CÂU HỎI ÔN TẬP CUỐI KỲ
MÔN: NHẬP MÔN AN TOÀN THÔNG TIN
Thi online, với nội dung được viết bằng chữ viết tay của mình

LO1: Giải thích sự ảnh hưởng của an toàn HTTT đến cá nhân, tổ chức và xã hội

Tình huống 1:

Trung tâm tin học của khoa 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_iuh.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 website này. 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 thẻ ngân hàng thanh toán. Thông tin các khóa học cũng được website 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.

Hãy nêu và giải thích ít nhất 3 tính cần thiết của an toàn HTTT đối với website của trung tâm.

Trả lời

- Tính bảo mật: Thông tin cá nhân của sinh viên và thông tin về thẻ ngân hàng của cá nhân từng sinh viên cần đảm bảo tính bảo mật để tránh bị kẻ xấu truy cập vào và đánh cắp, các thông tin này là thông tin cá nhân cho nên rất quan trọng, nếu để người ngoài truy cập được mà không phải chủ sở hữu thì hậu quả để lại rất lớn, có khi thông tin sẽ được đi rao bán, gây ảnh hưởng tới cá nhân từng sinh viên.
- Tính toàn vẹn: Các thông tin về các khóa học cần đảm bảo tính toàn vẹn. Dữ liệu luôn phải được đảm bảo là đáng tin cậy và chính xác từ một nguồn đáng tin cậy. Để chắc chắn rằng sinh viên sau khi đăng kí thì thông tin cá khóa học vẫn toàn vẹn không có sự thay đổi về các thông tin như thời gian học, học phí,...
- Tính sẵn dùng: Hệ thống thanh toán học phí trực tuyến các khóa học cần có tính sẵn dùng, đảm bảo rằng chủ tài khoản (sinh viên) có thể truy cập/giao dịch thông tin tài khoản và thanh toán bất cứ lúc nào mà họ muốn. Bên cạnh đó kết quả của các khóa học cũng cần có tính sẵn dùng để sinh viên có thể xem bất cứ khi nào họ muốn.

Tình huống 2:

Nhà ăn của trường Đại học Công nghiệp Tp. HCM có một Website ĐẶT THỰC ĐƠN CÁC MÓN ĂN TRỰC TUYẾN (http://www.cantin_iuh.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 mà khách 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

Hãy nêu và giải thích ít nhất 3 tính cần thiết của an toàn HTTT đối với website nhà ăn.

Trả lời

- Tính bảo mật: Thông tin cá nhân như họ tên, số điện thoại, địa chỉ email, mã số giáo viên/mã sinh viên mà hệ thống lưu trữ, quản lý và thông tin về thẻ ngân hàng thanh toán cần đảm bảo tính bảo mật. để tránh bị kẻ xấu truy cập vào và đánh cắp, các thông tin này là thông tin cá

nhân cho nên rất quan trọng, nếu để người ngoài truy cập được mà không phải chủ sở hữu thì hậu quả để lại rất lớn, có khi thông tin sẽ được đi rao bán, gây ảnh hưởng tới cá nhân. Nặng hơn thì với thông tin thẻ ngân hàng mà kẻ xấu có được, họ sẽ sử dụng cho những mục đích xấu, ảnh hưởng tới an toàn của thẻ ngân hàng cá nhân.
- Tính toàn vẹn: thực đơn các món ăn cho bữa ăn sáng/trưa/tối cần đảm bảo tính toàn vẹn. Để chắc chắn rằng về giá cả, thông tin món ăn,.. không bị thay đổi so với những gì đã được nêu.
- Tính sẵn dùng: Thực đơn các món ăn trực tuyến và thông tin cá nhân những khách hàng đã đăng ký thành viên cần đảm bảo tính sẵn dùng để khi mà họ giao dịch thì mọi thứ sẽ luôn ở trạng thái sẵn sàng, giúp giao dịch sẽ nhanh và đỡ tốn thời gian hơn cho cả đôi bên.

Tình huống 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 cũng như 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 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.
Hãy nêu và giải thích ít nhất 3 tính cần thiết của an toàn HTTT đối với website Đường sắt Việt Nam.
Trả lời
- Tính bảo mật: 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 cần đảm bảo tính bảo mật. để tránh bị kẻ xấu truy cập vào và đánh cắp, các thông tin này là thông tin cá nhân cho nên rất quan trọng, nếu để người ngoài truy cập được mà không phải chủ sở hữu thì hậu quả để lại rất lớn, có khi sẽ bị giả mạo thông tin cá nhân nhằm trục lợi hoặc các mục đích xấu.
- Tính toàn vẹn: thông tin về các chuyến tàu của website Đường sắt Việt Nam (www.dsvn.vn) cần đảm bảo tính toàn vẹn, không có sự sai sót trong lúc đưa lên nhằm cho việc mua bán vé với người dân sẽ được đảm bảo là sẽ chính xác và không có trục trặc sai sót gì diễn ra sau khi người dân đã mua vé thành công.
- Tính sẵn dùng: Hệ thống cung cấp thông tin tuyến tàu, giá vé, thời gian chạy, thời gian đến, tình trạng số ngồi mỗi toa, loại ghế, ngày đi,... cần đảm bảo tính sẵn dùng để khi cần tra cứu thì nó sẽ luôn trong tình trạng sẵn sàng, không chậm trễ cũng như đảm bảo tránh được các đợt tấn công như DDOS, DOS... có thể làm cho hệ thống mất đi tính sẵn dùng của dữ liệu. Hệ thống bị sập, đồng nghĩa thông tin không thể truy cập và xem được, dẫn tới mất đi tính sẵn dùng.

LO3: Áp dụng được một số lý thuyết toán trong các hệ mật mã

1. **Cho p=7, q=11, e=17. Hãy thực hiện phát sinh khóa công khai và khóa riêng phần theo cơ chế RSA. Thực hiện tạo và thẩm tra chữ ký RSA thông điệp m=9**
   Tạo chữ ký: S=m^d mod n
   Thẩm tra m=S^e mod n

-Phát sinh khóa :

- n = p*q = 77
- $\phi(n) = (p-1)*(q-1) = 60$
- Cho e= 17

  => $d= e^{-1} \bmod \phi n \Leftrightarrow d= 17^{-1} \bmod 60$ (d là nghịch đảo nhân của 17 modulo 60)

Áp dụng giải thuật Euclid mở rộng, ta có:

Q	ϕn	e	r	t1	t2	t
3	60	17	9	0	1	-3
1	17	9	8	1	-3	4
1	9	8	1	-3	4	-7
8	8	1	0	4	-7	60
//	1	0	//	**-7**	60	//

Nên nghịch đảo nhân của 17 modulo 60 là -7 hoặc 53

=> d= 53

- Tạo chữ ký:

$S= M^d \bmod n= 9^{53} \bmod 77$

Ta có : $B = 53_{(10)} = 110101_{(2)}$

Lập được bảng:

B[i]	$p= p^2$	p= p mod 77	p= p*9	p= p mod 77
1	1	1	9	9
1	81	4	36	36
0	1296	64	//	64
1	4096	15	135	58
0	3364	53	//	53
1	2809	37	333	**25**

=> $S= 9^{53} \bmod 77 = 25$

- Thẩm tra chữ ký:

$M'= S^e \bmod n= 25^{17} \bmod 77$

$= [(25^5 \bmod 77)^2 * (25^7 \bmod 77)] \bmod 77$

$= [(9765625 \bmod 77)^2 * (6103515625 \bmod 77)] \bmod 77$

$= (23^2 * 53) \bmod 77$

$= 28027 \bmod 77$

$= 9$

$=> M' = 25^{17} \bmod 77$

=> $M \equiv M' \bmod n$

2. Giả sử Alice và Bob thống nhất với nhau chọn số nguyên tố p = 23 và g = 7. Alice chọn một giá trị ngẫu nhiên bất kỳ x = 11 và bí mật x. Bob chọn một giá trị ngẫu nhiên bất kỳ y = 7 và bí mật y. Hãy trình bày quá trình tạo và trao đổi khóa phiên giữa Alice và Bob

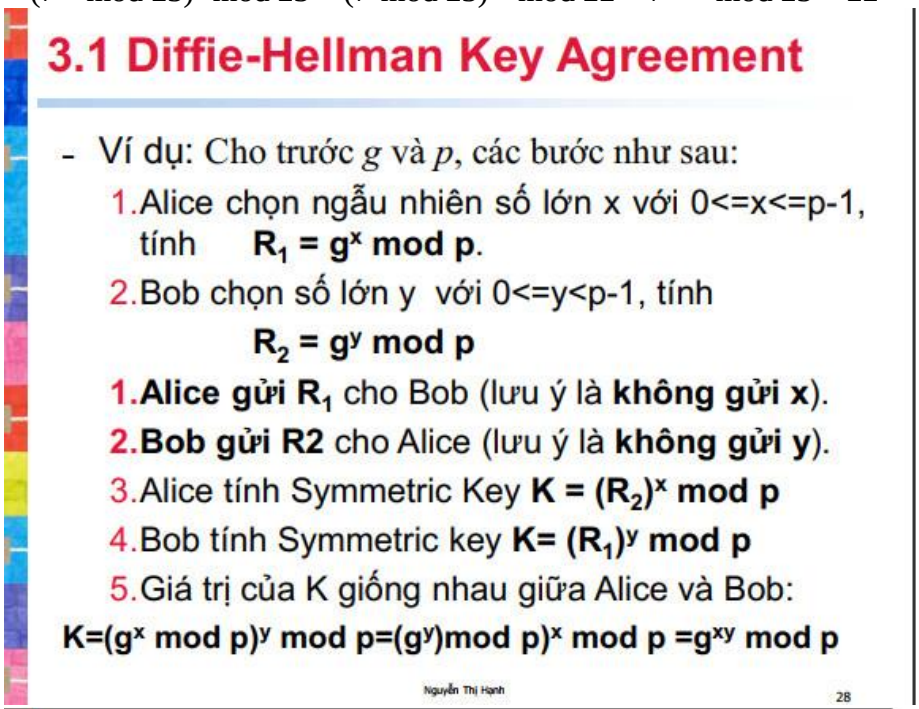
Alice chọn x = 11 và tính $R_1 = g^x \bmod p = 7^{11} \bmod 23 = 1977326743 \bmod 23 = 22$

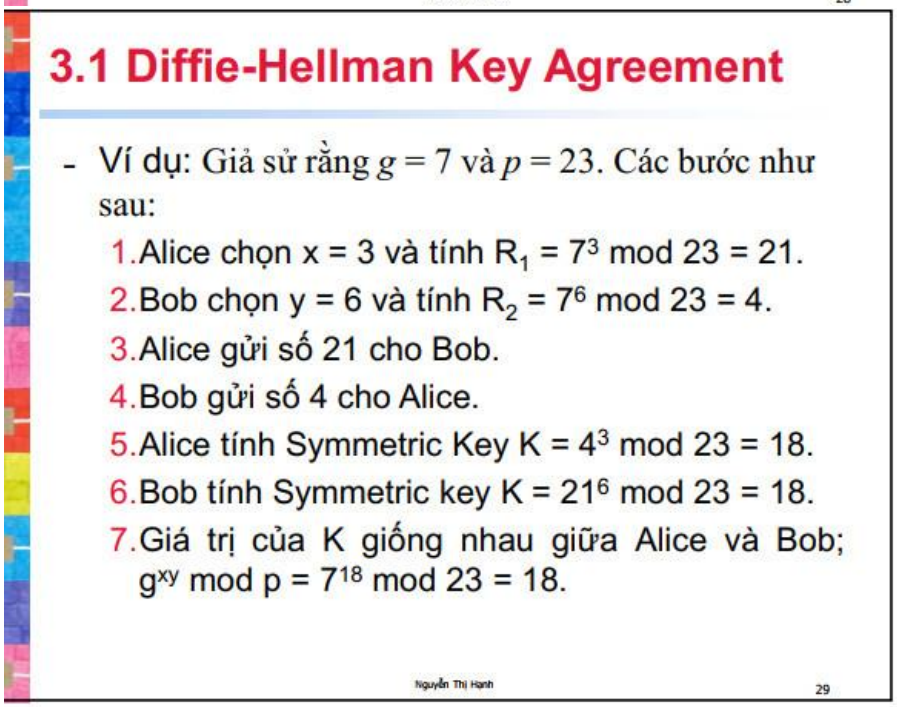
Bob chọn y = 7 và tính $R_2 = g^y \bmod p = 7^7 \bmod 23 = 823543 \bmod 23 = 5$

- Alice gửi số 22 cho Bob
- Bob gửi số 5 cho Alice

Alice tính Symmetric Key K= $(R_2)^x$ mod p = 5^{11} mod 23 = 48828125 mod 23 = 22
Bob tính Symmetric Key K= $(R_1)^y$ mod p = 22^7 mod 23 = 2494357888 mod 23 = 22
- Giá trị của K giống nhau giữa Alice và Bob:

K = $(g^x \text{ mod } p)^y$ mod p = (g^y)mod $p)^x$ mod p = g^{xy} mod p
= $(7^{11} \text{ mod } 23)^7$ mod 23 = $(7^7$mod $23)^{11}$ mod 22 = 7^{11*7} mod 23 = 22





LO4: Giải thích được các khái niệm cơ bản về An toàn thông tin, hệ mã hóa

1. Nêu và giải thích một ứng dụng của hàm băm trong thực tế

- Kiểm tra tính toàn vẹn của message và file: bằng cách so sánh giá trị băm của message trước và sau khi truyền để xác định xem liệu có thay đổi nào đã xảy ra trong quá trình truyền hay không.

- Xác thực mật khẩu: ta có thể lưu trữ mật khẩu bằng giá trị băm của nó để tăng tính bảo mật. Để kiểm tra, password được user đưa vào sẽ được hash và so sánh với giá trị băm đã được lưu. Để phòng chống tấn công bằng brute force, ta có thể tăng thời gian kiểm tra bằng cách sử dụng key stretching. Ngoài ra ta có thể sử dụng thêm salt để tránh trường hợp: 2 password giống nhau có kết quả lưu trữ giống nhau.

- Bằng chứng công việc — Proof of Work (PoW): được sử dụng trong blockchain để chống lại DOS, spam bằng cách yêu cầu một số công việc từ bên muốn truy cập. Đặc điểm chính của công việc này là: công việc phải có độ khó cao tốn nhiều thời gian (nhưng khả thi) ở phía requester nhưng lại dễ kiểm tra cho provider. Vì vậy hàm băm được sử dụng ở đây. Ví dụ công việc được đưa ra là tìm một message, sao cho giá trị băm của nó bắt đầu với 20 bit 0. Trung bình mỗi requester cần thử 2^{19} lần để tìm ra một message đúng.

- Hàm băm trong ứng dụng lưu mật khẩu: Khi ta đăng nhập vào một hệ thống nào đó để đảm bảo cho cơ sở dữ liệu của ta được an toàn trong lưu trữ, hệ thống tiến hành băm mật khẩu khi ta nhập vào được giá trị (h) băm duy nhất và lưu giá trị băm đó.
Lần khác đăng nhập, hệ thống cũng tiến hành băm mật khẩu ta vừa nhập được giá trị băm (h') sau đó đem so sánh với giá trị băm (h) của mật khẩu đã lưu trong cơ sở dữ liệu, nếu bằng nhau(h'=h) thì hệ thống sẽ cho chúng ta vào.

2. Trình bày và giải thích 1 phương pháp xác thực thông điệp

- Xác thực thông điệp là xác nhận nguồn gốc của dữ liệu, thuyết phục với NSD là dữ liệu này chưa bị sửa đổi hoặc giả mạo và là cơ chế quan trọng để duy trì tính toàn vẹn và không thể từ chối dữ liệu. Các phương pháp Xác thực thông điệp:
- Mã hóa thông điệp: Sử dụng mã hóa khóa bí mật, mã hóa khóa công khai
- Hàm băm (Hash Function): Một hàm ánh xạ một thông điệp có chiều dài bất kỳ vào một giá trị băm có chiều dài cố định sử dụng để chứng thực
- Mã chứng thực thông điệp (MAC): một hàm và một khóa bí mật tạo ra một giá trị có chiều dài cố định sử dụng để chứng thực.

Phương pháp xác thực thông điệp Mã chứng thực thông điệp (MAC):

• Là một kỹ thuật xác thực sử dụng một khóa bí mật để nén một thông điệp M có chiều dài bất kỳ thành một xác thực kích thước nhỏ cố định (đgl checksum hoặc MAC)

• Kỹ thuật này giả sử rằng 2 phía A và B chia sẽ 1 khóa bí mật K. Khi A có 1 thông điệp gởi đến B, A sẽ tính toán MAC như là một hàm của thông điệp và khóa: $MAC = C_K(M)$, với

M: Thông điệp đầu vào
C: Hàm MAC
K: Khóa bí mật chia sẻ giữa người gởi và người nhận
MAC: Mã chứng thực thông điệp có chiều dài cố định

• Thông điệp cộng với MAC được truyền tới người nhận. Người nhận thực hiện các tính toán tương tự trên các thông điệp đã nhận sử dụng cùng một khóa bí mật, để tạo ra một MAC mới.

• MAC vừa tạo sẽ được so với MAC nhận. Giả sử chỉ người nhận và người gửi biết khóa bí mật:

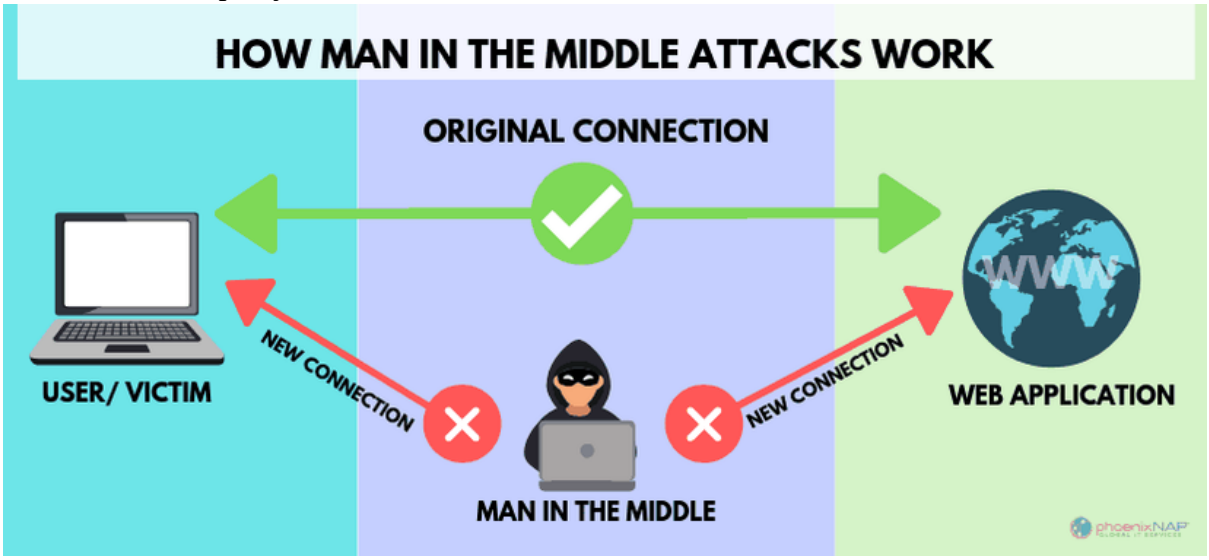
– Nếu MAC nhận phù hợp với MAC vừa tính thì thông điệp không bị thay đổi trong quá trình truyền và chắc chắn được gởi tới từ người gởi đã biết.

– Nếu MAC nhận khác với MAC vừa tính thì thông điệp đã bị thay đổi hoặc bị giả mạo và được gởi từ attacker.

3. Trình bày giao thức trao đổi khóa Diffie-Hellman. Nêu ưu điểm và nhược điểm của giao thức trao đổi khóa Diffie-Helman.
   - Là phương pháp trao đổi khóa cho phép hai bên thiết lập một khóa bí mật chia sẻ để mã hóa dữ liệu sử dụng trên đường truyền không an toàn mà không cần có sự thỏa thuận trước về khóa bí mật giữa hai bên. Khóa bí mật chia sẻ đó sẽ sử dụng để mã hóa dữ liệu với phương pháp mã hóa khóa đối xứng.
   - Giao thức trao đổi khóa Diffie-Hellman là sơ đồ khóa công khai để thiết lập khóa phiên chung chỉ 2 đối tác biết thuật toán dựa trên độ khó của toán tính logarit rời rạc
   - **Giao thức trao đổi khóa giữa 2 đối tác:**
   + A và B thống nhất chọn một số nguyên tố p và một phần tử sinh G và bắt đầu tạo khóa: A chọn 1 khóa riêng tư XA và tính khóa công khai YA dựa trên khóa bí mật qua công thức YA = GX mod P sau đó gởi khóa YA cho B.
   Tương tự, bên B cũng chọn một khóa bí mật y tính khóa công khai YB bằng công thức YB = Gy mod P. sau đó gởi YB cho A.
   Sau khi nhận khóa công khai của nhau cả 2 tiến hành xác định khóa phiên dựa vào số học modulo
   Secret Key by user A: K=(YB)X mod P
   Secret Key by user B: K= (YA)Y mod P
   Ưu điểm:
   + Người gửi và Người nhận không cần biết về nhau.
   + Giao tiếp có thể diễn ra trên kênh truyền không an toàn.
   Nhược điểm:
   + Không thể sử dụng cho trao đổi khóa bất đối xứng.
   + Không thể sử dụng cho việc ký chữ ký số.
   + Rất dễ bị tấn công man-in-the-middle vì không có xác thực bên tham gia trao đổi.
   Trình bày giao thức trao đổi khóa Station to Station. Hãy so sánh giao thức này với giao thức trao đổi khóa Diffie-Hellman.
4. Khóa phiên (Session Key) là gì? Khóa phiên có ưu điểm gì so với khóa bí mật chia sẻ (secret key) như thế nào?
   - Khóa phiên (Session Key) là khóa bí mật do KeyDistribution Center (KDC) tạo ra để giao dịch giữa 2 thành viên và chỉ được dùng một lần (sau khi giao dịch kết thúc thì khó phiên không còn tác dụng).
   - Trong các giao thức máy tính SSL, khóa phiên được tạo ngẫu nhiên và nó được trao đổi an toàn với máy tính khác (Sử dụng giao thức trao đổi khóa như Diffie-Hellman) và chỉ tồn tại trong bộ nhớ máy tính trong giới hạn phiên. Khi hết phiên bản cả hai bên sẽ xóa bản sao khóa của họ ra khỏi bộ nhớ máy của họ.
   - So sánh Session Key và Shared Secret Key:
   - **Session Key**
     - Chỉ dùng một lần
     - Thường chỉ dùng trong giao thức truyền thông – Web traffic
   - **Shared Secret Key**
     - Là loại khóa dài hạn, được sử dụng lại nhiều thời điểm nên được lưu trữ cố định ở đâu đó, thậm chí là được in trên giấy

- Có thể áp dụng vào bất kì hệ thống mã hóa nào.

5. Thế nào là tấn công Man-in-the-middle. Nêu (vẽ mô hình) và giải thích một giao thức/cơ chế mà có thể bị tấn công này tấn công.
   - Man-in-the-middle là một kiểu tấn công bí mật xảy ra khi kẻ tấn công tự nhét mình vào một phiên giao tiếp giữa người hoặc hệ thống (Thường là trình duyệt web và máy chủ web).
   - Một kịch bản Man-in-the-middle có ba đối tượng tham gia: Nạn nhân, đối tượng mà nạn nhân đang cố gắng kết nối, và kẻ tấn công ở giữa, kẻ tấn công đã chặn kết nối của nạn nhân và nạn nhân không nhận thức được kẻ này, đây là sự điều kiện tiên quyết cho kịch bản đánh cắp này.



Mô hình Man in the middle

   - Một giao thức/cơ chế mà có thể bị tấn công này tấn công

   HTTPS spoofing - Giả mạo HTTPS

   Khi truy cập website, HTTPS trong URL, chứ không phải là HTTP là dấu hiệu cho thấy website này an toàn. Kẻ tấn công có thể đánh lừa trình duyệt của bạn rằng đang truy cập một website đáng tin cậy bằng cách chuyển hướng trình duyệt của bạn đến một website không an toàn sau khi truy cập, kẻ tấn công có thể theo dõi các tương tác của bạn với website đó và có thể đánh cắp thông tin cá nhân bạn đang chia sẻ.

6. Trình bày khái niệm, các thành phần và công dụng của chứng chỉ số (Certificate). Ở Việt Nam có những cơ quan/công ty nào cung cấp các Certificate, cách dùng nhưng thế nào?
7. Hãy liệt kê các phương pháp chứng thực thực thể, theo bạn phương pháp nào là hiệu quả nhất hiện nay? Vì sao? Mô tả phương pháp này?

   Các phương pháp chứng thực thực thể :

   - Chứng thực bằng Passwords
   - Chứng thực bằng Challenge – Response
   - Chứng thực Zero-Knowledge ZKP
   - Chứng thực bằng sinh trắc học Biometrics.
   - Ngoài ra còn có các phương pháp sử dụng kết hợp các phương pháp trên.

• Hiện nay phương pháp chứng thực bằng Passwords được sử dụng chủ yếu, tuy nhiên, công nghệ ngày càng phát triển, việc chứng thực bằng sinh trắc học đang dần được sử dụng nhiều mang lại hiệu quả cao hơn.
Vì: Nhận dạng sinh trắc học (vân tay, móng mắt/võng mạc, DNA…) là những điểm đặc trưng nhận dạng của mỗi người, có thể nói không thể trùng nhau nên việc chứng thực sẽ có độ chính xác cao, tin cậy, thời gian chứng thực nhanh (dưới 1s) trong các trường hợp có thể đụng độ nhưng khả năng hầu như rất thấp và không đáng kể và vì cần phải sử dụng các thiết bị công nghệ cao nên giá thành đắt đó là nhược điểm lớn làm cho phương pháp này thực sự chưa phổ biến bằng phương pháp chứng thực truyền thống.
- Mô tả:
Phương pháp chứng thực bằng vân tay, võng mac/móng mắt
+ Sử dụng các thiết bị thu nhận (quét) và lưu trữ các đặc tính sinh trắc học.
+ Quét các đặc tính sinh trắc của chủ thể (đặc điểm vân tay, móng mắt...) đưa về dạng dữ liệu biểu diễn dưới dạng các bit và lưu trữ trong cơ sở dữ liệu.
+ Chứng thực: Chủ thể muốn giao dịch cần phải chứng thực danh tính/định danh cần tiến hành quét lại các thông tin bảo mật lưu trước đó qua các thiết bị quét như vân tay, móng mắt, sau khi quét, tiến hành đưa về chuỗi các bit và so sánh trong cơ sở dữ liệu:
Nếu đúng (trùng với dữ liệu đã lưu) → Xác thực thành công
Nếu không trùng với dữ liệu trước đó, hệ thống từ chối giao dịch đến khi chủ thể chứng thực thành công.

8. Chứng thực thực thể bằng sinh trắc học (biometrics) là gì, nêu ưu điểm và nhược điểm của phương pháp này, phương pháp này thường được áp dụng ở đâu.
Chứng thực thực thể bằng sinh trắc học (Biometrics) là sử dụng các phép đo lường về các đặc tính sinh lí học hoặc hành vi học mà nhận dạng một con người, các đặc thù của sinh trắc học không thể đoán , ăn cắp hay chia sẻ. ví dụ như vân tay, vân lòng bàn tay, võng mạc, móng mắt, khuôn mặt, giọng nói…
- Ưu điểm:
+ Có độ chính xác cao
+ thời gian chứng thực rất nhanh (nhỏ hơn 1s)
+ Sự tác động của người dùng thấp
+ Có sự kết hợp nhiều yếu tố: vân tay, võng mạc, giọng nói.
- Nhược điểm:
+ Giá thành: triển khai hệ thống sinh trắc học đòi hỏi chi phí cao cho cả phần cứng (thiết bị thu/quét, và nhận dạng) với các phần mềm hiện đại.
+ có thể nhận diện sai: do hư hỏng phần cứng, lỗi phần mềm làm cho hệ thống từ chối người dùng mặc dù đúng người.
- **Hiện nay:** công nghệ chứng thực bằng sinh trắc học được áp dụng rộng rãi hơn ở những ngân hang, các công ty (dùng chấm công, điểm danh) hay thực hiện bảo mật dữ liệu cá nhân trên các thiết bị di động cao cấp….

LO5: Mô tả được cơ chế/giao thức để thiết lập và nâng cao tính an toàn thông tin cho một tình huống cụ thể

Tình huống 1:

Giả sử khoa CNTT của trường trang bị một phòng máy tính (gồm 20 máy tính) dùng để phục vụ cho việc học tập và nghiên cứu của các thành viên trong câu lạc bộ CIA_Club. Bạn hãy:

1. **Đưa ra các giải pháp chứng thực, theo dõi, kiểm soát một cách tự động các thành viên vào ra phòng máy tính đó. Nêu lý do và giải thích tại sao chọn giải pháp này là hợp lý nhất.**
   Thẻ từ + camera
   Sinh trắc học + camera
   Chọn giải pháp vào? Tại sao hữu hiệu nhất (ưu điểm of giải pháp chọn và nhược điểm của giải pháp ko chọn)
   Chọn sinh trắc học + camera

(nêu được phương pháp, đưa ra cách thức cấu hình, cài đặt các trang thiết bị cũng như phần mềm).

Trong trường hợp này nên sử dụng phương pháp là Chọn sinh trắc học + camera
đầu tiên cần cài đặt tại cửa ra vào 1 cái máy có thể sử dụng sinh trắc học để mở cửa một các duy nhất.vì trong tình huốn này thì hiệu quả hơn.
- Sinh trắc học (Biometric) là phép đo lường về các đặc tính sinh lý học hoặc hành vi học mà nhận dạng một con người. Sinh trắc học đo lường các đặc tính mà không thể đoán, ăn cắp hoặc chia sẻ.
Công dụng: được dùng để mở khóa của của clb 1 cách duy nhất sau khi được lấy mẫu.
Camera là 1 phần mên cho phép người quản lí có thể theo dõi nhưng việc xảy ra tại nơi được lắp camera và lưu lại hình ảnh đó cho phép hình ảnh đó có thể hiển thị lại theo trình tự thời gian đã ghi lại trước đó.
Sinh trắc học mặc dù tốn kém trong việc lăp đặt thiết bị tại cửa ra vào, thời gian lấy mẫu của mỗi sinh viên là tiêu tốn thời gian. tuy nhiên - ư điểm của sinh trắc học khi dã được lấy mẫu thành công thì việc xác thật 1 cách nhanh chóng với đô chính xác rất cao, không thể bị giả mạo bởi ai đó, không thể mất và bỏ quên ở đâu đó.
- nhực điểm của việc sử dụng thẻ từ thẻ từ chỉ phù hợp với những nơi có sl sinh viên đông, dễ dàng bị đánh cắp hoặc quên đem theo,
Vì vậy thẻ từ không thể phù hợp được sử dụng trong trường hợp này vì ai cũng sở hưu 1 thẻ từ, mà không phải ai cũng là thành viên của clb đó cho nên thẻ từ không được sử dụng.
Thẻ từ + Camera: Thẻ sinh viên hiện tại là thẻ từ luôn nên có thể tận dụng thẻ sv làm thẻo nhưng khổng thể sử dụng làm cửa ra vào của clb
Sinh trắc học + Camera: (số lượng sinh ít có giới hạn cụ thể) → thích hợp cho sử dụng phương pháp này cho clb.

Mô tả việc sinh viên vào ra như thế nào : sử dụng sinh trắc học như vân tay để quét vào của ra vào, để từ đó tại khóa cửa có thể nhận biết là thành viên của clb đã được ghi danh trong việc lấy mẫu trước đó, từ đó cửa sẽ được mở trực tiếp đi vào clb 1 cách dễ dàng.

2. **Đưa ra các giải pháp chứng thực, theo dõi, kiểm soát một cách tự động các thành viên sử dụng các tài nguyên trong phòng máy tính đó.**
   Nêu lý do và giải thích tại sao chọn giải pháp này là hợp lý nhất

(nêu được phương pháp, đưa ra cách thức cấu hình, cài đặt các trang thiết bị cũng như phần mềm).

Cấu hình hệ thống máy: <<mạng máy tính>> , phân quyền người dùng (username + PW)
Sử dụng phương pháp username + PW.
Đầu tiên cần cấp quyền cho các thành viên của clb thông qua username + PW với username + PW là mssv của họ từ đó để có thể đăng nhập vào máy tính và sử dụng máy tính đó như 1 chiếc

máy tính bình thường, từ đó việc theo dỗ các thành viên sử dụng nguồn tài nguyên của mái tính sẻ được ghi nhận lại thông qua phần mềm chứa username + PW được phân quyền, từ đó viêc sinh viên sử dụng các nguồn tài nguyên như thế nào thì người quản lý cũng có thể theo dõi được.
Lý do sử dung: việc phân vùng cấp quyền cho username + PW
-đầu tiên sẽ quản lý được việc sử dụng tài nguyên mái tính của mỗi thành viên là như thế nào.
- có thể sử dựng với sl thành viên nhiều hơn 20 bạn thành viên vì không phải lúc nào thành viên đó chỉ sử dụng một máy duy nhất so với mỗi cá nhân thành viên sử dụng 1 cái máy thành máy cá nhân,

Tình huống 2:

Trung tâm tin học của khoa 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_iuh.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 website này. 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 thẻ ngân hàng thanh toán. Thông tin các khóa học cũng được website 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.

1. **Bạn liệt kê ít nhất 2 nhóm hoạt động/chức năng nào của hệ thống website trong tình huống trên cần cài đặt các cơ chế bảo mật để nâng cáo tính bảo mật và an toàn cho hoạt động/chức năng đó. Nêu lý do tại sao**
   - **Các chức năng …….. cần tính sẵn dùng. Nếu mất tính sẵn dùng thì sao…. (phân tích hậu quả)**
   - **Chức năng thanh toán học phí trực tuyến cần nâng cao tính an toàn để có tính xác thực và tính chóng từ chối. Vì sao …. (phân tích hậu quả)**
   - **Chức năng nhập kết quả….**

   Các chức năng như xem, đăng ký và thanh toán học phí cần tính sẵn dùng. Nếu mất tính sẵn dùng thì các sinh viên cần tìm các khóa học cần thiết sẽ rất khó khăn nếu như không có được sự gúp đỡ của người khác, việc đk khóa học sẽ rất khó khăn cho người có nhu cầu bên cạnh đó sẽ gây khó chịu cho người xem, việc thanh toán sẽ trở nên khó khăn cho người dùng vì nó gây ra hậu quả nghiêm trọng

   - Chức năng thanh toán học phí trực tuyến cần được nâng cao tính an toàn để có tính xác thực và chống từ chối. Vì khi hệ thống thanh toán trực tiếp không được nâng cao sẽ gây ra các tình trạng hacker tìm ra các lỗ hỏng để lấy đi số tiền mà sinh viên trực tiếp đk, từ đó gây ra hậu quả nghiêm trọng như sinh viên có đăng kí và thanh toán mà không có tên trong khóa học gây ra sự tranh cãi và mất đi lòng tin của sinh viên đối với hệ thông thanh toán của website.
2. **Bạn sẽ dùng cơ chế bảo mật nào (mã/giải mã đối xứng/bất đối xứng, hàm băm, chữ ký số, chứng thư số, xác thực thông điệp, xác thực thực thể,…) để áp dụng cho các từng nhóm hoạt động/chức năng đã nêu ở trên. Trình bày, giải thích cách cài đặt/cấu hình cho cơ chế đó. Nêu lý do tại sao chọn cơ chế này mà không chọn cơ chế khác**

   Thanh toán/đóng HP: bảo mật 2 lớp, lý do

   Lớp 1: Username + PW

   Lớp 2: OTP/~~Chữ ký số~~

Dữ liệu cần bảo mật: Thông tin cá nhân (SV, KH, GV, …), KQ học tập, số dư, đơn hàng : Username + PW

Dữ liệu cần tính toàn vẹn: Thông tin của khóa học, thông tin sản phẩm, thông tin of dịch vụ, thông tin đơn hàng: username + PW

Lý do, phân tích hậu quả

Thanh toán/đóng HP: bảo mật 2 lớp, lý do

Lớp 1: Username + PW

Lớp 2: OTP/

Cần được sử dụng 2 lớp các thực vì khi người xấu có thể đột nhập vào bằng Username + PW mà không thể lấy cắp đi số tiền có trong tài khoảng và cần sự xác định của otp vì chỉ người chủ nhật sự mới có thể nhận được mã xác thực otp của hệ thống cung cấp mà không mất đi số tiền của chính mình, khi người chủ trược tiếp sử dụng số tiền trong tài khoảng và thanh toán khi có otp mới thành công 100%.

Dữ liệu cần bảo mật: Thông tin cá nhân (SV, KH, GV, …), KQ học tập, số dư, đơn hàng : Username + PW. Đây là những thông tin mà chỉ người dùng chỉ có username + PW có thể xem và không thể lấy cắp đi thứ gì của người đó. Những thông tin nào cần được bảo mật 1 cách toàn vẹn thông qua Username + PW.

Dữ liệu cần tính toàn vẹn: Thông tin của khóa học, thông tin sản phẩm, thông tin of dịch vụ, thông tin đơn hàng: có thể sử dụng Username + PW có thể xem các thông tin đó để tìm hiểu đúng thông tin 1 cách chính xác từ đó có thể nắm bắt thông tin một cách trực tiếp.

Tình huống 3:
Để phục vụ cho nhu cầu học tập và tra cứu của cán bộ, giảng viên và sinh viên của trường, nhà trường đã xây dựng một *hệ thống thư viện trực tuyến www.thuviendientu.iuh.edu.vn*, hệ thống giúp độc giả (cán bộ, giảng viên và sinh viên của trường) có thể tìm kiếm các loại sách, báo, tạp chí,… Đối với tài liệu điện tử thì độc giả có thể đọc trực tuyến hoặc tải về, đối với sách trong thư viện thì độc giả có thể đăng ký mượn. Độc giả cũng có thể yêu cầu mua các loại tài liệu điện tử và thanh toán phí mua trực tuyến. Hệ thống cũng giúp cho các thủ thư có thể quản lý thông tin mượn và trả sách của độc giả, hệ thống còn có tính năng thông báo nhắc nhở đến hạn trả sách bằng email, tạo báo cáo, thống kê.
Yêu cầu: Với tình huống đã cho, bạn hãy

1. **Chỉ ra ít nhất 2 loại thông tin/dữ liệu/chức năng nào cần nâng cao tính an toàn và nêu lý do tại sao.**
   - Các chức năng như: tìm kím các loại sách, đk mượn sách hoặc tải về đảm bảo tính sản dùng:
   -> nếu như mất đi tính sản dùng thì việc tìm kím 1 cuốc sách là tất khó đối với sinh viên, việc đk mược sách gây khó khăn cho sinh viên, và tải về cũng gây rất khó khăn cho sv, khi mất đi tính sẳn dùng gây cho sinh viên không thể truy cập vào đó, khi không thể truy cập vào đó để thực hiện các công việc cân thực hiện là tìm kím đk mượn sách và tải về.
   - mua các loại tài liệu điện tử và thanh toán phí mua trực tuyến cần được nâng caotinhs an toàn.

-> tài khoản của sinh viên cần được bảo mật khi thanh toán trong lúc giao dình vì các hackwr có thể truy cập và chuyênt tiền của sinh viên qua 1 nơi khác mà không thể thực hiện vào viêck mua sách từ đó gây ra hậu quả làm mất đi lòng tin của sv và gây tiếng xấu cho hệ thống thư viện,

2. **Đưa ra giải pháp để cài đặt nâng cao tính an toàn cho từng loại thông tin/dữ liệu/chức năng ở trên (Trình bày, giải thích cách cài đặt/cấu hình cho cơ chế đó)**

Thanh toán : bảo mật 2 lớp, lý do
Lớp 1: Username + PW
Lớp 2: OTP/
Cần được sử dụng 2 lớp các thực vì khi người xấu có thể đột nhập vào bằng Username + PW mà không thể lấy cắp đi số tiền có trong tài khoảng và cần sự xác định của otp vì chỉ người chủ nhật sự mới có thể nhận được mã xác thực otp của hệ thống cung cấp mà không

mất đi số tiền của chính mình, khi người chủ trược tiếp sử dụng số tiền trong tài khoảng và thanh toán khi có otp mới thành công 100%.

Tình huống 4:
Để phục vụ nhu cầu học tập và nghiên cứu của cán bộ, giảng viên và sinh viên của trường (gọi chung là độc giả), nhà trường đã trang bị một *phòng đọc sách* cho các độc giả. Phòng này có trang bị máy lạnh, bàn ghế, wifi, và 100 chiếc máy tính để bàn. Sinh viên có thể tự vào ra phòng đọc sách trong khoảng thời gian thư viên mở để ngồi đọc sách, học tập nghiên cứu và dùng các máy tính. Các máy tính chỉ dùng để học tập/nghiên cứu chứ không cho phép chơi game.
Yêu cầu: Với tình huống đã cho, bạn hãy

1. **Đưa và mô tả giải pháp (Trình bày, giải thích cách cài đặt/cấu hình cho cơ chế đó) mà có thể cài đặt để kiểm soát sự vào ra phòng đọc sách của các độc giả một cách tự động và nêu lý do tại sao**
   Cài đặt 1 cửa ra vào được mở/đóng bằng một trong 2 phương pháp: Thẻ từ + Camera hoặc Sinh trắc học + Camera. Nhưng Thẻ từ + Camera hiệu quả hơn
   Thẻ từ là gì, công dụng làm gì, camera dùng làm gì
   - thẻ từ là thẻ mà mỗi sinh viên sau khi nhập học tại trường, khi hoành thành thủ tục nhập học thành công từ đó nhà trường sẽ cấp 1 thẻ từ cho sinh viên sử dụng khi học tập tại trường.
   Công dụng: dùng làm 1 công cụ để quẹt cửa ra vào tại phòng đọc sách của trường với tư vào là sinh viên.
   Camera: dùng để theo dõ mọi hoạt động của sinh khi họ bước vào phòng đọc sách bên cạnh đó khi 1 người ngoài lợi dụng sinh viên để mở cửa dùm mỗi khi sv sử dụng thẻ để vào và đi theo phía sau, khi có sự mất đồ trong phòng đọc sách cũng có thể dùng lại camera để kiểm tra lại 1 cách chính xác nhất với thời điểm đã xảy ra.

   - Đưa ra ưu điểm của thẻ từ:
     tất cả sinh viên của trường điều có 1 cái thẻ từ riêng biệt cho nên việc tận dụng nó để sử dụng vào phòng đọc sách là thuận tiện nhất, không tốn thêm bất kì chi phí phát sinh ra bên ngoài, ngoại trừ đạt thêm 1 cái cửa để quét thẻ cho việc ra vào.
   - Đưa nhược điểm của sinh trắc học
     Sinh trắc học không được sử dụng trong tình huống vì nó tốn rất nhiều chi phí và thời gian cho việc lấy mẫu để thực hiện sinh trắc học.

   Mô tả việc sinh vào ra như thế nào
   sử dụng thẻ sinh viên để quét vào của ra vào, để từ đó tại khóa cửa có thể nhận biết là sinh viên của trường để mở cửa cho sinh viên bước vào, từ đó hệ thống nhận biết cho nên sẽ mở của cho sv đi vào.

   Thẻ từ + Camera: Thẻ sinh viên hiện tại là thẻ từ luôn nên có thể tận dụng thẻ sv làm thẻo vào ra phòng đọc sách
   Sinh trắc học + Camera: (số lượng sinh viên nhiều → tốn kém thời gian lấy mẫu sinh trắc sinh trắc học)

2. Đưa và mô tả giải pháp (Trình bày, giải thích cách cài đặt/cấu hình cho cơ chế đó) mà có thể kiểm soát việc sử dụng wifi và thiết bị máy móc ở phòng đọc sách và nêu lý do tại sao?

   Username + PW: username chính là mã sinh viên luôn → thuận tiện

Sự dụng Username + PW cấp quyền cho mỗi sinh viên để sử dụng các thiết bị máy và wifi tại phòng đọc sách, sử dụng mssv để làm Username + PW từ đó mỗi sinh viên có thể thuận tiện cho việc sử dụng của mỗi sinh viên, người quản lý có thể tìm và thấy những gì mà sinh viên có thể đã sử dụng các nguồn tài nguyên của phòng học như: thiết bị, sách, wifi.. có thể quản lý được việc làm của sinh viên 1 cách dễ dàng nhất. Trong trường học các thiết bị hư hỏng hay bị mất đề điều có thể tìm thấy sinh viên nào đã làm.