On tap An toan thong tin CK

Hệ thống thông tin kế toán (Đại học Vinh)

ÔN TẬP AN TOÀN THÔNG TIN

Cấu trúc đề thi cuối kỳ:
Câu 1 (3 điểm): (Câu 1 □ 5)
Câu 2 (3 điểm): (Dạng câu 6,7) (Chữ ký điện tử RSA hoặc trao đổi khóa diffie-hellman)
Câu 3 (2 điểm): (Câu 8 □ 13)
Câu 4 (2 điểm): (Câu 14 □ 20)

Câu 1:

Trung tâm tin học của ngành công nghệ thông tin có nhiệm vụ đào tạo các khóa học ngắn hạn về CNTT cho các sinh viên của trường. Hiện nay trung tâm có một website http://www.ttth.vinhuni.edu.vn để sinh viên xem, đăng ký và thanh toán học phí các khóa học qua website. Sau khi thi xong sinh viên cũng có thể xem kết quả của các khóa học qua websitenày. Khi đăng ký học các khóa học sinh viên phải cung cấp đầy đủ thông tin cá nhân để trung tâm lưu trữ quản lý. Khi thanh toán học phí trực tuyến sinh viên phải cung cấp thông tin về thẻngân hàng thanh toán và được xác thực thông qua điện thoại. Thông tin các khóa học cũng đượcwebsite cung cấp cho sinh viên tham khảo và chọn lựa. Giáo viên sau khi giảng dạy thì nhập các kết quả thi của sinh viên thông qua website bằng tài khoản người dùng trên website.

Hãy nêu và giải thích tính bí mật, tính sẵn sàng, tính toàn vẹn, tính chống chối bỏ của an toànHTTT đối với website của trung tâm.

Bài làm

-**Tính bí mật của hệ thống thông tin:** Bảo vệ dữ liệu để không bị lộ ra ngoài trái phép. Trong hệ thống quản lý thì thông tin cá nhân của sinh viên được lưu trữ và Khi thanh toán học phí trực tuyến sinh viên phải cung cấp thông tin về thẻ ngân hàng thanh toán và được xác thực thông qua điện thoại

-**Tính toàn vẹn:** Chỉ những người dùng được ủy quyền mới được phép chỉnh sửa dữ liệu.

Giáo viên sau khi giảng dạy thì nhập các kết quả thi của sinh viên thông qua website bằng tài khoản người dùng trên website

-**Tính sẵn sàng:** Đảm bảo dữ liệu luôn sẵn sàng khi những người dùng hoặc ứng dụng được ủy quyền yêu cầu

Sinh viên có thể xem, đăng kí, thanh toán học phí và thông tin các khóa học cũng đc website cung cấp cho sinh viên tham khảo và chọn lựa, có thể xem kết quả của các khóa học qua website

-**Tính chống đối:** Khả năng ngăn chặn việc từ chối một hành vi đã làm

Khi thanh toán học phí trực tuyến sinh viên phải cung cấp thông tin về thẻ ngân hàng thanh toán và được xác thực thông qua điện thoại.

Câu 2:

Nhà ăn của trường Đại học Vinh có một Website ĐẶT THỰC ĐƠN CÁC MÓN ĂN TRỰC TUYẾN (http://www.cantin.vinhuni.edu.vn) nhằm giúp cho các nhân viên, giáo viên và sinh viên (gọi chung là khách hàng) của trường có thể tìm và đặt thực đơn các món ăn cho bữa ăn sáng/trưa/tối thông qua website và thức ăn sẽ được giao tới tận phòng/khoa của khách hàng màkhách hàng yêu cầu. Website có hiển thị danh mục và

giá cả của các món ăn để khách hàng tham khảo. Để có thể đặt các món ăn, khách hàng phải đăng ký làm thành viên của Website. Để đăng ký thành viên thì khách hàng phải cung cấp thông tin cá nhân như họ tên, số điện thoại, địa chỉ email, mã số giáo viên/mã sinh viên để hệ thống lưu trữ và quản lý. Khi đặt món khách hàng có thể thanh toán đơn đặt hàng trực tuyến hoặc trả tiền mặt ngay khi nhận các món ăn. Khi thanh toán thực đơn trực tuyến khách hàng phải cung cấp thông tin về thẻ ngân hàng thanh toán và được xác thực thông qua điện thoại.

Hãy nêu và giải thích tính bí mật, tính sẵn sàng, tính toàn vẹn, tính chống chối bỏ của an toànHTTT đối với website nhà ăn

Bài làm

-**Tính bí mật của hệ thống thông tin:** Bảo vệ dữ liệu để không bị lộ ra ngoài trái phép.
Khách hàng chỉ xem được các món mà mình đã đặt nhưng không thể xem các món người khác đặt, Khách hàng cung cấp thông tin cá nhân như họ tên số điện thoại địa chỉ email, mã số sinh viên/giáo viên để hệ thống lưu trữ và quản lý
Để đặt hàng thì khách hàng phải đăng kí thành viên
-**Tính toàn vẹn:** Chỉ những người dùng được ủy quyền mới được phép chỉnh sửa dữ liệu.
Hệ thống quản lý không cho phép khách hàng thay đổi hóa đơn của khách hàng
Khi thanh toán thực đơn trực tuyến khách hàng phải cung cấp thông tin về thẻ ngân hàng thanh toán và được xác thực thông qua điện thoại
-**Tính sẵn sàng:** Đảm bảo dữ liệu luôn sẵn sàng khi những người dùng hoặc ứng dụng
Hệ thống đưa ra danh mục và giá cả các món ăn để khách hàng tham khảo
Khi đặt món khách hàng có thể thanh toán trực tiếp tiền mặt hoặc trực tuyến
-**Tính chống đối:** Khả năng ngăn chặn việc từ chối một hành vi đã làm
Khi khách hàng đã thanh toán hóa đơn thì không thể hủy bỏ đơn hàng của mình

Câu 3:

Đường sắt Việt Nam sử dụng website www.dsvn.vn để giúp hành khách đặt và mua vé trực tuyến. Thông qua website, các nhà ga quản lý được quá trình bán, mua vé của người dân cũngnhư thể hiện các tính ưu việt khác thông qua các nghiệp vụ điều hành. Website hiển thị các thông tin cần thiết mà khách hàng mong muốn: tuyến tàu, giá vé, thời gian chạy, thời gian đến, tình trạng số chỗ cho mỗi toa ... Để có thể đặt vé, hành khách truy cập vào website và tra cứu thông tin: chọn ngày đi, ga đi, ga đến, thời gian phù hợp, loại ghế ... cũng như bắt buộc phải cung cấp đúng thông tin cá nhân: họ tên người đi, thông tin giấy tờ tùy thân (số CMND hoặc thẻ căn cước, số hộ chiếu ...), năm sinh và một số thông tin bổ sung khác. Khách hàng cũng có thể thanh toán trực tuyến hoặc thanh toán tại các địa điểm chỉ định (ngân hàng, nhà ga, đại lý, các điểm thu hộ ...). Quản lý ga/nhân viên tùy theo chức năng, nhiệm vụ được giao thực hiện
Hãy nêu và giải thích tính bí mật, tính sẵn sàng, tính toàn vẹn, tính chống chối bỏ của an toàn HTTT đối với website Đường sắt Việt Nam.

Bài làm

-**Tính bí mật của hệ thống thông tin:** Bảo vệ dữ liệu để không bị lộ ra ngoài trái phép.
Dữ liệu thông tin cá nhân của khách hàng được lưu trữ và bảo mật
Thông tin ngày đi ngày đến ga đi ga đến loại ghế… chỉ khách hàng được biết
-**Tính toàn vẹn:** Chỉ những người dùng được ủy quyền mới được phép chỉnh sửa dữ

liệu.
Khách hàng không được phép thay đổi thông tin chuyến đi của mình đã đặt vé
Quản lý ga/nhân viên tùy theo chức năng, nhiệm vụ được giao thực hiện 2 các thao tác nghiệp vụ liên quan đến quy định đặt chỗ, bán vé, hủy vé, đổi ngày, cập nhật thông tin liên quan đến giá vé, giảm giá, các ưu đãi, khuyến cáo ... cũng thông qua cổng thông tin này
-**Tính sẵn sàng:** Đảm bảo dữ liệu luôn sẵn sàng khi những người dùng hoặc ứng dụng Website hiển thị các thông tin cần thiết mà khách hàng mong muốn: tuyến tàu, giá vé, thời gian chạy, thời gian đến, tình trạng số chỗ cho mỗi toa ...
Khách hàng cũng có thể thanh toán trực tuyến hoặc thanh toán tại các địa điểm chỉ định (ngân hàng, nhà ga, đại lý, các điểm thu hộ ...).
-**Tính chống đối:** Khả năng ngăn chặn việc từ chối một hành vi đã làm
2 thao tác nghiệp vụ liên quan đến quy định đặt chỗ, bán vé, hủy vé, đổi ngày, cập nhật thông tin liên quan đến giá vé, giảm giá, các ưu đãi, khuyến cáo của nhân viên và quản lý các thao tác nghiệp vụ liên quan đến quy định đặt chỗ, bán vé, hủy vé, đổi ngày, cập nhật thôngtin liên quan đến giá vé, giảm giá, các ưu đãi, khuyến cáo ... cũng thông qua cổng thông tin này.

Câu 4:

Ngân hàng Vietcombank là một ngân hàng chuyên cung cấp cho khách hàng đầy đủ các dịch vụ tài chính hàng đầu trong lĩnh vực thương mại quốc tế; trong các hoạt động truyền thống như kinh doanh vốn, huy động vốn, tín dụng, tài trợ dự án…cũng như mảng dịch vụ ngân hàng hiện đại: kinh doanh ngoại tệ và các công vụ phái sinh, dịch vụ thẻ, ngân hàng điện tử…

Sở hữu hạ tầng kỹ thuật ngân hàng hiện đại, Vietcombank có nhiều lợi thế trong việc ứng dụng công nghệ tiên tiến vào xử lý tự động các dịch vụ ngân hàng, phát triển các sản phẩm, dịch vụ ngân hàng điện tử dựa trên nền tảng công nghệ cao. Không gian giao dịch công nghệ số (Digital lab) cùng các dịch vụ: VCB Internet Banking, VCB Money, SMS Banking, Phone Banking,…đã, đang và sẽ tiếp tục thu hút đông đảo khách hàng bằng sự tiện lợi, nhanh chóng, an toàn, hiệu quả, tạo thói quen thanh toán không dùng tiền mặt cho đông đảo khách hàng.

Hãy nêu và giải thích tính bí mật, tính sẵn sàng, tính toàn vẹn, tính chống chối bỏ của an toàn HTTT đối với công ty/doanh nghiệp được mô tả ở trên.

Bài làm

- **Tính bí mật của hệ thống thông tin:** Bảo vệ dữ liệu để không bị lộ ra ngoài trái phép.

Không gian giao dịch công nghệ số (Digital lab) cùng các dịch vụ: VCB Internet Banking, VCB Money, SMS Banking, Phone Banking,…đã, đang và sẽ tiếp tục thu hút đông đảo khách hàng bằng sự tiện lợi, nhanh chóng, an toàn, hiệu quả, tạo thói quen thanh toán không dùng tiền mặt cho đông đảo khách hàng

- **Tính toàn vẹn:** Chỉ những người dùng được ủy quyền mới được phép chỉnh sửa dữ liệu.

Khách hàng không có quyền tự thay đổi các giao dịch

- **Tính sẵn sàng:** Đảm bảo dữ liệu luôn sẵn sàng khi những người dùng hoặc ứng dụng

Có đầy đủ các ứng dụng VCB Internet Banking, VCB Money, SMS Banking, Phone Banking…khách hàng có thể tự hoàn thành những giao dịch ngay trên các ứng dụng một cách nhanh chóng an toàn và hiệu quả

- **Tính chống đối:** Khả năng ngăn chặn việc từ chối một hành vi đã làm

Tất cả các giao dịch của khách hàng trên hệ thống ứng dụng của VCB đều được lưu lại một cách chi tiết nhất

Câu 5:

Bệnh viện Hồng Đức là một trong những bệnh viện tốt nhất tại Việt Nam. Hàng năm, Hồng Đức khám và điều trị cho hàng trăm ngàn bệnh nhân, hơn 5.000 bệnh nhân nội trú và phẫu thuật nội soi hơn 2.000 ca. Tính đến thời điểm hiện tại Hồng Đức đã đạt được nhiều thành tựu trong việc khám và điều trị bệnh cho bệnh nhân. Không ngừng nỗ lực để phục vụ cộng đồng tốt hơn và để đáp ứng nhu cầu của xã hội. Bệnh viện được trang bị đồng bộ với kỹ thuật và công nghệ y khoa hiện đại nhất, đáp ứng các yêu cầu chẩn đoán, điều trị theo phương pháp mới cũng như các kỹ thuật cao cấp. Đặc biệt bệnh viện đã áp dụng tối đa hệ thống thông tin vào tất cả các hoạt động của bệnh viện từ việc quản lý nhân viên, bệnh nhân, thiết bị đến việc xử lý các quy trình nghiệp vụ như đăng ký khám bệnh trực tuyến, khám bệnh và điều trị bệnh từ xa, điều trị bệnh, mổ, xét nghiệm, nội soi, thanh toán viện phí trực tuyến, liên kết với các công ty bảo hiểm trong việc điều trị cho các bệnh nhân có mua bảo hiểm…

Hãy nêu và giải thích tính bí mật, tính sẵn sàng, tính toàn vẹn, tính chống chối bỏ của an toàn HTTT đối với công ty/doanh nghiệp được mô tả ở trên

Bài làm

- **Tính bí mật của hệ thống thông tin:** Bảo vệ dữ liệu để không bị lộ ra ngoài trái phép.

Người ngoài không thể xem được kết quả khám bệnh và điều trị của bệnh nhân

- **Tính toàn vẹn:** Chỉ những người dùng được ủy quyền mới được phép chỉnh sửa dữ liệu.

Bệnh nhân không thể chỉnh sửa kết quả khám và điều trị

- **Tính sẵn sàng:** Đảm bảo dữ liệu luôn sẵn sàng khi những người dùng hoặc ứng dụng

Các hoạt động của bệnh viện từ việc quản lý nhân viên, bệnh nhân, thiết bị đến việc xử lý các quy trình nghiệp vụ như đăng ký khám bệnh trực tuyến, khám bệnh và điều trị bệnh từ xa, điều trị bệnh, mổ, xét nghiệm, nội soi, thanh toán viện phí trực tuyến, liên kết với các công ty bảo hiểm trong việc điều trị cho các bệnh nhân có mua bảo hiểm

- **Tính chống đối:** Khả năng ngăn chặn việc từ chối một hành vi đã làm

Hồ sơ bệnh án và các thông tin liên quan đến bệnh nhân đều được ghi lại và lưu trữ

Câu 6:

Hãy trình bày quá trình tạo chữ ký số theo cơ chế RSA khi Alice muốn gửi thông điệp M đến Bob với giá trị băm của M là 15, p=23, q=11, e=19.

* Tạo cặp khóa

Có p=23, q=11 => n=p*q=23*11=253

Phi(n) = (p-1) * (q-1) = (23-1) * (11-1) = 220

Vì GCD(19, 220) = 1

⇨ d = e ^-1(mod phi(n))

Áp dụng thuật toán ơ clid mở rộng ta có

m	a	r	q	y0	y1	y
220	19	11	11	0	1	-11
19	11	8	1	1	-11	12
11	8	3	1	-11	12	-23
8	3	2	2	12	-23	58
3	2	1	1	-23	58	-81
2	1	0	.	.	.	.

⇨ d = -81 + 220 = 139

Vậy ta có:

PR(139,253), PU(19,253)

* Ký số

S = Sigk = M^d(mod n)

= 15^139 (mod 253)

Áp dụng thuật toán lũy thừa nhanh ta có

Đổi 1392 = 1000 1011

b[i]	p = p^2	p = p mod 253	p*x	p = mod 253
1	1^2=1	1	1*15=15	15
0	15^2=225	225	-	225
0	225^2=50625	25	-	25
0	25^2=625	119	-	119
1	119^2=14161	246	246*15=3690	148
0	148^2=21904	146	-	146
1	146^2=21316	64	64*15=960	201
1	201^2=40401	174	174*15=2610	80

⇨ s = 80

* Kiểm tra chữ ký:

Ver(M, S) = TRUE

⇔ M = S ^ e (mod n)

⇔ 15 = 80 ^ 19 (mod 253)

Áp dụng thuật toán lũy thừa nhanh ta có:

Đổi 192 = 10011

b[i]	p = p^2	p = p mod 253	p*x	p = mod 253
1	1^2=1	1	1*80=80	80
0	80^2=6400	75	-	75
0	75^2=5625	59	-	59
1	59^2=3481	192	192*80=15360	180
1	180^2=32400	16	16*80=1280	15

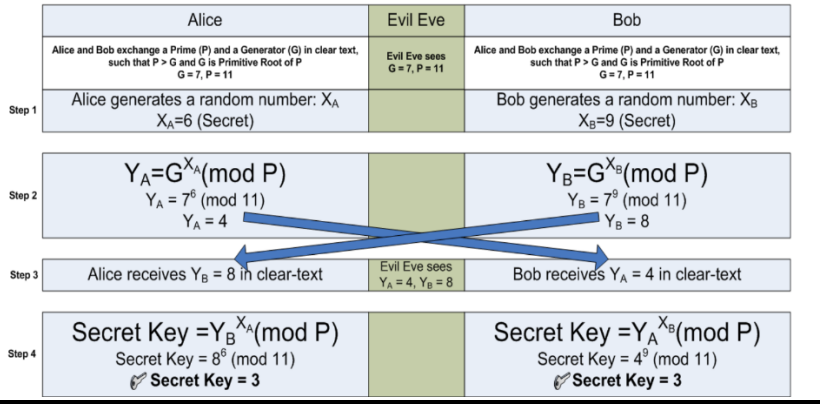
⇨ S ^ e (mod n)

⇔ 80 ^ 19 (mod 253) = 15

Vậy chữ ký là đúng

Câu 7: Giả sử Alice và Bob thống nhất với nhau chọn số nguyên tố p = 11 và g = 7. Alice chọnmột giá trị ngẫu nhiên bất kỳ x = 13 và bí mật x. Bob chọn một giá trị ngẫu nhiên bất kỳ y = 17 và bí mật y. Hãy trình bày quá trình tạo và trao đổi khóa phiên giữa Alice và Bob.

Giải:



	Alice	Evil Eve	Bob
	P = 11, G = 7	P =11 G = 7	P = 11, G = 7
Step1	X=13		Y=17
Step2	YA = G^X(mod P) YA = 7^13 (mod 11) = 2		YB = G^Y (mod P) YB = 7^17 (mod 11) = 6
Step3	Alice nhận YB = 6	YA=2 YB=6	Bob nhận YA = 2
Step4	Secret Key = YB ^X(mod P) = 6^13 (mod 11) = 7		Secret Key = YA ^ Y (mod P) = 2^17 (mod 11) = 7

Câu 8:

*** Trình bày thuật toán RSA. Cho biết ưu và nhược điểm của RSA**

Thuật toán RSA:

1. Chọn hai số nguyên tố lớn p và q và tính $N = pq$. Cần chọn p và q sao cho:

$M < 2^{i-1} < N < 2^i$. Với $i = 1024$ thì N là một số nguyên dài khoảng 309 chữ số.

2. Tính $\phi(n) = (p - 1)(q - 1)$

3. Tìm một số e sao cho e nguyên tố cùng nhau với $\phi(n)$

$$UCLN(e, \phi(n)) = 1 \qquad 1 < e < \phi(n)$$

4. Tìm một số d sao cho $e.d \equiv 1 \bmod \phi(n)$ (d là nghịch đảo của e trong phép modulo n)

5. Hủy bỏ n, p và q. Chọn khóa công khai K_U là cặp (e, N), khóa riêng K_R là cặp (d, N)

6) Việc mã hóa thực hiện theo công thức:
   - Theo phương án 1, mã hóa bảo mật: $C = E(M, K_U) = M^e \bmod N$
   - Theo phương án 2, mã hóa chứng thực: $C = E(M, K_R) = M^d \bmod N$

7) Việc giải mã thực hiện theo công thức:
   - Theo phương án 1, mã hóa bảo mật: $\bar{M} = D(C, K_R) = C^d \bmod N$
   - Theo phương án 2, mã hóa chứng thực: $\bar{M} = D(C, K_U) = C^e \bmod N$

Bản rõ M có kích thước $i-1$ bít, bản mã C có kích thước i bít.

Ưu điểm:

+ Đơn giản trong việc lưu chuyển khóa: Chỉ cần đăng ký một khóa công khai => mọi người sẽ lấy khóa này để trao đổi thông tin với người đăng ký => không cần thêm kênh bí mật truyền khóa.

+ Mỗi người chỉ cần một cặp khóa (PR, PU) là có thể trao đổi thông tin với tất cả mọi người.

+ Là tiền đề cho sự ra đời của chữ ký số và các phương pháp chứng thực điện tử

Nhược điểm:

- Tốc độ xử lý

+ Các giải thuật khóa công khai chủ yếu dùng các phép nhân chậm hơn nhiều so với các giải thuật đối xứng

+ Không thích hợp cho mã hóa thông thường

+ Thường dùng trao đổi khóa bí mật đầu phiên truyền tin

- Tính xác thực của khóa công khai

+ Bất cứ ai cũng có thể tạo ra một khóa công khai

+ Chừng nào việc giả mạo chưa bị phát hiện có thể đọc được nội dung các thông báo gửi cho người kia

+ Cần đảm bảo những người đăng ký khóa là đáng tin

*** Nêu nguyên tắc của mã hóa khóa công khai? Tại sao trong mã hóa khóa công khai không cần dùng đến kênh an toàn để truyền khóa?**

Mật mã hóa khóa công khai là một dạng mật mã hóa cho phép người sử dụng trao đổi các thông tin mật mà không cần phải trao đổi các khóa chung bí mật trước đó. Điều này được thực hiện bằng cách sử dụng một cặp khóa có quan hệ toán học với nhau là khóa công khai và khóa bí mật *(theo Wikipedia)*. Do đó, Mã hóa khóa công khai sinh ra để xử lý nhược điểm về truyền tải khóa chung của Mã hóa đối xứng

Câu 9: Khóa là gì? Trong các hệ thống mã hóa, có các loại khóa nào? Hãy liệt kê tên (tiếng anh và tiếng việt), đặc điểm chính, đóng vai trò gì trong từng loại hệ thống mã hóa. Tạisao cần giữ bí mật khóa chỉ có người gửi và người nhận biết?

Bài làm

- Khóa (key) được sử dụng trong quá trình mã hóa và giải mã

- Mã hóa công khai - Mã hóa cổ điển - Mã hoá đối xứng - Mã hoá bất đối xứng

+ **Mã hóa cổ điển** (classical cryptographic) dựa trên kỹ thuật thay thế (thay thế kí tự hoặc các kí tự này bằng kí tự hoặc các kí tự khác tương ứng) và hoán vị (thay đổi trật tự, vị trí các ký tự) trong văn bản gốc. Các kỹ thuật này có thể áp dụng đối với một ký tự (monoalphabetic) hoặc nhiều ký tự (polyalphabetic) tùy vào mục đích sử dụng.

Một số hệ mã cổ điển

- Mã hóa Caesar
- Mã hóa đơn bảng
- Mã hóa Affine
- Mã hóa Vigenère
- Mã hóa Playfair
- Mã hóa Hill
- Mã hàng rào sắt

+ **Mã hoá đối xứng** Là những hệ mật được sử dụng chung 1 khóa trong quá trình mã hóa và mã hóa. Do đó khóa phải được giữ bí mật tuyệt đối.

Một số hệ mật mã khóa đối xứng hiện đại mà mình thấy hay được sử dụng là DES, AES, RC4, RC5,...

Hệ mật sẽ bao gồm:

- Bản rõ (plaintext-M): bản tin được sinh ra bởi bên gửi
- Bản mật (ciphertext-C): bản tin che giấu thông tin của bản rõ, được gửi tới bên nhận qua một kênh không bí mật
- Khóa (Ks): nó là giá trị ngẫu nhiên và bí mật được chia sẻ giữa các bên trao đổi thông tin và được tạo ra từ:

    - Bên thứ 3 được tin cậy tạo và phân phối tới bên gửi và bên nhận
    - Hoặc, bên gửi tạo ra và chuyển cho bên nhận
- Mã hóa (encrypt-E): C = E(KS, M)
- Giải mã (decrypt): M = D(KS, C) = D(KS, E(KS, M))

Cơ chế hoạt động (dễ hiểu lắm)

- Người gửi sử dụng khóa chung (Ks) để mã hóa thông tin rồi gửi cho người nhận.
- Người nhận nhận được thông tin đó sẽ dùng chính khóa chung (Ks) để giải mã.

+ Hệ mật mã khóa bất đối xứng

Ở hệ mật này thay vì người dùng dùng chung 1 khóa như ở hệ mật mã khóa đối xứng thì ở đây sẽ dùng 1 cặp khóa có tên là public key và private key.

Hệ mật mã khóa bất đối xứng mình thấy được dùng nhiều nhất là RSA

Hệ mật sẽ bao gồm:

- Bản rõ (plaintext-M): bản tin được sinh ra bởi bên gửi
- Bản mật (ciphertext-C): bản tin che giấu thông tin của bản rõ, được gửi tới bên nhận qua một kênh không bí mật
- Khóa: Bên nhận có 1 cặp khóa:
    - Khóa công khai (Kub) : công bố cho tất cả mọi người biết (kể cả hacker)
    - Khóa riêng (Krb) : bên nhận giữ bí mật, không chia sẻ cho bất kỳ ai
- Mã hóa (encrypt-E): C = E(Kub, M)
- Giải mã (decrypt): M = D(Krb, C) = D(Krb, E(Kub, M))

Yêu cầu đối với cặp khóa (Kub, Krb) là:

- Hoàn toàn ngẫu nhiên
- Có quan hệ về mặt toán học 1-1.
- Nếu chỉ có giá trị của Kub không thể tính được Krb.
- Krb phải được giữ mật hoàn toàn.

Cơ chế hoạt động (cũng dễ hiểu không kém đối xứng)

- Người gửi(A) gửi thông tin đã được mã hóa bằng khóa công khai (Kub) của người nhận(B) thông qua kênh truyền tin không bí mật
- Người nhận(B) nhận được thông tin đó sẽ giải mã bằng khóa riêng (Krb) của mình.
- Hacker cũng sẽ biết khóa công khai (Kub) của B tuy nhiên do không có khóa riêng (Krb) nên Hacker không thể xem được thông tin gửi

Câu 10: Mã hóa bất đối xứng dùng 2 khóa khác nhau cho 2 quá trình mã hóa và giải mã.Trìnhbày (có giải thích) việc dùng phương pháp mã hóa bất đối xứng để giải quyết bài toán?

a. Bảo mật dữ liệu.

b. Chứng thực nguồn gốc thông điệp

(chú ý trả lời ai là người tạo khóa)

Bài làm

Mã hóa bất đối xứng

Đây là loại hình mã hóa ra đời sau mã hóa đối xứng và còn được gọi là công nghệ mã hóa public-key:

a. Bảo mật dữ liệu.

- Mã hóa bất đối xứng được cho là an toàn hơn mã hóa đối xứng vì nó sử dụng 2 key riêng biệt cho 2 quy trình mã hóa và giải mã.
- Public key được sử dụng để mã hóa sẽ được công khai, nhưng private key để giải mã là hoàn toàn bí mật.
- Phương pháp mã hóa này được sử dụng trong các giao tiếp hàng ngày qua internet.
- Khi một tin nhắn được mã hóa bằng public key, nó chỉ có thể được giải mã bằng private key. Tuy nhiên, khi một tin nhắn được mã hóa bằng private key, nó có thể được giải mã bằng public key.

b. Chứng thực nguồn gốc thông điệp

- Chứng chỉ kỹ thuật số trong mô hình máy khách-máy chủ có thể được sử dụng để tìm thấy các public key.
- Điểm hạn chế của mã hóa bất đối xứng là mất nhiều thời gian thực hiện hơn so với mã hóa đối xứng.
- Các kỹ thuật mã hóa bất đối xứng phổ biến bao gồm RSA, DSA và PKCS.

Câu 11:

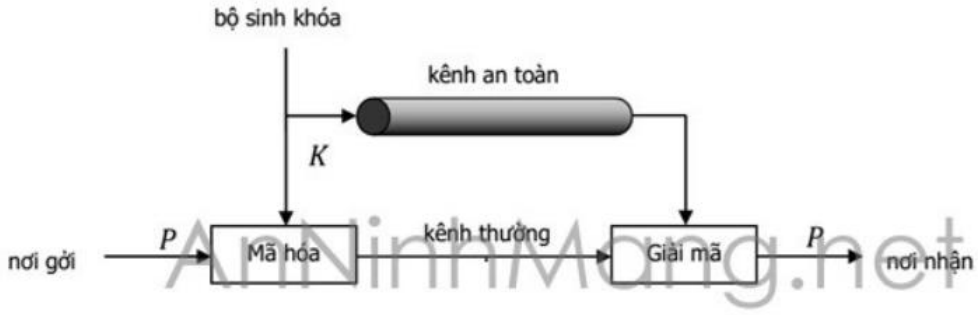
+ Hệ mã hóa đối xứng là gì? vẽ mô hình cơ bản và cho biết các thành phần cơ bản của mã hóa đối xứng? Trình bày ưu điểm và hạn chế của hệ mã đối xứng

+ Định nghĩa mã hóa đối xứng, vẽ mô hình cơ bản và cho biết các thành phần cơ bản của mã hóa đối xứng.

Bài làm

Hệ thống mã hóa đối xứng (Symmetric cryptosystem) là hệ thống mã hóa sử dụng một khóa bí mật chia sẻ (shared-secret-key) cho cả hai quá trình mã hóa và giải mã.

Hình 1: Mô hình mã hóa đối xứng



Mô hình trên gồm 5 yếu tố:

Bản rõ P (plaintext)

- Thuật toán mã hóa E (encrypt algorithm)
- Khóa bí mật K (secret key)
- Bản mã C (ciphertext)
- Thuật toán giải mã D (decrypt algorithm)

Trong đó: C = E (P, K) và P = D (C, K)

Thuật toán mã hóa và giải mã sử dụng chung một khóa, thuật toán giải mã là phép toán ngược của thuật toán mã hóa.

Vì vậy mô hình trên được gọi là phương pháp mã hóa đối xứng

Ưu điểm: độ an toàn cao (phụ thuộc vào thuật toán và khóa), quá trình mã hóa và giải mã nhanh do đó mã hóa đối xứng được sử dụng phổ biến trong việc truyền dữ liệu.

Ưu điểm: Một số vấn đề cần quan tâm của hệ thống mã hóa đối xứng liên quan đến khóa, bao gồm:

+ Do quá trình mã hóa và giải mã sử dụng chung một khóa nên khóa (secret key) sử dụng cần phải được bảo quản an toàn tuyệt đối.

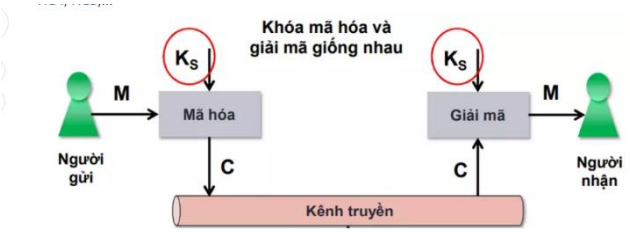
+ Vấn đề phân phối khóa

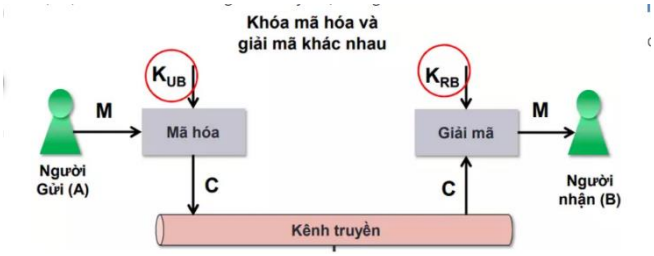
+ Vấn đề quản lý khóa (với hệ thống có n nút khác nhau thì số lượng khóa cần thiết cho hệ thống là n(n+1)/2

+ Không cung cấp tính chống thoái thác thông tin

Câu 12:

Vẽ mô hình hệ mã hóa đối xứng và hệ mã hóa bất đối xứng? So sánh hệ mã đối xứng và hệ mã bất đối xứng





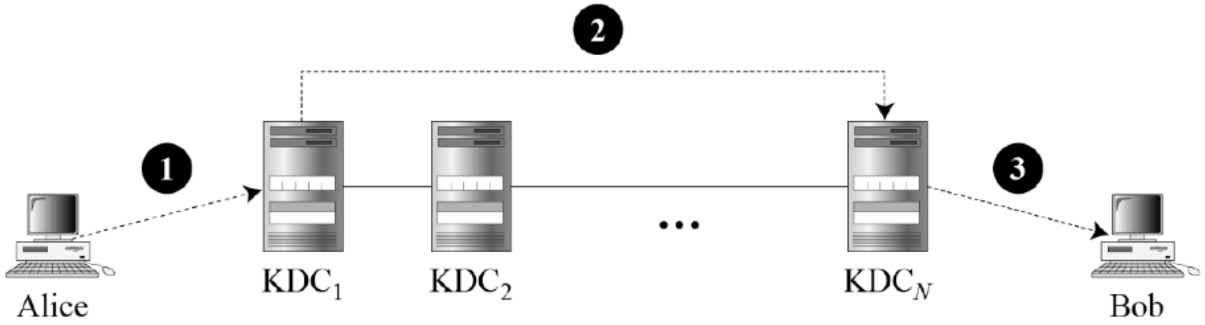
So sánh hệ mã đối xứng và bất đối xứng

Symmetric-key Encryption	Public-key Encryption
Cùng thuật toán với cùng khóa được dùng cho việc mã hóa và giải mã	Một thuật toán được dùng để mã hóa và giải mã với một cặp khóa, một khóa dành cho mã hóa và một dành do giải mã
Sender và Receiver phải cùng chia sẻ thuật toán và khóa	Sender và receiver phải có một trong cặp khóa (không giống nhau)
Khóa phải giữ bí mật	Một trong hai khóa phải được giữ bí mật
Không thể hoặc ít nhất không thực thể để giải mã một thông điệp nếu những thông tin khác có sẵn.	Không thể hoặc ít nhất không thực thể để giải mã một thông điệp nếu những thông tin khác có sẵn.
Sự hiểu biết về thuật toán cộng với các mẫu ciphertext phải đủ thì mới xác định ra được khóa	Sự hiểu biết về thuật toán + một trong hai khóa + các mẫu ciphertext phải đủ thì mới có thể xác định được khóa còn lại.

Câu 13: Trong mã hóa khóa công khai, khóa riêng và khóa công khai có phải là 2 khóa tùy ý, không liên quan? Nếu có liên quan, tại sao không thể tính khóa riêng từ khóa công khai?Tại sao trong hệ mã RSA nếu biết khóa công khai (n,e) thì rất khó tìm khóa bí mật (n,d)

Câu 14: Khóa phiên (Session Key) là gì? Khóa phiên khác khóa bí mật chia sẻ (secret key) như thế nào? (Vẽ mô hình KDC (Key Distribution Center))

Session Key (Khóa phiên) là khóa bí mật do trung tâm quản lí và phân phối khóa tạo ra để giao dịch giữa 2 thành viên và chỉ được sử dụng 1 lần sau khi kết thúc giao dịch khóa phiên không còn tác dụng)



Câu 15: Thế nào là tấn công Man-in-the-middle. Nêu (vẽ mô hình) và giải thích một giaothức/cơ chế mà có thể bị tấn công này tấn công.

Khái niệm: là một cuộc tấn công mà kẻ tấn công bí mật chuyển tiếp và có thể làm thay đổi giao tiếp giữa hai bên mà họ tin rằng họ đang trực tiếp giao tiếp với nhau. Một ví dụ về các cuộc tấn công man-in-the-middle là nghe trộm (eavesdropping), trong đó kẻ tấn công kết nối độc lập với các nạn nhân và chuyển tiếp thông tin giữa họ để họ tin rằng họ đang nói chuyện trực tiếp với nhau qua kết nối riêng tư, trong khi thực ra toàn bộ cuộc trò chuyện được kiểm soát bởi kẻ tấn công. Người tấn công phải có khả năng đánh chặn tất cả các thông tin liên quan đi lại giữa hai nạn nhân và tiêm những thông tin mới.

Câu 16:

Trình bày giao thức trao đổi khóa Diffie-Hellman. Nêu ưu điểm và nhược điểm của giao thức trao đổi khóa Diffie-Helman?

Khái niệm: là một phương pháp trao đổi khóa được phát minh sớm nhất trong mật mã học. Phương pháp trao đổi khóa Diffie–Hellman cho phép hai bên (người, thực thể giao tiếp) thiết lập một khóa bí mật chung để mã hóa dữ liệu sử dụng trên kênh truyền thông không an toàn mà không cần có sự thỏa thuận trước về khóa bí mật giữa hai bên. Khóa bí mật tạo ra sẽ được sử dụng để mã hóa dữ liệu với phương pháp mã hóa khóa đối xứng.

*** Ưu điểm của Thuật toán Diffie Hellman**

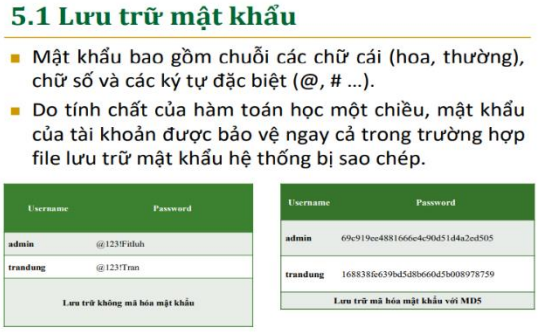
- Người gửi và người nhận không cần biết trước về nhau.
- Sau khi các khóa được trao đổi, việc truyền dữ liệu có thể được thực hiện thông qua một kênh không an toàn.
- Việc chia sẻ khóa bí mật là an toàn.

*** Nhược điểm của Thuật toán Diffie Hellman**

- Thuật toán không thể bị kiện vì bất kỳ trao đổi khóa bất đối xứng nào.
- Tương tự, nó không thể được sử dụng để ký chữ ký điện tử.
- Vì nó không xác thực bất kỳ bên nào trong quá trình truyền, trao đổi khóa Diffie Hellman dễ bị tấn công trung gian.

Câu 17:

Hàm băm là gì? Nêu và giải thích ứng dụng hàm băm trong việc lưu trữ mật khẩu (Vẽ mô hình).

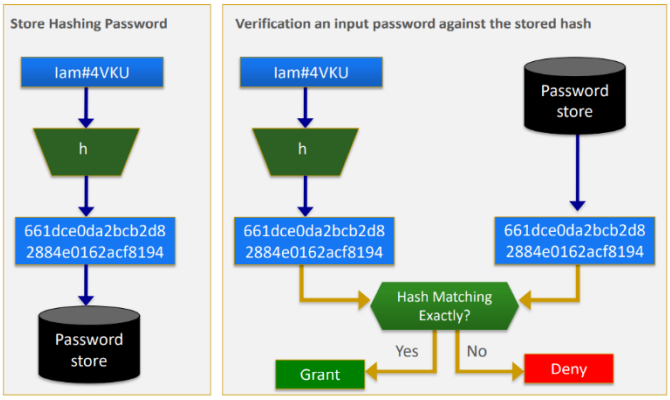


5.1 Lưu trữ mật khẩu

Dùng lưu trữ mật khẩu (băm password):

- Hàm băm được dùng để tạo **one-way password file**, trong cơ chế này giá trị băm của password được lưu, điều này tốt hơn là lưu chính bản rõ password. → password không bị truy xuất bởi kẻ tấn công nơi chứa password.
- Khi user nhập vào một password, thì giá trị băm của password được so với giá trị băm được lưu để kiểm tra.

Password Verification



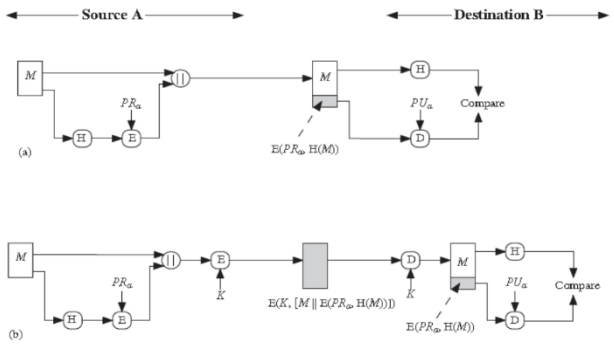
Câu 18:

Hàm băm là gì? Nêu và giải thích ứng dụng hàm băm trong chữ ký điện tử (Vẽ mô hình).

5.3. Chữ ký điện tử(Chữ ký số)

- Giá trị băm của thông điệp được mã hóa bằng **private key** của user, bất kỳ ai biết **public key** của user thì có thể thẩm tra thông điệp mà được gắn kết với chữ ký số.
- Kẻ tấn công muốn hiệu chỉnh thông điệp thì sẽ cần phải biết private key của user.

5.3. Chữ ký điện tử(Chữ ký số)



Câu 19: Hàm băm là gì? Trình bày và giải thích các tính chất của hàm băm?

4. Hàm băm (Hash Function)

- **Hàm băm** là các thuật toán không sử dụng khóa để mã hóa, nó có nhiệm vụ băm thông điệp được đưa vào theo một thuật toán ***h* một chiều nào đó**, rồi đưa ra một **bản băm – văn bản đại diện – có kích thước cố định**. Do đó người nhận không biết được nội dung hay độ dài ban đầu của thông điệp đã được băm bằng hàm băm.
- Giá trị của hàm băm là duy nhất, và **không thể suy ngược** lại được nội dung thông điệp từ giá trị băm này.

Tính chất hàm băm

1. Tính 1 chiều (Preimage resistant – one-way property):

Cho trước giá trị băm h việc tìm x sao cho H(x)=h là rất khó

- Dạng tấn công thứ nhất là người C bắt đầu với một bức điện được ký có giá trị (x, y), trong đó y = sigK(h(x)) (cặp (x, y) có thể là bất kỳ bức điện trước đó mà B đã ký). Sau đó, C tính z = h(x) và cố gắng tìm x‟ # x để h(x‟) = h(x). Nếu C làm được điều này thì cặp (x‟, y) sẽ là một bức điện được ký có giá trị (một bức điện giả mạo có giá trị). Để ngăn cản việc này, hàm Băm h phải thoả mãn tính chất 1

Tính chất hàm băm

2. Tính kháng đụng độ yếu (Second preimage resistant – weak collision resistance – Tính chống trùng yếu):

Cho thông điệp đầu vào x, việc tìm một thông điệp x' với (x'≠ x) sao cho h(x')=h(x) là rất khó

- Một dạng tấn công khác mà người C có thể làm là: đầu tiên anh ta tìm 2 bức điện x ≠ x‟ sao cho h(x) = h(x‟). Sau đó C đưa bức điện x cho B và thuyết phục B ký vào cốt bức điện h(x); và vì vậy, anh ta tìm được y. Như vậy, cặp (x‟, y) là một cặp chữ ký giả có giá trị. Điều này là nguyên nhân mà việc thiết kế hàm Băm phải thoả mãn tính chất 2.

Tính chất hàm băm

3. Tính kháng đụng độ mạnh-tính chống trùng mạnh (Strong Collision resistance):

Không thể tính toán để tìm được hai thông điệp đầu vào $x_1 \neq x_2$ sao cho chúng có cùng giá trị băm

(Nghịch lý ngày sinh – Birthday paradox)

Dạng tấn công thứ 3 là chọn một giá trị cốt z ngẫu nhiên. Người C sẽ tính một chữ ký với một giá trị ngẫu nhiên z, sau đó anh ta tìm một bức điện x sao cho z = h(x). Nếu anh ta làm được điều này thì cặp (x, y) là cặp chữ ký giả có giá trị. Như vậy một tính chất nữa mà h cần thoả mãn là tính một chiều.

Câu 20:

Chữ ký số là gì? Trình bày và giải thích quá trình tạo chữ ký số và thẩm tra chữ ký số?

Khái niệm về chữ ký số (Digital Signature)

- Khái niệm về Digital Signature được để xuất bởi Diffie & Hellman (1976)
- "Chữ ký điện tử (còn gọi là chữ ký số) là thông tin được mã hoá bằng Khoá riêng của người gửi, được gửi kèm theo văn bản nhằm đảm bảo cho người nhận định danh, xác thực đúng nguồn gốc và tính toàn vẹn của tài liệu nhận.

Trình bày và giải thích quá trình tạo chữ ký số và thẩm tra chữ ký số

Nguyên lý ký điện tử trong hệ mật mã công khai

1. Người gửi (chủ nhân văn bản): ký văn bản bằng cách mã hóa nó với khóa bí mật của mình, rồi gửi cho bên nhận.

2. Người nhận tiến hành kiểm tra chữ ký bằng cách sử dụng khóa công khai của người gởi để giải mã văn bản. Nếu giải mã thành công thì văn bản ký là đúng người gửi