ứng dụng mật mã

AN TOÀN & BẢO MẬT THÔNG TIN

Giảng viên: Ths Phạm Thanh Bình

Bộ môn Kỹ thuật máy tính & mạng

http://dhthuyloi.blogspot.com

Chương 3:

MẬT MÃ KHOÁ CÔNG KHAI VÀ ỨNG DỤNG

- Giới thiệu chung
- Thuật toán mã hoá RSA
- Các hàm Hash và MAC
- Chữ ký số và chứng thực

Bài 3.4 Chữ kí số và chứng thực

- Chữ kí số
- Các giao thức chứng thực

Chữ kí số

- Chữ ký số là một cơ chế chứng thực cho phép tác giả thông điệp gắn thêm một đoạn mã vào thông điệp. Đoạn mã này đóng vai trò như một chữ ký.
- Chữ ký được tạo ra bằng cách tính giá trị hash của thông điệp và mã hóa nó bằng khóa riêng của tác giả.
- Chữ ký bảo đảm về nguồn gốc và tính toàn vẹn của thông điệp

Các tính chất của chữ kí số

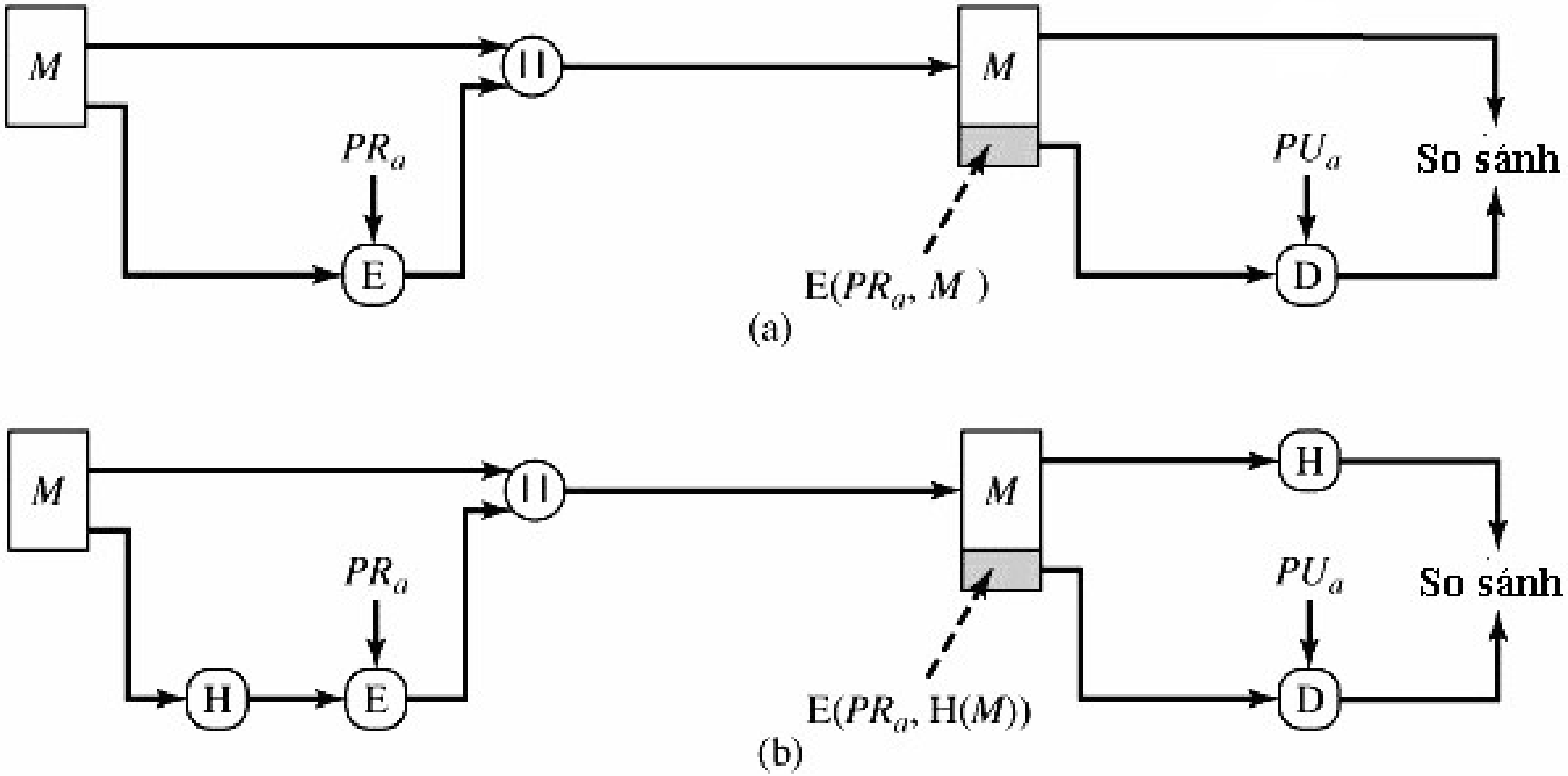
- Phải xác minh được tác giả cùng thời gian của chữ ký.
- Phải chứng thực được nội dung thực sự vào thời gian ký.
- Phải kiểm tra được bởi một bên thứ ba, để giải quyết các tranh chấp.

Có hai loại chữ kí số:

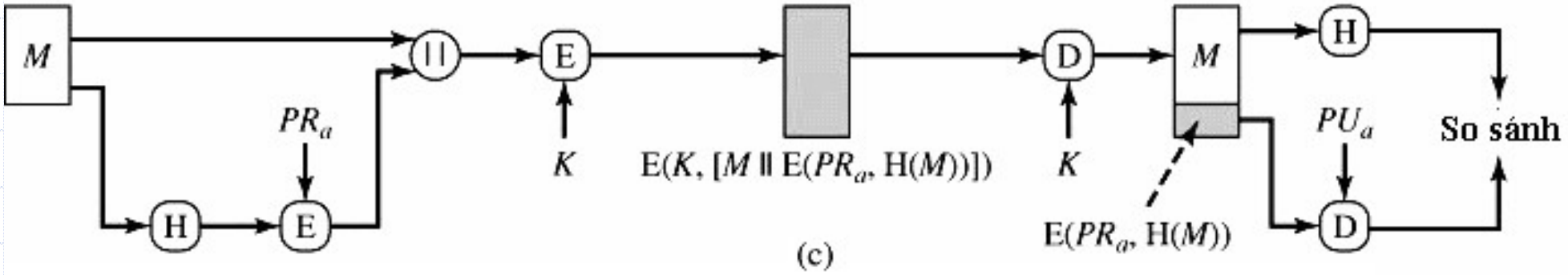
- Chữ kí số trực tiếp
- Chữ kí số trọng tài

Chữ kí số trực tiếp

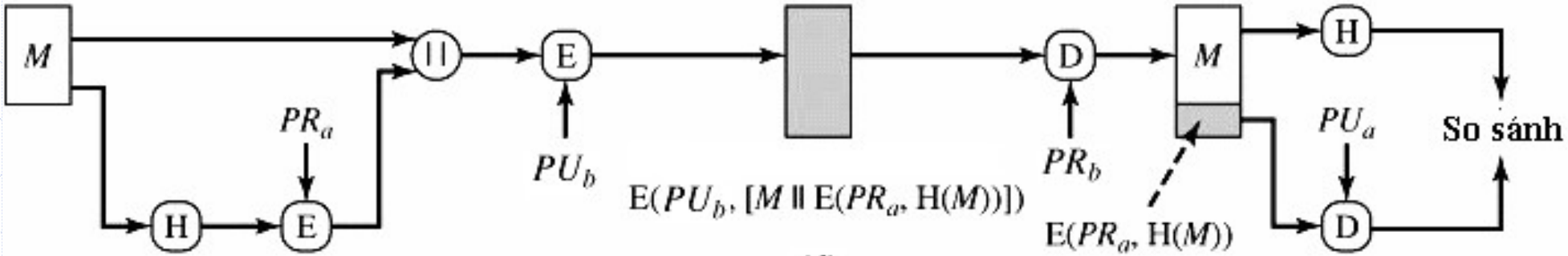
- Loại chữ ký này chỉ liên quan đến hai bên tham gia (nguồn và đích).
- Một chữ ký số có thể tạo ra bằng cách mã hoá toàn bộ thông điệp bằng khoá riêng của người gửi (hình a), hoặc mã hoá mã hash của thông điệp với khoá riêng của người gửi (hình b).


M
PR_a
E
M
PU_a
So sánh
E(PR_a, M)
D
(a)
M
PR_a
H
E
M
H
PU_a
So sánh
E(PR_a, H(M))
D
(b)

- Có thể tăng cường tính bảo mật bằng cách thêm một lần mã hoá toàn bộ thông điệp và chữ ký bằng mật khoá chia sẻ (hình c) , hoặc bằng khoá-công-khai của của người nhận (hình d)


M
PRa
H
E
||
E
K
E(K, [M || E(PRa, H(M))])
D
K
M
H
PUa
So sánh
E(PRa, H(M))
D

(c)


M
PRa
H
E
||
E
PUb
E(PUb, [M || E(PRa, H(M))])
D
PRb
M
H
PUa
So sánh
E(PRa, H(M))
D

(d)

Nhược điểm:

- Chưa ghi lại thời gian phát sinh chữ kí
- Thiếu cơ chế để xử lý khi xảy ra tranh chấp.
- Người gửi có thể đổ lỗi cho kẻ trộm lấy cắp khóa khoá riêng, rồi giả mạo chữ ký của anh ta

Chữ kí số trọng tài

- Những nhược điểm của chữ ký số trực tiếp có thể được giải quyết nhờ vào bên thứ ba tin cậy (trọng tài).
- Giả sử cần gửi thông điệp từ X đến người nhận Y. Trước hết X phải kí vào thông điệp rồi gửi tới trọng tài A.
- A sẽ tiến hành kiểm tra thông điệp và chữ kí, nếu thấy hợp lệ thì sẽ gắn thêm thời gian và nhãn "đã kiểm tra" vào thông điệp, rồi gửi cho Y.

- Trọng tài đóng một vài trò chủ yếu và nhạy cảm trong hình thức này
- Tất cả các bên tham gia đều phải thỏa thuận về sự tin cậy tuyệt đối để cơ chế phân xử thực sự có hiệu quả.

Trọng tài ký xác nhận, chứng minh nó chuẩn sau khi đã hoàn thành quá trình xác nhận

Một số ví dụ về chữ kí số trọng tài

IDx: Tên của X
Kxa: khoá mà X và A biết
Kay: khoá mà A và y biết
Kxy: khoá mà x và y biết
thông điệp M

Ví dụ 1:

Mã hóa đối xứng, trọng tài thấy nội dung thông điệp

nếu IDx trong trùng với ID ngoài: trùng lại đúng
so sánh H(M)khớp nhau: là thông điệp k bị thay đổi, còn nguyên vẹn

X gửi cho trọng tài A 3 trường: công khai được mã hoá

(1) $X \rightarrow A: ID_X || M || E(K_{xa}, [ID_X || H(M)])$

(2) $A \rightarrow Y: E(K_{ay}, [ID_X || M || E(K_{xa}, [ID_X || H(M)]) || T])$

Hạn chế quyền lực trọng tài: cần mã hoá thông điệp M

Y giải mã khi trọng tài gửi thông điệp
Y giải mã: X gửi thông điệp, thông điệp M,Y lưu phần cuối (không đọc được) làm bằng chứng

Biết được, trọng tài kiểm tra thông điệp tại thời điểm T

Y tin tưởng vào trọng tài đã kiểm tra, Y không thể kiểm tra được khoá hay thông điệp

Ký hiệu	Ý nghĩa
X	= người gửi
Y	= người nhận
A	= trọng tài
M	= thông điệp
T	= timestamp, nhãn thời gian để xác định thời gian phát sinh chữ kí

- *Vẽ sơ đồ biểu diễn quá trình thực hiện chữ kí số trọng tài trong Ví dụ 1.*

Nhận xét:

- Cả người gửi và người nhận đều phải tin tưởng tuyệt đối vào trọng tài A
- Nếu A không công tâm, anh ta có thể sửa đổi thông điệp, hoặc thông đồng với X để phủ nhận thông điệp đã kí, hoặc thông đồng với Y để giả mạo chữ kí của X.

Bài tập 1:

- *Hãy đề xuất giải pháp khắc phục nhược điểm của mô hình chữ kí số trong Ví dụ 1?*

Ví dụ 2:

Mã hóa đối xứng, trọng tài không thấy nội dung thông điệp

(1) $X \rightarrow A: ID_X || E(K_{xy}, M) || E(K_{xa}, [ID_X || H(E(K_{xy}, M))])$

(2) $A \rightarrow Y: E(K_{ay}, [ID_X || E(K_{xy}, M)]) || E(K_{xa}, [ID_X || H(E(K_{xy}, M)) || T])$

Nhận xét:

- Cả người gửi và người nhận đều phải tin tưởng tuyệt đối vào trọng tài A
- A không có khả năng sửa đổi thông điệp, nhưng vẫn có thể thông đồng với X để phủ nhận thông điệp đã kí, hoặc thông đồng với Y để giả mạo chữ kí của X.

Bài tập 2:

- *Hãy đề xuất giải pháp khắc phục nhược điểm của mô hình chữ kí số trong Ví dụ 2?*

Một số ví dụ về chữ kí số trọng tài

- **Ví dụ 3:**

Mã hóa khoá-công-khai, trọng tài thấy nội dung thông điệp

(1) X → A: $ID_X || M || E(PR_x, [ID_X || H(M)])$

(2) A → Y: $E(PR_a, [ID_X || M || E(PR_x, [ID_X || H(M)]) || T])$

Nhận xét:

- A biết nội dung thông điệp, nhưng không thể sửa đổi thông điệp hay làm giả chữ kí

Bài tập 3:

- *Hãy đề xuất giải pháp nâng cao tính bảo mật của mô hình chữ kí số trong Ví dụ 3?*

Ví dụ 4:

Mã hóa khoá-công-khai. Trọng tài không thấy nội dung thông điệp

(1) $X \rightarrow A: ID_X || E(PR_x, [ID_X || E(PU_y, E(PR_x, M))])$

(2) $A \rightarrow Y: E(PR_a, [ID_X || E(PU_y, E(PR_x, M)) || T])$

Nhận xét:

- A không biết nội dung thông điệp, không thể sửa đổi thông điệp hay làm giả chữ kí

Bài tập 4:

- Mô hình chữ kí số trong Ví dụ 4 có nhược điểm gì?
- Giải pháp khắc phục như thế nào?

Bài tập 5:

- Vẽ sơ đồ biểu diễn quá trình thực hiện chữ kí số trọng tài trong các ví dụ trên.

Các giao thức chứng thực

- Giao thức là tập hợp các quy tắc để các bên tham gia liên lạc trao đổi thông tin với nhau
- Các giao thức chứng thực cho phép các bên tham gia liên lạc tự nhận dạng lẫn nhau và chuyển giao khoá phiên

Giao thức chứng thực dùng mã hoá đối xứng

- Giữa hai bên liên lạc A và B cần có một bên thứ ba gọi là KDC (Key Distribution Center - Trung tâm phân phối khóa tin cậy)
- Bên A sẽ chia sẻ khoá K_a với KDC
- Bên B sẽ chia sẻ khoá K_b với KDC
- KDC sẽ sinh ra khoá phiên K_s (session key). Ks chỉ tồn tại trong một thời gian ngắn để A và B thực hiện phiên liên lạc.

Giao thức Needham-Schroeder

1. A → KDC: $ID_A||ID_B||N_1$
2. KDC → A: $E(K_a, [K_s||ID_B||N_1||E(K_b, [K_s||ID_A])])$
3. A → B: $E(K_b, [K_s||ID_A])$
4. B → A: $E(K_s, N_2)$
5. A → B: $E(K_s, f(N_2))$

Nhận xét:

- N_1, N_2 là các giá trị nonce (lời gọi), có tác dụng chống tấn công nhại (đối phương chặn một thông điệp, sao chép thông tin, và sau đó gửi nhại chính thông điệp đó đến đích)
- Khi A gửi cho KDC một nonce (N_1), theo quy ước KDC sẽ phải trả lời A bằng một giá trị tương ứng với N_1, nếu không có nghĩa là thông điệp trả lời đã bị giả mạo

- KDC sinh ra khóa phiên K_s rồi gửi cho A
- A gửi thông điệp đã mã hóa (có chứa K_s) cho B
- B gửi lại A một nonce (N_2), chứng tỏ B đã nhận được K_s, và muốn kết nối với A
- A trả lời B bằng một thông điệp có chứa N_2. Phiên kết nối giữa A và B hình thành. Sau đó A và B có thể trao đổi các thông tin được mã hóa bởi K_s

Nhược điểm:

- Chưa có cơ chế kiểm tra thời hạn sử dụng của khóa phiên K_s.
- Nếu kẻ tấn công (bằng cách nào đó) có được một khóa phiên K_s cũ, anh ta có thể dùng nó để đóng giả A nhằm lừa gạt B

Cụ thể:

- Kẻ tấn công (X) lắng nghe và lấy được một thông điệp A gửi cho B ở bước 3 (có chứa khóa phiên cũ mà anh ta đã biết), sao chép thông điệp đó lại để dùng sau này.
- Khi cần tấn công, X chặn một thông điệp A gửi cho B ở bước 3, thay thế nó bằng thông điệp cũ đã lưu, và gửi nhại lại cho B
- Khi B trả lời ở bước 4 (dùng K_s cũ), X chặn thông điệp này và lấy được N_2. Từ đó X có thể đóng giả A để nói chuyện với B

Giải pháp khắc phục:

- Cần gắn thêm nhãn thời gian T để thiết lập thời hạn sử dụng cho khóa phiên (xem giao thức Denning sau đây)

Giao thức Denning

1. A → KDC: $ID_A||ID_B$
2. KDC → A: $E(K_a, [K_s||ID_B||T||E(K_b, [K_s||ID_A||T])])$
3. A → B: $E(K_b, [K_s||ID_A||T])$
4. B → A: $E(K_s, N_1)$
5. A → B: $E(K_s, f(N_1))$

Nhận xét:

- Khóa phiên K_s được gắn kèm với nhãn thời gian T
- B chỉ chấp nhận thông điệp (chứa khóa phiên K_s) ở bước 3 nếu giá trị của nhãn thời gian T đủ gần với thời gian hiện hành của B, bao gồm độ trễ mạng và sai số cho phép
- Đồng hồ của các bên tham gia liên lạc phải được đồng bộ hóa với nhau.

Lưu ý:

- Các giao thức trên chỉ áp dụng cho trường hợp các bên tham gia liên lạc đồng thời online trên mạng (ví dụ dịch vụ Chat)
- Nếu một bên tham gia liên lạc không online (ví dụ dịch vụ Email) thì cần có giải pháp khác

Trường hợp A, B không đồng thời trực tuyến (Chứng thực một chiều)

1. A → KDC: $ID_A||ID_B||N_1$
2. KDC → A: $E(K_a, [K_s||ID_B||N1||E(K_b, [K_s||ID_A])])$
3. A → B: $E(K_b, [K_s||ID_A])||E(K_s, M)$

Nhận xét:

- Phương pháp này không sử dụng nhãn thời gian T nên vẫn có nguy cơ bị tấn công nhại.
- Tuy nhiên, việc xử lý email thường không tức thời, nên người nhận B chủ yếu dùng khoá phiên K_s để giải mã thông điệp M, chứ không dùng K_s để tiếp tục giao tiếp với A.

Giao thức chứng thực dùng mã hoá khoá công khai (của Denning)

- Giữa hai bên liên lạc A và B cần có một bên thứ ba gọi là AS (Authentication Server – Server chứng thực)
- AS không sinh ra khoá phiên K_s mà sẽ đưa ra "chứng chỉ" khoá công khai
- Khóa phiên được chọn và mã hóa bởi A

1. A → AS: $ID_A||ID_B$
2. AS → A: $E(PR_{as}, [ID_A||PU_a||T])||E(PR_{as}, [ID_B||PU_b||T])$
3. A → B: $E(PR_{as}, [ID_A||PU_a||T])||E(PR_{as}, [ID_B||PU_b||T])||E(PU_b, E(PR_a, [K_s||T]))$

Nhận xét:

- AS sinh ra chứng chỉ khoá công khai (chứa khoá công khai của người dùng), mỗi chứng chỉ chỉ có hiệu lực trong khoảng thời gian T
- Khi A nhận được chứng chỉ do AS gửi, A sẽ biết được khoá công khai của B, và dùng nó để chuyển giao khoá phiên K_s cho B
- Khoá phiên được mã hoá 2 lần: Lần 1 bởi PR_a để chứng thực, lần 2 bởi PU_b để giữ bí mật

Hết Phần 3_3