100 điểm cuối thay
vào đó hãy sử dụng IPsec IKE (Trao đổi khóa Internet)

IKE: PSK và PKI

xác thực (chứng minh bạn là ai) với một trong hai

- bí mật chia sẻ trước (PSK)
- hoặc • với PKI (chứng chỉ và khóa công khai/riêng tư).

PSK: đôi bên bắt đầu bí mật

- chạy IKE để xác thực lẫn nhau và tạo IPsec SA (mỗi bên một hướng), bao gồm mã hóa, khóa xác thực
- PKI: cả hai bên bắt đầu bằng cặp khóa công khai/riêng tư, chứng chỉ

• chạy IKE để xác thực lẫn nhau, lấy IPsec SA (một trong mỗi hướng).

- tương tự với bắt tay trong SSL.

giai đoạn IKE

IKE có hai giai đoạn

- **giai đoạn 1:** thiết lập IKE SA hai chiều
 - lưu ý: IKE SA khác với IPsec SA • còn gọi là hiệp hội bảo mật ISAKMP
- **giai đoạn 2:** ISAKMP được sử dụng để đàm phán an toàn cặp IPsec của SA
giai đoạn 1 có hai chế độ: chế độ tích cực và chế độ chính
 - chế độ tích cực sử dụng ít tin nhắn hơn
 - chế độ chính cung cấp khả năng bảo vệ danh tính và linh hoạt hơn

Tóm tắt IPsec

Trao đổi bản tin IKE lấy thuật toán, khóa bí mật, SPI
con số

giao thức AH hoặc ESP (hoặc cả hai)

- AH cung cấp tính toàn vẹn, xác thực nguồn •

Giao thức ESP (với AH) cung cấp thêm mã hóa IPsec ngang

hàng có thể là hai hệ thống đầu cuối, hai bộ định tuyến/tường lửa hoặc
một bộ định tuyến/tường lửa và một hệ thống đầu cuối

đại cương chương 8

An ninh mạng là gì?

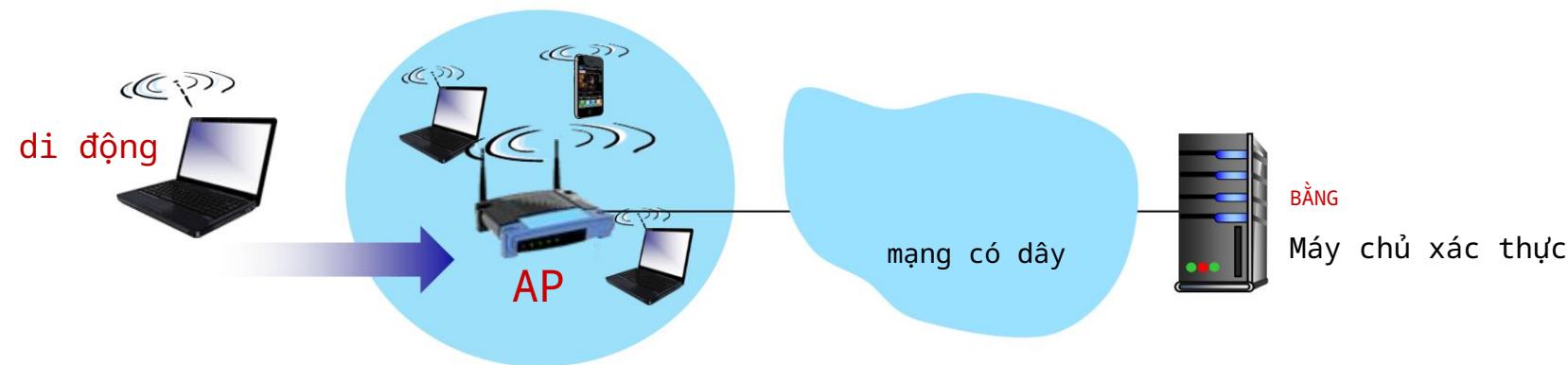
Nguyên tắc mật mã Xác
thực, toàn vẹn thông điệp Bảo
mật e-mail Bảo mật kết nối TCP:
TLS Bảo mật tầng mạng: IPsec
Bảo mật trong mạng di động và không
dây

- 802.11 (Wi-Fi)
- 4G/5G

Bảo mật vận hành: tường lửa và IDS



802.11: xác thực, mã hóa

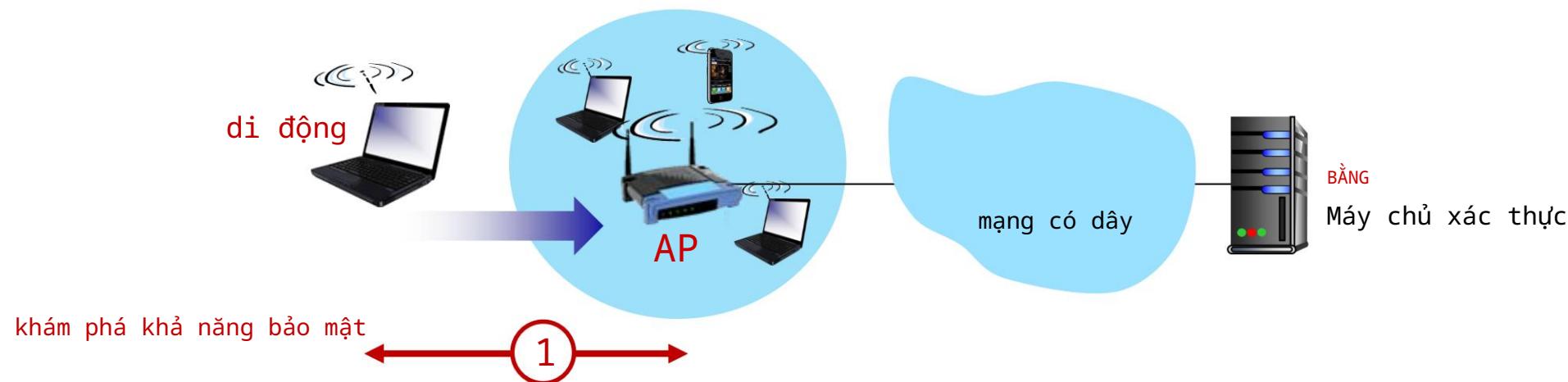


Điện thoại di động

đến phải: liên kết với điểm truy cập: (thiết lập) liên lạc qua
liên kết không dây

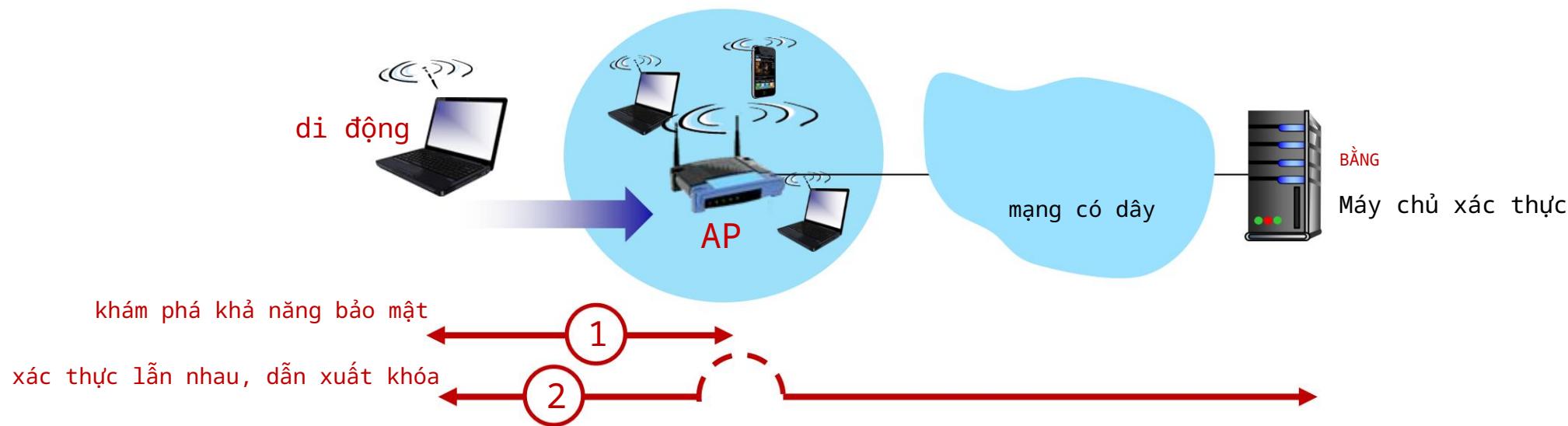
xác thực với mạng

802.11: xác thực, mã hóa



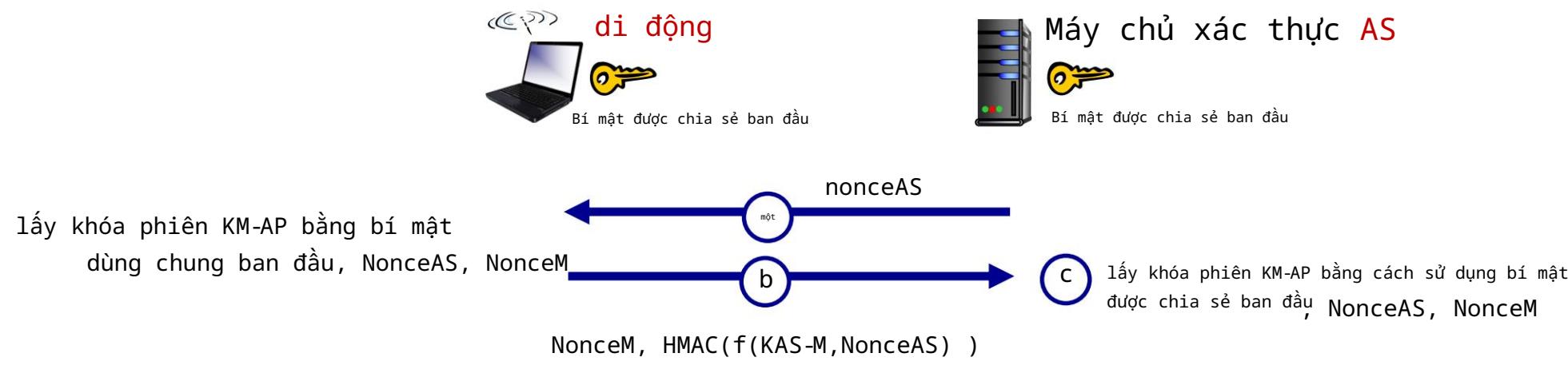
- ① khám phá các khả năng bảo mật: AP quảng cáo sự hiện diện của nó, các hình thức xác thực và mã hóa được cung cấp thiết bị yêu cầu các hình thức xác thực cụ thể, mong muốn mã hóa mặc dù thiết bị, AP đã trao đổi tin nhắn, thiết bị chưa được xác thực, không có khóa mã hóa

802.11: xác thực, mã hóa



- ② xác thực lẫn nhau và dẫn xuất khóa đối xứng được chia sẻ: AS, thiết bị di động đã chia sẻ bí mật chung (ví dụ: mật khẩu) AS, thiết bị di động sử dụng bí mật chung, nonces (ngăn chặn các cuộc tấn công chuyển tiếp), băm mật mã (đảm bảo tính toàn vẹn của thông báo) để xác thực lẫn nhau
AS, khóa phiên đối xứng dẫn xuất di động

802.11: Bắt tay WPA3



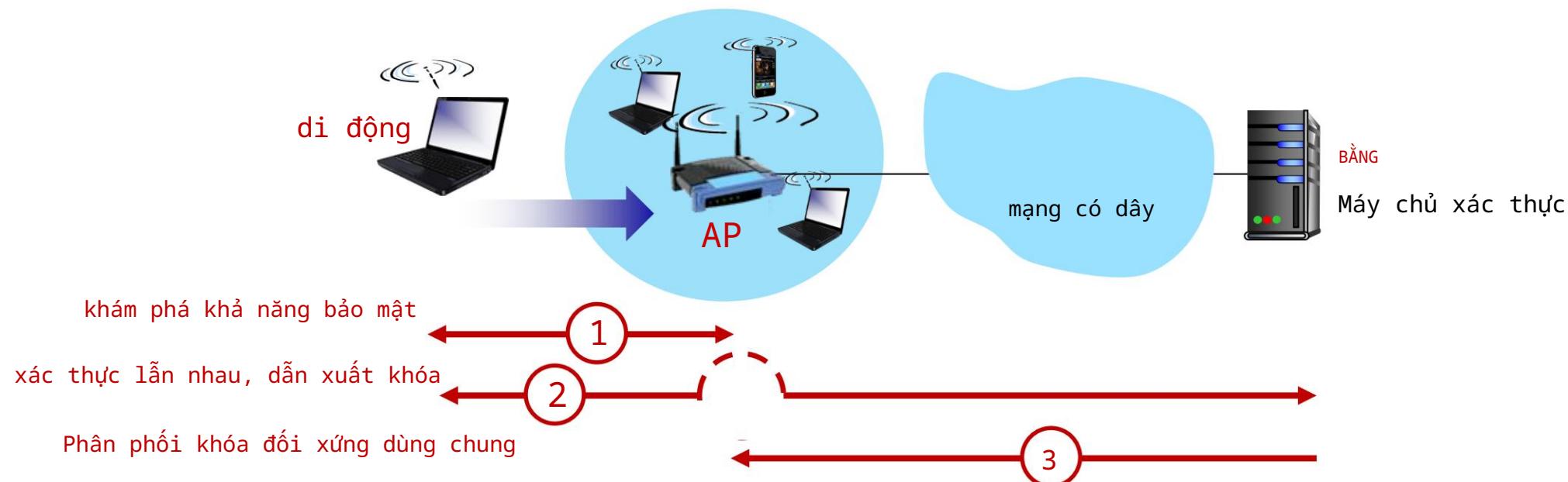
một AS tạo NonceAS, gửi đến di động Di động nhận NonceAS

b NonceAS • tạo NonceM • tạo khóa phiên chia sẻ đối xứng KM-AP sử dụng NonceAS, NonceM và bí mật chia sẻ ban đầu

- gửi NonceM và giá trị do HMAC ký bằng cách sử dụng NonceAS và bí mật được chia sẻ ban đầu AS lấy được khóa phiên được chia sẻ đối xứng KM-AP

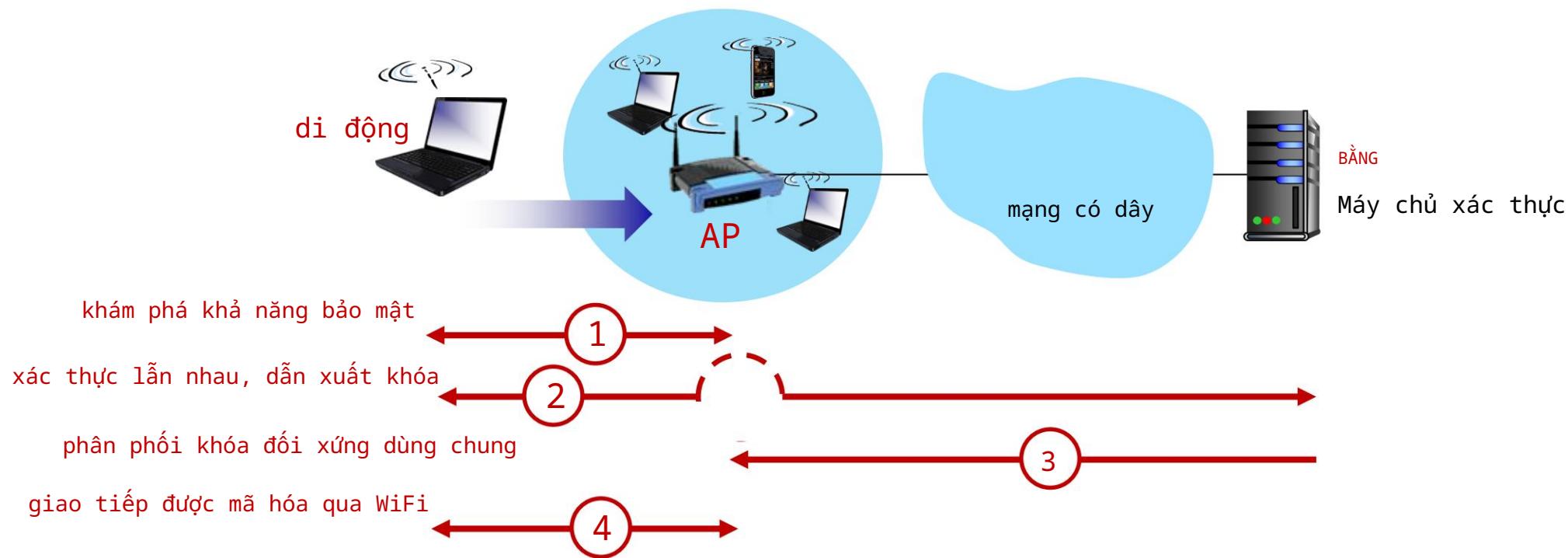
c AS lấy được khóa phiên được chia sẻ đối xứng KM-AP

802.11: xác thực, mã hóa



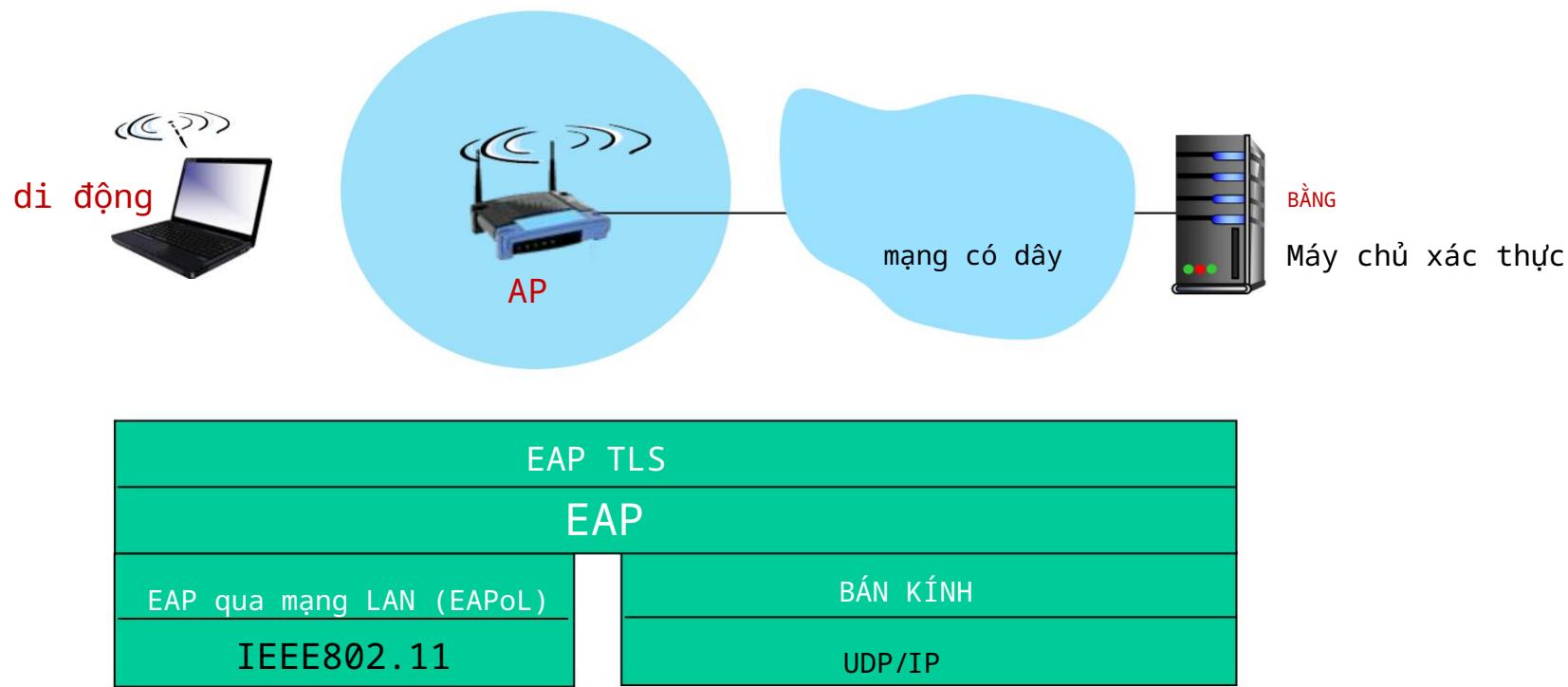
- ③ phân phối khóa phiên đối xứng được chia sẻ (ví dụ: đối với mã hóa AES) cùng một khóa được lấy tại thiết bị di động, AS thông báo cho AP về phiên đối xứng được chia sẻ

802.11: xác thực, mã hóa



- ④ giao tiếp được mã hóa giữa thiết bị di động và máy chủ từ xa thông qua AP cùng một khóa được lấy tại thiết
 bị di động, AS AS thông báo cho AP về phiên đối xứng được chia sẻ

802.11: xác thực, mã hóa



Giao thức xác thực mở rộng (EAP) [RFC 3748] xác định giao thức yêu cầu/phản hồi đầu cuối giữa thiết bị di động, AS

đại cương chương 8

An ninh mạng là gì?

Nguyên tắc mật mã

Xác thực, toàn vẹn thông điệp

Bảo mật e-mail Bảo mật kết nối

TCP: TLS Bảo mật lớp mạng:

IPsec Bảo mật trong mạng di

động và không dây • 802.11 (WiFi) • 4G/5G

Bảo mật vận hành: tường lửa và IDS



Xác thực, mã hóa trong 4G LTE



thiết bị di động đến

- phải:
- liên kết với BS: (thiết lập) liên lạc qua liên kết không dây 4G
 - xác thực chính nó với mạng và xác thực mạng điểm khác biệt đáng chú ý so với WiFi
 - SIMcard của điện thoại di động cung cấp nhận dạng toàn cầu, chứa khóa dùng chung
 - Dịch vụ trong mạng khách phụ thuộc vào đăng ký dịch vụ (trả phí) trong mạng gia đình

Xác thực, mã hóa trong 4G LTE

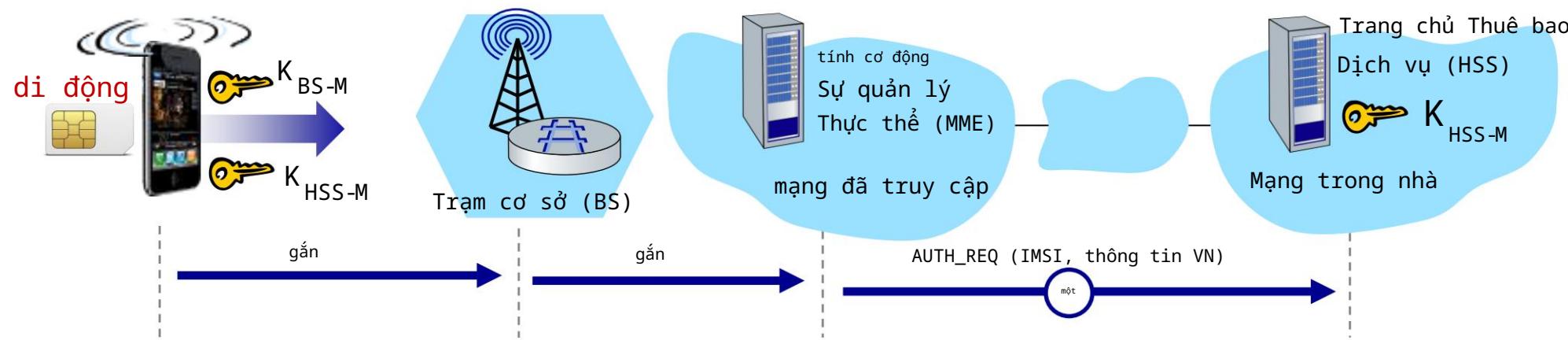


di động, BS sử dụng khóa phiên dãy xuất KBS-M để mã hóa thông tin liên lạc qua liên kết 4G

MME trong mạng khách + HHS trong mạng nhà, cùng đóng vai trò Wi-Fi AS

- trình xác thực cuối cùng là HSS
- mối quan hệ tin cậy và kinh doanh giữa khách thăm và nhà mạng lưới

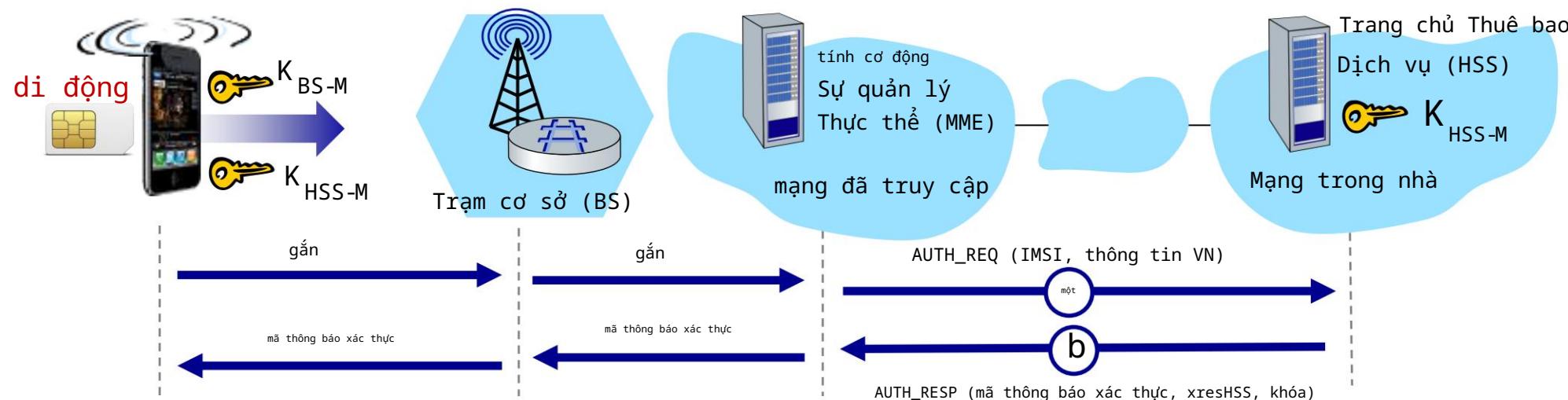
Xác thực, mã hóa trong 4G LTE



○ yêu cầu xác thực tới HSS mạng gia đình

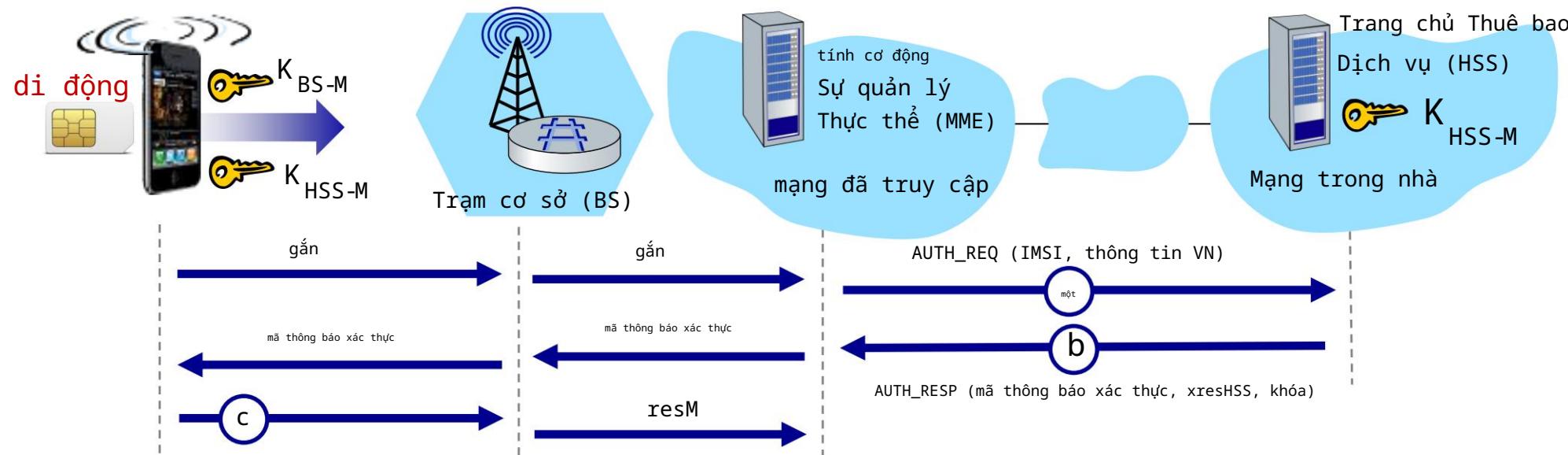
- di động gửi bản tin đính kèm (chứa IMSI của nó, thông tin mạng đã truy cập) được chuyển tiếp từ BS đến MME đã truy cập đến HSS nhà
- IMSI xác định mạng gia đình của điện thoại di động

Xác thực, mã hóa trong 4G LTE



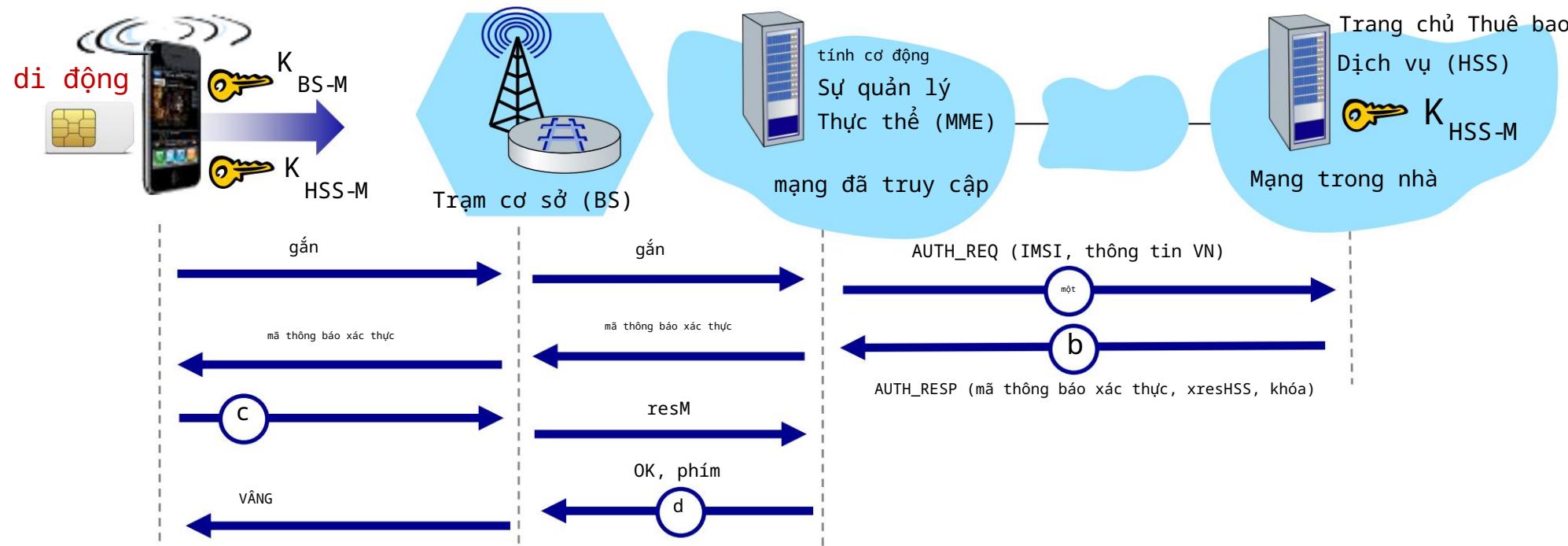
- b. HSS sử dụng khóa bí mật được chia sẻ trước, KHSS-M, để lấy mã thông báo xác thực , auth_token và mã thông báo phản hồi xác thực dự kiến, xresHSS . auth_token chứa thông tin được HSS mã hóa bằng KHSS-M , cho phép thiết bị di động biết rằng bất kỳ ai đã tính toán auth_token đều biết bí mật chia sẻ trước
- mạng di động đã được xác thực • HSS đã
 - truy cập giữ xresHSS để sử dụng sau này

Xác thực, mã hóa trong 4G LTE



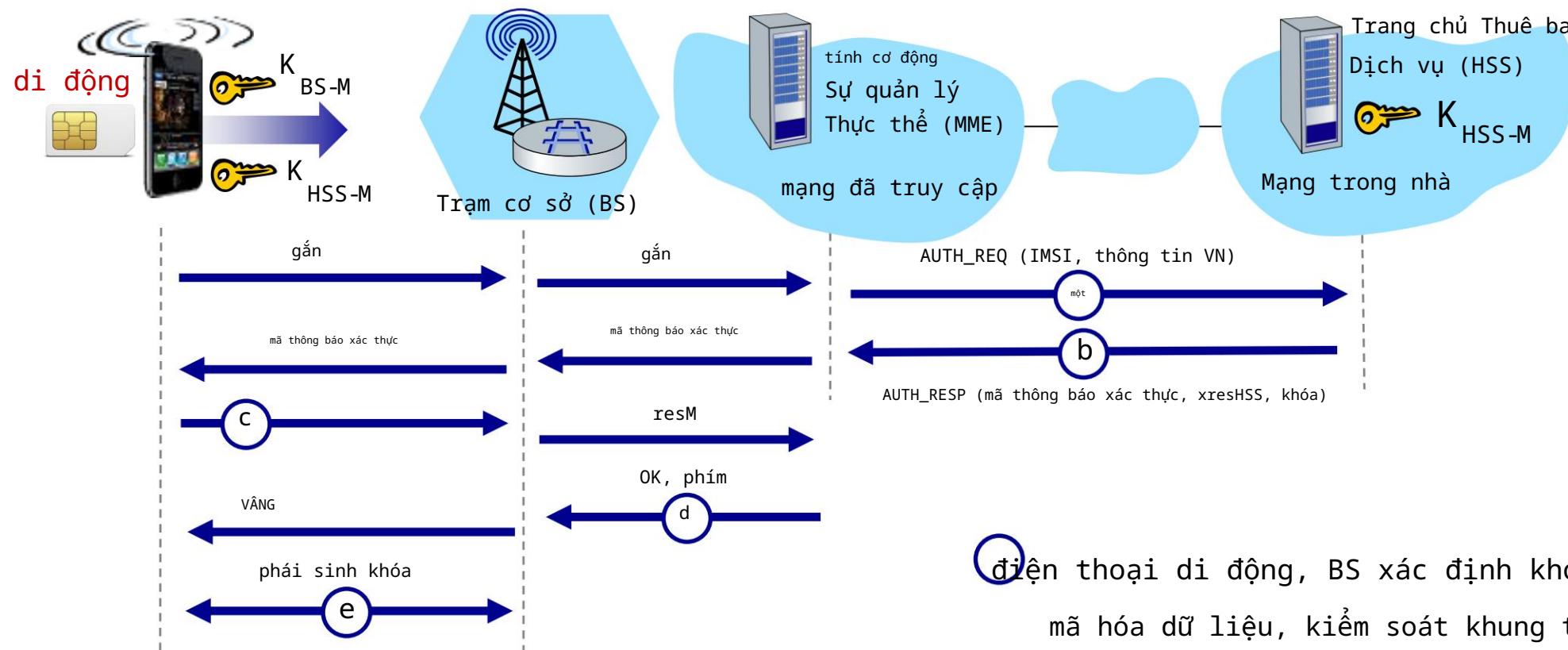
- c. phản hồi xác thực từ thiết bị di động: • thiết bị di động tính toán $resM$ bằng cách sử dụng khóa bí mật của nó để thực hiện cùng một phép tính mã hóa mà HSS đã thực hiện để tính toán $xresHSS$ và gửi $resM$ đến MME

Xác thực, mã hóa trong 4G LTE



- đ. di động được xác thực bởi mạng:
 - MMS so sánh giá trị $resM$ do di động tính toán với giá trị do HSS tính toán của $xresHSS$.
 - Nếu chúng khớp nhau, điện thoại di động được xác thực!
 - (tại sao?) • MMS thông báo cho BS rằng thiết bị di động được xác thực, tạo khóa cho BS

Xác thực, mã hóa trong 4G LTE



điện thoại di động, BS xác định khóa cho
mã hóa dữ liệu, kiểm soát khung trên
Kênh không dây 4G Có
thể sử dụng AES

Xác thực, mã hóa: từ 4G đến 5G

4G: MME trong mạng truy cập đưa ra quyết định xác thực

5G: mạng gia đình đưa ra quyết định xác thực • MME được truy cập đóng vai trò “trung gian” nhưng vẫn có thể từ chối

4G: sử dụng khóa chia sẻ trước **5G:**

khóa không chia sẻ trước cho IoT

4G: IMSI của thiết bị được truyền dưới dạng văn bản rõ ràng tới BS

5G: mật mã khóa công khai dùng để mã hóa IMSI

đại cương chương 8

An ninh mạng là gì?

Nguyên tắc mã hóa

Xác thực, toàn vẹn thông điệp

Bảo mật e-mail Bảo mật kết

nối TCP: TLS Bảo mật lớp mạng:

IPsec Bảo mật trong mạng di

động và không dây Bảo mật vận

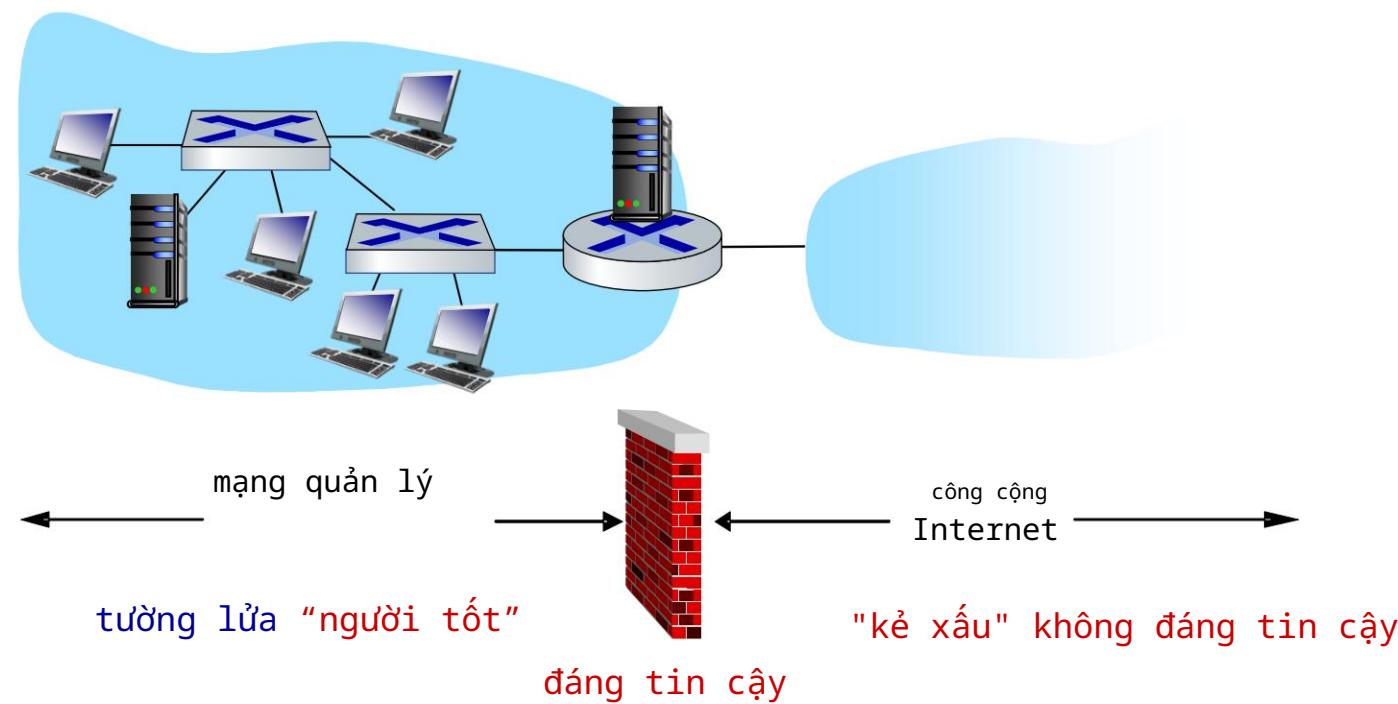
hành: tường lửa và IDS



tường lửa

bức tường lửa

cô lập mạng nội bộ của tổ chức từ mạng lớn hơn Internet, cho phép một số gói đi qua, chặn những gói khác



Tường lửa: tại sao

ngăn chặn các cuộc tấn công từ chối dịch

vụ: SYN lũ lụt: kẻ tấn công thiết lập nhiều kết nối TCP không có thật, không tài nguyên còn lại cho các kết nối "thực sự"

ngăn chặn sửa đổi/truy cập bất hợp pháp dữ liệu nội bộ

ví dụ: kẻ tấn công thay thế trang chủ của CIA bằng một thứ khác

chỉ cho phép truy cập được ủy quyền vào bên trong mạng

tập hợp người dùng/máy chủ được xác thực

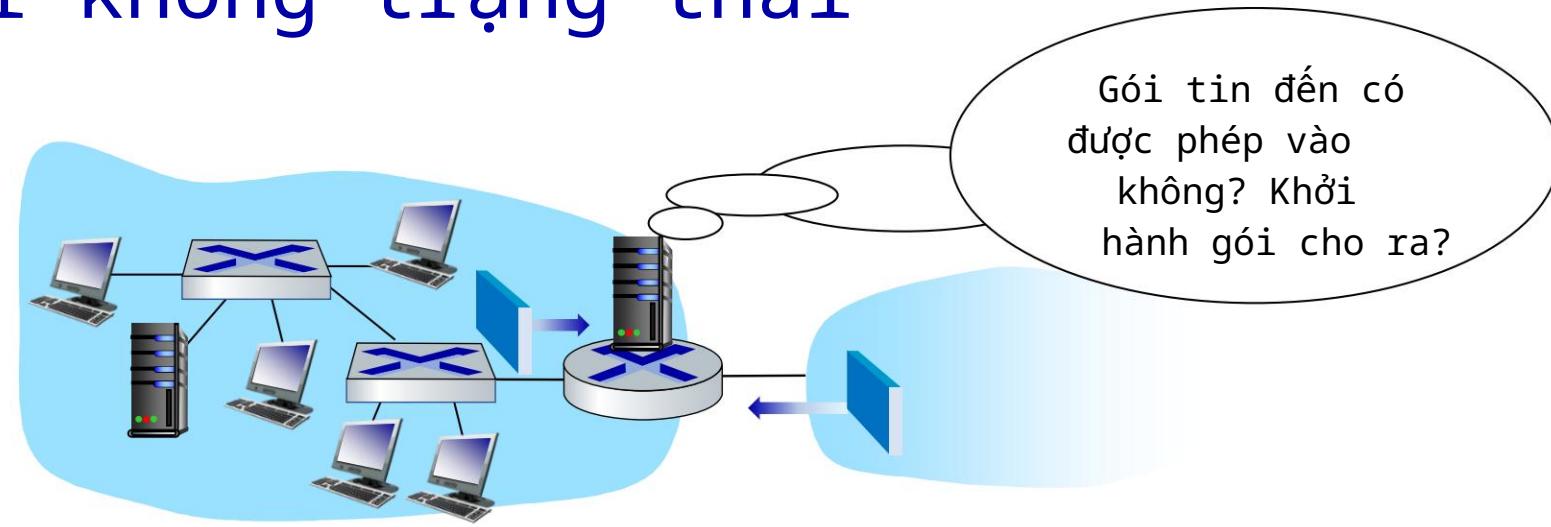
ba loại tường lửa: bộ lọc

gói không trạng thái bộ

lọc gói trạng thái cổng

ứng dụng

Lọc gói không trạng thái

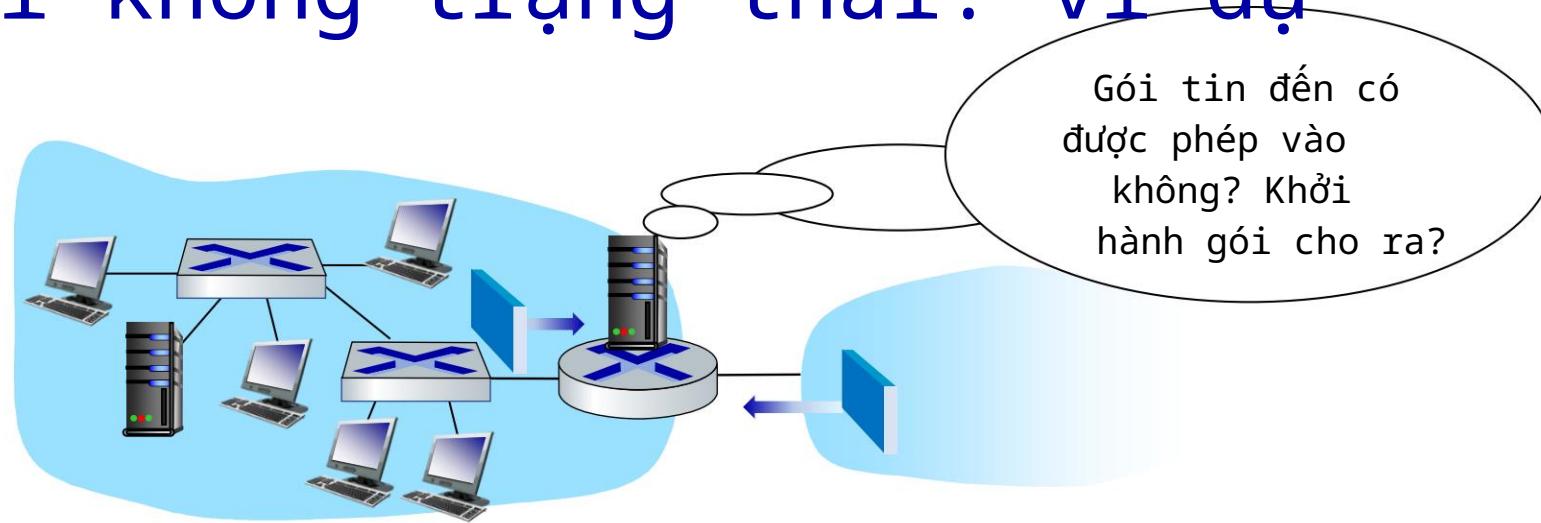


mạng nội bộ được kết nối với Internet thông qua **tường lửa** của bộ định tuyến

lọc **từng gói**, quyết định chuyển tiếp/bỏ gói dựa trên:

- địa chỉ IP nguồn, địa chỉ IP đích • TCP/
UDP nguồn, số cổng đích • Loại thông báo
ICMP • TCP SYN, bit ACK

Lọc gói không trạng thái: ví dụ



ví dụ 1: chặn các datagram đến và đi với trường giao thức IP = 17 và với cổng nguồn hoặc cổng đích = 23 •

kết quả: tất cả các luồng UDP vào, ra và kết nối telnet đều bị chặn

ví dụ 2: chặn các phân đoạn TCP gửi đến với ACK=0 •

kết quả: ngăn máy khách bên ngoài tạo kết nối TCP với máy khách bên trong, nhưng cho phép máy khách bên trong kết nối với bên ngoài

Lọc gói không trạng thái: thêm ví dụ

Chính sách	Cài đặt tường lửa
không có truy cập Web bên ngoài	thả tất cả các gói đi tới bất kỳ địa chỉ IP nào , cổng 80 thả tất cả các
không có kết nối TCP nào đến, ngoại trừ những kết nối chỉ dành cho máy chủ Web công cộng của tổ	gói TCP SYN đến vào bất kỳ IP nào ngoại trừ 130.207.244.203, cổng 80
chức. ngăn Web-radio ăn hết băng thông có sẵn.	loại bỏ tất cả các gói UDP đến - ngoại trừ DNS và bộ định tuyến phát sóng.
ngăn không cho mạng của bạn bị sử dụng cho một cuộc tấn công DoS smurf.	loại bỏ tất cả các gói ICMP đến một địa chỉ "broadcast" (ví dụ: 130.207.255.255) loại bỏ tất cả lưu
ngăn không cho mạng của bạn bị theo dõi	lượng đã hết hạn ICMP TTL

Danh sách kiểm soát truy cập

ACL: bảng quy tắc, được áp dụng từ trên xuống dưới cho các gói đến: (hành động, điều kiện) cặp: trông giống như chuyển tiếp OpenFlow (Ch. 4)!

hoạt động	nguồn Địa chỉ	địa chi đích	giao thức	nguồn Hải cảng	định mệnh Hải cảng	bit cờ
cho phép	222.22/16	bên ngoài của 222.22/16	TCP	> 1023	80	không tí nào
cho phép	bên ngoài của 222.22/16	222.22/16	TCP	80	> 1023 ACK	
cho phép	222.22/16	bên ngoài của 222.22/16	UDP	> 1023	53	---
cho phép	bên ngoài của 222.22/16	222.22/16	UDP	53	> 1023	----
phù nhận	tất cả các	tất cả các	tất cả các	tất cả các	tất cả các	tất cả các

Lọc gói trạng thái

bộ lọc gói không trạng thái: công cụ nặng tay • thửa

nhận các gói “không có ý nghĩa gì”, ví dụ: cổng đích = 80, bit ACK được đặt, mặc dù không có kết nối TCP nào được thiết lập:

hoạt động	địa chỉ nguồn	địa chỉ đích	giao thức	cổng nguồn	cảng đích	bit cờ
cho phép	bên ngoài của 222.22/16	222.22/16	TCP	80	> 1023 ACK	

bộ lọc gói trạng thái: theo dõi trạng thái của mọi kết nối TCP

- thiết lập kết nối theo dõi (SYN), phân tách (FIN): xác định xem liệu đến, các gói gửi đi “có ý nghĩa” • hết

thời gian kết nối không hoạt động tại tường lửa: không còn chấp nhận các gói

Lọc gói trạng thái

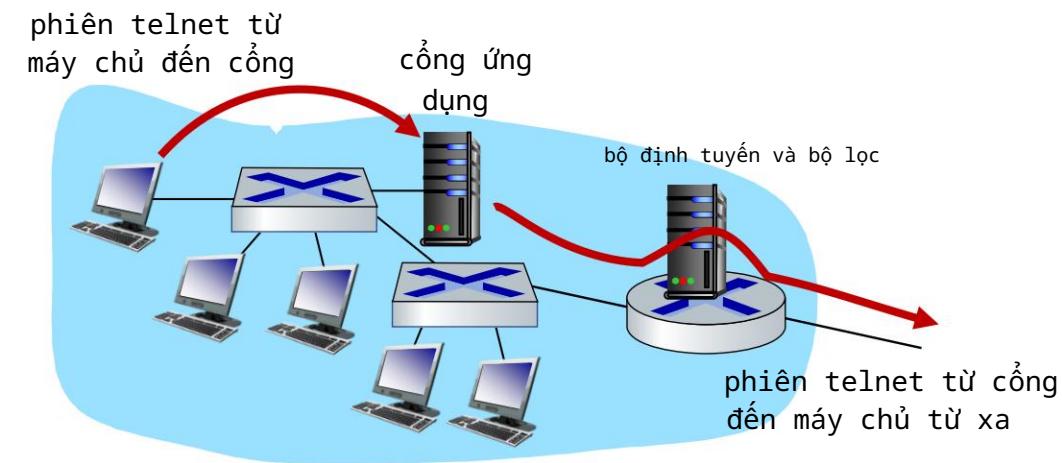
ACL được tăng cường để cho biết cần kiểm tra bảng trạng thái kết nối trước khi nhận gói

hoạt động	địa chỉ nguồn	địa chỉ đích	nguyên thủy	cổng nguồn	cảng đích	bit cờ	kiểm tra kết nối
cho phép	222.22/16	bên ngoài của 222.22/16	TCP	> 1023	80	không tí nào	
cho phép	bên ngoài của 222.22/16	222.22/16	TCP	80	> 1023	xác nhận	X
cho phép	222.22/16	bên ngoài của 222.22/16	UDP	> 1023	53	---	
cho phép	bên ngoài của 222.22/16	222.22/16	UDP	53	> 1023	----	X
phù nhận	tất cả các	tất cả các	tất cả các	tất cả các	tất cả các	tất cả các	

cổng ứng dụng

lọc các gói trên
dữ liệu ứng dụng cũng như
trên các trường IP/TCP/UDP.

ví dụ: cho phép chọn
người dùng nội bộ đến telnet
bên ngoài



1. yêu cầu tất cả người dùng telnet phải telnet qua cổng.
 2. đối với người dùng được ủy quyền, cổng thiết lập kết nối telnet đến máy chủ đích
 - cổng chuyển tiếp dữ liệu giữa 2 kết nối
- bộ định tuyến chặn tất cả các kết nối telnet không bắt nguồn từ cổng

Hạn chế của tường lửa, cổng

Giả mạo IP: bộ định tuyến không thể biết liệu dữ liệu "thực sự" có đến từ nguồn được xác nhận quyền sở hữu hay không

nếu nhiều ứng dụng cần được xử lý đặc biệt , thì mỗi ứng dụng đều có ứng dụng riêng. Cổng vào

phần mềm máy khách phải biết cách liên hệ với cổng , ví dụ: phải đặt

- địa chỉ IP của proxy trong trình duyệt Web

các bộ lọc thường sử dụng chính sách tắt cả hoặc không có gì cho UDP đánh đổi: mức độ giao tiếp với thế giới bên ngoài, mức độ bảo mật nhiều trang web được bảo vệ cao vẫn bị tấn công

Hệ thống phát hiện xâm nhập

lọc gói: • chỉ
hoạt động trên tiêu đề TCP/IP •
không kiểm tra tương quan giữa các phiên

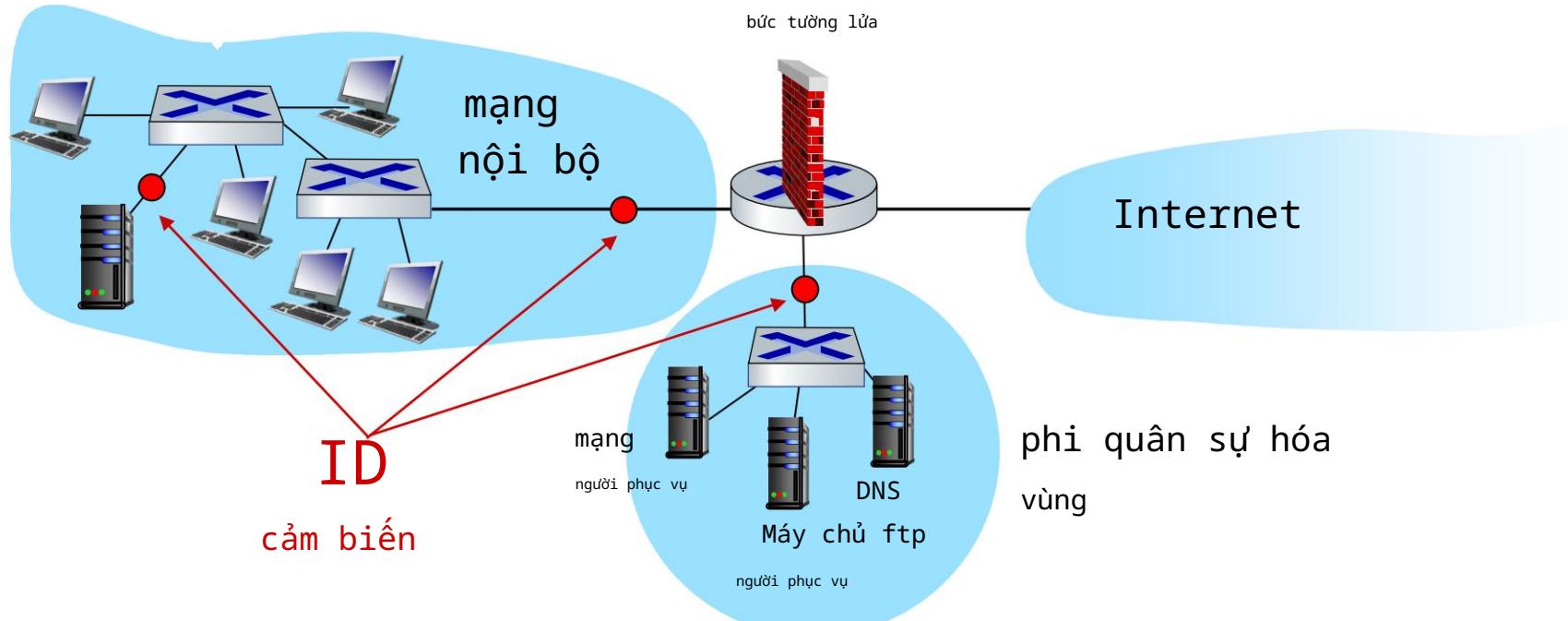
IDS: hệ thống phát hiện xâm nhập •

kiểm tra sâu gói tin: xem xét nội dung gói tin (ví dụ: kiểm tra chuỗi ký
tự trong gói tin so với cơ sở dữ liệu của virus đã biết, chuỗi tấn công)

- kiểm tra mối tương quan giữa nhiều gói tin
 - quét cổng •
 - lập bản đồ mạng •
 - tấn công DoS

Hệ thống phát hiện xâm nhập

nhiều IDS: các loại kiểm tra khác nhau tại các địa điểm khác nhau



An ninh mạng (tổng hợp)

các kỹ thuật cơ bản.....

tính toàn vẹn của thông báo bằng mã hóa
(đối xứng và khóa công khai) xác thực
điểm cuối

.. được sử dụng trong nhiều tình huống bảo mật khác nhau
email bảo mật truyền tải bảo mật (TLS) IP sec



Bảo mật vận

hành 802.11, 4G/5G : tường lửa và IDS