Soan Ly thuyet - Tong hop

Nhập môn lập trình (Trường Đại học Công nghiệp Thành phố Hồ Chí Minh)

MỤC LỤC

LƯU Ý: Nhấn (Ctrl + Câu muốn chọn). Sẽ tự động nhảy đến câu cần tìm.

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

- Ứng dụng trong Hàm băm trong thực tế 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.

+ Chữ ký số : Hầu như tất cả các lược đồ chữ ký số đều yêu cầu tính toán bản tóm lược của thông điệp bằng các hàm băm mật mã. Điều này cho phép việc tính toán và tạo chữ ký được thực hiện trên một khối dữ liệu có kích thước tương đối nhỏ và cố định thay vì trên toàn bộ văn bản dài. Tính chất toàn vẹn thông điệp của hàm băm mật mã được sử dụng để tạo các lược đồ chữ ký số an toàn và hiệu quả.

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

- Một phương pháp xác thực thông điệp là mã chứng thực thông điệp (MAC) vì :

+ Một hàm và một khóa bí mật tạo ra một giá trị có chiều dài cố định sử dụng để chứng thực.

+ Là một kỹ thuật xác thực, nó sử dụng một khóa bí mật (mà chỉ người gửi và người nhận biết) cùng với một hàm để tạo ra một giá trị có chiều dài cố định (gọi là checksum -Mã kiểm sai hoặc MAC)

+ Khi trước để tạo ra MAC thường sử dụng mật mã khối (block cipher – như DES) nhưng ngày nay người ta thường sử dụng hàm băm nên nhiều khi mất bồ sẽ thấy HMAC nhiều hơn là MAC (H là viết tắt của Hash đó).

+ MAC sau đó được tích hợp với bản rõ thành tập thông điệp gửi đi trên khênh truyền không an toàn.

+ Người nhận sau khi nhận được thông điệp sẽ lấy bản rõ và một lần nữa dùng cơ chế trên để tạo ra MAC. Nếu MAC lúc này (mới tạo) trùng MAC kèm theo thông điệp thì xác thực thành công (Cơ chế gần giống phương pháp xác thực bằng hàm băm).

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

- 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 và được trao đổi khóa như sau :

+ Trong giao thức Diffie-Hellman hai bên tạo một symmetric session key mà không cần KDC.

+ Hai bên chọn p (nguyên tố lớn – 1024-bit), g là phần tử sinh trong nhóm <Zp*,x>, không cần bí mật (được công khai).

+ Các bước của giao thức thực hiện như sau:

- Alice chọn ngẫu nhiên số lớn x với 0<=x<=p-1,tính R1 = gx mod p.
- Bob chọn số lớn y với 0<=y<p-1, tính R2 = gy mod p
- Alice gửi R1 cho Bob (lưu ý là không gửi x).
- Bob gửi R2 cho Alice (lưu ý là không gửi y).
- Alice tính Symmetric Key K = (R2)x mod p
- Bob tính Symmetric key K= (R1)y mod p
- Giá trị của K giống nhau giữa Alice và Bob:

K=(gx mod p)y mod p=(gy)mod p)x mod p =gxy 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.

4) Trình bày giao thức trao đổi khóa Station to Station. Hãy so sánh giao thức này với giao thức trao đổi khóa Diffie-Hellman.

- Là một giao thức dựa trên Diffie-Hellman
- Dùng Digtal signature với Public-key Certificates để thiết lập nên session key giữa Alice và Bob
- Giao thức này ngăn chặn được tấn công man-in-the-middle.Sau khi chặn R1, Eve không thể gửi R2 của cô ta cho Alice và giả bộ nó được gửi đến từ Bob bởi vì Eve không thể giả mạo được Private key của Bob để tạo ra Sinature – Signature không thể được thẩm tra bằng public key của Bob được xác định trong Certificate. Cùng cách tương tự Eve không thể giả private key của Alice để ký thông điệp thứ 3 gửi bởi Alice.
- So sánh giao thức này với giao thức trao đổi khóa Diffie-Hellman.

+ Điểm giống : Alice và Bob có thể tạo ra một session key giữa chúng mà không cần dùng một KDC. Phương pháp tạo session-key này được tham chiếu như một symmetric-key agreement.

+ Điểm khác:

- Station of Station : Dùng Digtal signature với Public-key Certificates để thiết lập nên session key giữa Alice và Bob và ngăn chặn được tấn công man in the middle
- Diffie – Helman : Dễ bị tấn tấn công man in the middle

5) 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 phiên là một khóa đối xứng sử dụng một lần được sử dụng để mã hóa tất cả các thông báo trong một phiên giao tiếp.

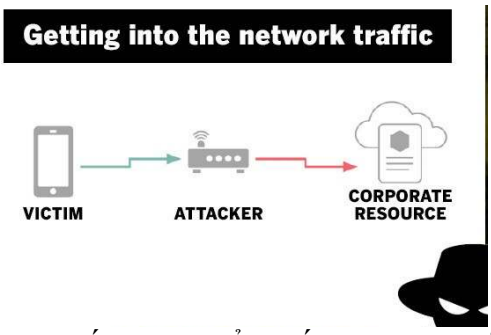
+ Một thuật ngữ có liên quan chặt chẽ là khóa mã hóa nội dung (CEK), khóa mã hóa lưu lượng (TEK) hoặc khóa đa hướng đề cập đến bất kỳ khóa nào được sử dụng để mã hóa tin nhắn, trái với các mục đích sử dụng khác như mã hóa các khóa khác (khóa mã hóa khóa (KEK) hoặc gói khóa Chìa khóa)

- Ưu điểm của khóa phiên (Session Key) so với khóa bí mật chia sẻ (secret key): Chỉ dùng một lần, thường chỉ dùng trong giao thức truyền thông – web traffic.

6) 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.

- Tấn công Man-in-the-middle: Còn được gọi là tấn công xen giữa, 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.

- Vẽ mô hình:



- Giải thích một giao thức/cơ chế mà có thể bị tấn công này tấn công:

+ Bước 1: Kẻ xấu sẻ hỏi về chìa khóa công khai của nạn nhân.

+ Bước 2: Gửi một thông điệp giả mạo.

Ví dụ: Giả sử A muốn liên lạc với B. Trong khi đó, M muốn chặn cuộc đối thoại để nghe trộm và có thể gửi tin sai cho B.

+ Đầu tiên, A hỏi B về chìa khóa công khai của mình. Nếu B gửi chìa khoá công cộng của mình đến A, nhưng M có thể chặn nó, một cuộc tấn công xen giữa có thể bắt đầu. M gửi một thông điệp giả mạo đến A mạo nhận rằng nó đến từ B, nhưng thiệt ra đó là khóa công khai của M.

+ Alice, tin rằng khóa công khai này là của B, mã hóa tin nhắn của cô bằng chìa khoá của M và gửi tin nhắn được mã hóa về B. M một lần nữa chặn lại, giải mã tin nhắn sử dụng khóa riêng của mình, có thể thay đổi nó nếu cô ấy muốn và mã hóa lại nó bằng khóa công khai mà B gửi cho A. Khi B nhận được thông tin mới mã hóa, anh tin rằng nó đến từ A.

=> Thí dụ này cho thấy sự cần thiết của A và B phải có một số cách để đảm bảo rằng họ thực sự sử dụng các mật mã khóa công khai của nhau, chứ không phải là khóa công khai của kẻ tấn công. Nếu không, các cuộc tấn công như vậy nói chung có thể xảy ra, về nguyên tắc, đối với bất kỳ thông tin nào được gửi bằng công nghệ khoá công khai. Một loạt các kỹ thuật khác nhau có thể giúp bảo vệ chống lại các cuộc tấn công MITM.

7) 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?

- Khái niệm chứng chỉ số:

+ Chứng chỉ số (Hay còn gọi là Chứng chỉ SSL) là một tệp tin điện tử được tạo ra bởi các công ty bảo mật hàng đầu thế giới để xác minh một cá nhân, chủ thể, website… riêng biệt trên môi trường Internet.

+ Có thể hiểu giống như việc mỗi gia đình đều có một số nhà riêng, hay mỗi cá nhân đều sở hữu một chứng minh nhân dân riêng biệt.

- Các thành phần và công dụng của chứng chỉ số:

+ Dữ liệu cá nhân của chủ sở hữu chữ ký số: Dữ liệu cá nhân là toàn bộ thông tin để xác nhận tính hợp pháp của chủ sở hữu bao gồm các thông tin cần thiết như: Tên, Quốc gia, địa chỉ, Email, Số điện thoại, tên công ty…

+ Public Key của chủ sở hữu: Public Key (Khóa công khai) là giá trị mà nhà cung cấp chứng chỉ số đưa ra để chứng thực quyền sở hữu chứng chỉ số và được mã hóa trên môi trường Internet và tạo thành cặp mã khóa đối xứng giữa chủ sở hữu và người bán chứng chỉ số.

+ Chữ ký của CA Cấp chứng chỉ (CA viết tắt của Certificate Authority): Chữ ký của CA cấp chứng chỉ được gọi là chứng thực gốc. Đây là chữ ký đại diện của CA xác nhận chứng chỉ số đang có là hợp lệ. Do đó khi kiểm tra chứng chỉ số đầu tiên phải kiểm tra xem chữ ký của CA có hợp lệ hay không nhé. Cái này cũng tương đương giống như chữ ký xác nhận hay con dấu của Công An Tỉnh nơi bạn làm Chứng Minh Thư.

- Cơ quan/công ty nào cung cấp các Certificate ở Việt Nam và cách dùng:

+ Các cơ quan/công ty: Hosting Việt, Comodo, Godaddy, Namecheap,…

+ Cách dùng: Kích hoạt chứng chỉ -> Tạo file Bundle (chứng chỉ của comodo, godaddy) -> Cài đặt chứng chỉ SSL

8) 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:

+ Passwords, One-Time Password, SMS OTP, Token Key (Token card), Smart OTP.

- Phương pháp nào là hiệu quả nhất hiện nay là: Smart OTP.

- Giải thích: Có thể được sử dụng mọi lúc mọi nơi vì được tích hợp sẵn trên ứng dụng của điện thoại. Thanh toán tiền online dễ dàng thông qua Smart OTP với ngân hàng.

- Mô tả phương pháp:

+ Smart OTP là sự kết hợp hài hoà giữa Token Key và SMS OTP.

+ Smart OTP có thể được sử dụng mọi lúc mọi nơi vì nó được tích hợp sẵn trên ứng dụng của điện thoại. Khi có phiên giao dịch trực tuyến thì Smart OTP sẽ được gửi về ứng dụng trên smartphone.

+ Hai ngân hàng đã sử dụng cách thanh toán tiền Online bằng phương thức Smart OTP và SMS OTP là Vietcombank và TPBank. Người dùng phải kê khai thông

tin và đăng ký trực tiếp với ngân hàng họ muốn. Lưu ý, mỗi thiết bị chỉ nên dùng 1 mã OTP riêng biệt.

9) 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 một kĩ thuật cho phép một bên (party) chứng minh sự nhận dạng (identify) của một bên khác. Trong đó thực thực thể(entity) có thể là một người hoặc tiến trình hoặc server. Thực thể mà idenity cần chứng minh được gọi là người thỉnh cầu (claimant). Bên mà cố gắng chứng minh identity của cliamant được gọi là người thẩm định (verifier).
- Ưu điểm và nhược điểm của phương pháp:

+ Ưu điểm: Là phép đo lường về các đặc tính sinh lý học hoặc hành vi học mà nhận dạng một con người (Không thể đoán, đánh cắp hoặc chia sẻ). Không đòi hỏi con người phải ghi nhớ như mật khẩu hoặc mã pin. Luôn có tính sẵn dùng cho cá nhân và duy nhất.

+ Nhược điểm: Tốn nhiều chi phí lắp đặt cho thiết bị phần cứng. Sẽ có những lỗi nhất định như: Từ chối người dùng hợp lệ, chấp nhận người dùng không hợp lệ.

- Phương pháp này thường được áp dụng ở đâu:

+ Ngân hàng: Nhận diện khách hàng.
+ Nhà nước: Đăng ký thẻ căn cước.
+ Điện thoại thông minh: Nhận diện người dùng.

10) Khóa là gì? Có mấy loại khóa, đặc tính của khóa, công dụng từng loại khóa,các phát sinh của từng loại khóa.

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

- Có 3 loại khóa thường dung:

  + Khóa bí mật

  + khóa riêng tư (private key) và khóa công khai (public key)

- Đặc tính và công dụng của từng loại khóa:

  + Khóa bí mật: là loại khóa được sử dụng trong thuật toán mã hóa đối xứng. Loại khóa này sử dụng chung cho cả mã hóa và giải mã (1key duy nhất) yêu cầu bí mật chỉ có người giử và người nhận biết tuyệt đối không được để kẻ thứ 3 biết được.

  + Khóa công khai và khóa riêng tư: là loại khóa được sử dụng trong thuật toán mã hóa bất đối xứng. Mỗi người đều có 1 cặp khóa công khai và riêng tư của

mình và chia sẻ khóa công khai cho tất cả mọi người đều biết tuy nhiên khóa riêng tư phải giữ bí mật chỉ có chủ nhân khóa mới biết. Hai loại khóa này dùng để mã hóa và giải mã theo những phương thức khác nhau mà đáp ứng nhu cầu khác nhau của người sử dụng như đảm bảo tính bảo mật hay xác thực thông điệp.

- Cách phát sinh:

+ Khóa bí mật: người mã hóa chọn khóa ngẫu nhiên hay theo một quy luật toán học nhất định và truyền khóa và bản mã cho người nhận để người nhận dùng khóa đó giải mã bản mã vừa nhận được

+ Khóa riêng tư, khóa công khai: Mỗi người tự đăng kí cho mình một cặp khóa riếng tư và công khai cho trung tâm quản lí và phân phối khóa.

11) Định nghĩa hàm băm. Hàm băm (Hash) dùng để giải quyết vấn đề gì trong bảo mật thông tin hiện đại? Hai hàm băm thường được dùng là gì? So sánh hai hàm băm này? Cho biết các ứng dụng của hàm băm và cho ví dụ minh họa

- Định nghĩa hàm băm: 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 băm là duy nhất, không thể suy ra nội dung thông điệp bằng giá trị băm này (hàm 1 chiều)

- Hàm băm giải quyết vấn đề của hai bài toán về chứng thực thông điệp và tính toàn vẹn dữ liệu của an toàn và bảo mật thông tin.

- Hàm băm thường dùng hiện nay là: MD5 và SHA1.

- So sánh hai hàm MD5 và SHA1:

+ Khả năng chống lại tấn công:

- Để tạo ra thông điệp có giá trị băm cho trước, cần 2^{128} thao tác với MD5 (giá trị băm 128 bit) và 2^{160} với SHA1 (giá trị băm 160 bit)
- Để tìm 2 thông điệp có cùng giá trị băm cần 2^{64} thao tác với MD5 và 2^{80} với SHA1

+ Khả năng chống lại thám mã: cả 2 đều có cấu trúc tốt.

+ Tốc độ:

- Cả 2 dựa trên phép toán 32 bit, thực hiện tốt trên các kiến trúc 32 bit.
- SHA1 thực hiện nhiều hơn 16 bước và thao tác trên thanh ghi 160 bit nên tốc độ thực hiện chậm hơn.

+ Tính đơn giản: Cả hai đều được mô tả đơn giản dễ dàng cài đặt trên phần cứng và phần mềm.

- Các ứng dụng của hàm băm và ví dụ:

  + Lưu mật khẩu

  + Tạo chữ kí điện tử

  + Đấu giá trực tuyến.

  + Trong Download file

  Ví dụ về 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.

12) Trình bày, giải thích và cho ví dụ minh họa về các tính chất của hàm băm

- Các tính chất của hàm băm:

+ Tính 1 chiều (Preimage resistant – one –way property) : cho trước giá trị băm h, việc tìm bản rõ x sao cho khi băm x thành h(x) mà bằng với giá trị băm bản gốc h(x) =h là rất khó. Ví dụ:

+ 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 ($x' \neq x$) sao cho h(x')=h(x) là rất khó. Ví dụ:

+ 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 lí ngày sinh – Birthday paradox) Ví dụ:

13) Về mặt lý thuyết, giá trị Hash có thể trùng không? Vậy tại sao nói giá trị Hash có thể xem là "dấu vân tay của thông điệp"?

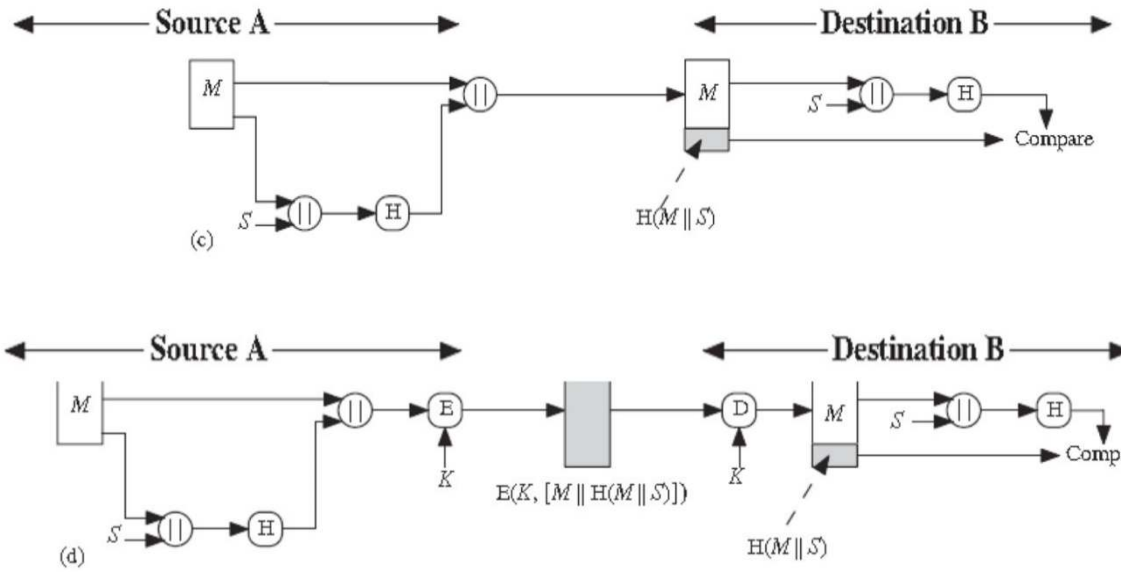
Về lí thuyết, giá trị Hash là duy nhất không thể trùng. Hàm Hash tạo nên dấu vân tay (tức là thông tin đặc trưng) của một tệp, mẩu tin hay dữ liệu h = H(M) Nén mẩu tin có kích thước tùy ý về dấu vân tay có kích thước cố định. Hàm Hash được giả thiết là công khai, mọi người đều biết cách sử dụng.

14) Xác thực thông điệp là gì, nêu và giải thích các phương pháp xác thực thông điệp (đưa ra các mô hình để minh họa và giải thích).

Xác thực thông điệp liên quan đến các khía cạnh sau khi truyền tin trên mạng đảm bảo bảo vệ tính toàn vẹn của thông điệp tức là bảo vệ thông điệp không bị sửa đổi hặc các biện pháp phát hiện nếu thông điệp bị thay đổi trên đường truyền. Xác thực danh tính, nguồn gốc chống thoái thác Không từ chối bản gốc.

Các mô hình minh họa:

• Ví dụ cơ chế chứng thực đơn giản (tt)



15) Chữ ký số là gì? Nêu các ứng dụng cụ thể của chữ ký điện tử. Nêu những lợi ích cơ bản khi áp dụng chữ ký số?

Chữ ký số (hay còn gọi là chữ ký điện tử) là thông tin đã được mã hóa bằng khóa riêng của người gửi, được gửi kè theo văn bản nhằm đảm bảo cho ngời nhận định danh, xác thực đúng nguồn gốc và tính toàn vẹn của tài liệu nhận

- Ứng dụng cụ thể của chữ ký số:

  + Xác thực thông điệp(Message Authentication) người ký được xác nhận là chủ chữ ký.

  + Toàn vẹn thông điệp (Message Integrity) Nội dung chưa bị thay đổi hoặc xáo trộn kể từ khi nó được kí điện tử.

  + Chống từ chối (Non-repudiation) Chứng minh tất cả các bên về nguồn gốc của nội dung đã ký. Từ " thoái thác" dùng để chỉ hành động của một người kí từ chối bất kì mối liên kết nào với nội dung đã kí.

  + Bảo mật (Confidentiality)

- Lợi ích cơ bản của việc sử dụng chữ kí số:

16) Trình bày và giải thích giao thức trao đổi khóa Diffie-Hellman. Nêu ưu điểm và nhược điểm của giao thức trao đổi khóa Diffie-Helman. Diffie-Helman có phải là một phương pháp mã hóa công khai không? Giải thích tại sao có hoặc tại sao không?

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 X_A và tính khóa công khai Y_A dựa trên khóa bí mật qua công thức $Y_A = G^X \bmod P$ sau đó gởi khóa Y_A cho B.

Tương tự, bên B cũng chọn một khóa bí mật y tính khóa công khai Y_B bằng công thức $Y_B = G^y \bmod P$. sau đó gởi Y_B 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: $K=(Y_B)^X \bmod P$

Secret Key by user B: $K= (Y_A)^Y \bmod P$

- Ưu điểm:

Giao thức là an toàn đối với việc tấn công thụ động. nghĩa là một người thứ 3 dù biết b_A và b_B thì cũng sẽ rất khó mà biết được $K_{A,B}$.

17) Tấn công phát lại thông điệp là gì? Nêu tác hại của tấn công phát lại thông điệp và so sánh với việc sửa lại thông điệp và mạo danh. Nêu các phương pháp chống lại tấn công phát lại thông điệp

- Tấn công phát lại thông điệp là hình thức tấn công kẻ thứ 3 sao chép thông điệp của bên gởi sau một thời gian kẻ thứ 3 này tiến hành gởi thông điệp đã sao

chép cho người nhận, người nhận cứ tin rằng đây là thông điệp do người đầu tiên gởi (do 2 thông điệp có cùng một nội dung)

- Tác hại:

- Phương pháp cống lại tấn công phát lại thông điệp: đảm bảo an toàn trên kênh truyền và đảm bảo tính bảo mật cũng như toàn vẹn dữ liệu bằng các biện pháp sử dụng các thuật toán mã hóa, hàm băm, chữ kí điện tử….nhằm xác minh danh tính của người gởi cũng như toàn vẹn về nội dung thông điệp.

18) Session Key là gì? Nêu và giải thích một giao thức để tạo một Session Key giữa hai người dùng (Alice và Bob).

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)

- Giao thức để tạo thành một Session Key:

+ A gởi yêu cầu đến KDC để nhận được khóa phiên nhằm thực hiện truyền thông với B (bao gồm định danh A, B, và một định danh duy nhất N_1 cho phiên gọi là Nonce: nhãn thời gian, biến đếm, số ngẫu nhiên)

+ KDC trả lời yêu cầu bằng 1 tin tức được mã hóa bằng khóa K_a . A là người duy nhất nhận được tin tức .

+ A giữ khóa phiên K_s để dùng liên lạc, và gửi về phía B một thông tin đã nhận được từ trung tâm (EK_b [K_s || ID_A), người B biết được khóa phiên K_s và biết được thông tin nhận được đã được gử từ KDC (do mã hóa bằng K_b)

+ Phía B gửi cho A 1 nonce mới N_2 đã được mã hóa bằng khóa phiên đã nhận được.

+ Nhờ khóa phiên K_s , A trả lời lại f(N_2) cho B.

⇨ Các bước 1,2,3 --→ phân phối khóa

Bước 3,4,5→ Xác thực.

19) Chứng thực thực thể là gì? Tại sao khi xây dựng một hệ thống thông tin thì phải xây dựng cơ chế chứng thực thực thể? Nêu những phương pháp chứng thực thực thể hiện có hiện nay.

Chứng thực thực thể là một kĩ thuật được thiết kế cho phép một bên(party) chứng minh sự nhận dạng (identity) của một bên khác.

- Xác thực thực thể là tạo ra liên kết giữa định danh và đối tượng, thực thể gồm 2 bước: Chủ thể cung cấp một định danh trong hệ thống , chủ thể cung cấp thông tin xác thực có thể chứng minh sự liên kết giữa định danh và chủ thể.

20) 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.

21) 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….

22) Chữ ký điện tử là gì? Mục tiêu của chữ ký điện tử? Trình bày hiện trạng áp dụng chữ ký điện tử ở Việt Nam

(gợi ý: Định nghĩa chữ ký điện tử: ứng dụng của mã hóa khóa công khai, người dùng có (PU_A, PR_A); Tạo chữ ký: $S_{AM}=E(M,PR_A)$ – giải thích; Thẩm tra chữ ký $D(S_{AM}, PU_A)$ -→ Yes/No – Giải thích; Mục tiêu của chữ ký số; Hiện trạng áp dụng chữ ký: 4 lĩnh vực đó là cơ quan Thuế, Bảo hiểm xã hội, Hải quan và Chứng khoán)

• **Chữ ký điện tử** :là đoạn thông tin đi kèm với dữ liệu. Những dữ liệu bao gồm: hình ảnh, video, văn bản…. Chữ ký điện tử thường được sử dụng trong các giao dịch điện tử. Nhằm mục đích để chứng thực tác giả đã ký vào dữ liệu đó. Chữ ký điện tử là một thay thế cho chữ ký viết tay của cá nhân hay doanh nghiệp.

Mục tiêu của chữ ký điện tử:

• **Xác thực (Authentication):** là quá trình kiểm tra danh tính của một tài khoản bất kỳ đang truy cập vào hệ thống hiện tại với cơ sở nền tảng thông qua chữ ký điện tử riêng của chính người truy cập. Nếu không có bước này thì hệ thống sẽ không xác định được người truy cập là ai,từ đó không thể đưa ra các phản hồi phù hợp.

• **Chống phủ nhận (Non-repudiation:** là yếu tố trụ cột của đảm bảo an toàn thông tin. Ở đây có thể hiểu là bảo đảm việc truyền đi và nhận lại thông tin giữa người gửi với người nhận qua công nghệ như chữ ký kỹ thuật số .Tính chống phủ nhận là cam kết xác thực, người gửi sẽ không thể chối bỏ những gì mình đã gửi. Tương tự như vậy, bên nhận sẽ không thể phủ định việc mình đã nhận thông qua bản hợp đồng kỹ thuật số và chữ ký điện tử từ hai bên xác nhận

→ Lợi ích,ứng dụng: (mở rộng)

+Quy trình đơn giản:

Bước 1: Tạo file dữ liệu định dạng .docx

Bước 2: Tạo chữ ký điện tử

Bước 3: Người nhận chèn chữ ký vào văn bản, tài liệu

Bước 4: Hoàn tất chữ ký điện tử

+ Nâng cao trình độ sử dụng công nghệ thông tin; Chữ ký điện tử không chỉ sử dụng cho Khai thuế điện tử mà còn sử dụng cho các giao dịch điện tử Hải Quan, Ngân hàng, Chứng khoán, bảo hiểm xã hội….

+ **Việc ứng dụng rộng rãi chữ ký điện tử giúp doanh nghiệp tiết kiệm chi phí hành chính, giảm thời gian thủ tục**: Hoạt động giao dịch điện tử cũng được nâng tầm đẩy mạnh phát triển nhanh hơn. Không mất thời gian đi lại, chờ đợi.

. Không phải in ấn các hồ sơ khai báo thuế.

. Việc ký kết các văn bản ký điện tử có thể diễn ra ở bất kỳ đâu, bất kỳ thời gian nào một cách dễ dàng, tiện lợi và nhanh chóng

<u>-Trình bày hiện trạng áp dụng chữ ký điện tử ở Việt Nam:</u>

Được áp dụng trên nhiều lĩnh vực và chú trọng phát triển cung cấp dịch vụ công trực tuyến thông qua việc ứng dụng Chữ ký điện tử và tiêu biểu nhất ở 4 mảng chính :

+Thuế: Tính đến 31/3/2019, số lượng DN đã đăng ký tham gia sử dụng dịch vụ công trực tuyến với cơ quan thuế là 703.753 DN (không bao gồm các đơn vị chi nhánh, trực thuộc) trên tổng số 711.748 DN đang hoạt động, đạt tỷ lệ 98,87%.

+Hải quan: việc cung cấp dịch vụ công trực tuyến là một trong những công việc quan trọng đã và đang được ngành Hải quan triển khai thực hiện trong nhiều năm qua. Hiện nay, Tổng cục Hải quan đang cung cấp 181 dịch vụ công trực tuyến ứng dụng chữ ký điện tử để xác thực các dịch vụ như: Hệ thống VNACCS/VCIS Cổng thông tin một cửa quốc gia và Cổng thanh toán điện tử thu thuế xuất nhập khẩu Cổng thông tin điện tử Hải quan.

+ **BHXH**: sau gần 03 năm kể từ khi Thủ tướng Chính phủ ban hành Quyết định số 08/2015/QĐ-TTg ngày 09/3/2015 về giao dịch điện tử trong việc thực hiện thủ tục tham gia BHXH, bảo hiểm y tế, bảo hiểm thất nghiệp và đề nghị cấp sổ BHXH, thẻ

bảo hiểm y tế, dịch vụ công trực tuyến ứng dụng chữ ký điện tử của ngành BHXH đã có những phát triển cả về số lượng và chất lượng.

+ **Chứng khoán**: hiện nay, Ủy ban Chứng khoán Nhà nước đang sử dụng Chữ ký điện tử trong các hệ thống như: hệ thống giám sát giao dịch chứng khoán; phần mềm quản lý báo cáo thống kê nội bộ; hệ thống cơ sở dữ liệu (CSDL) quản lý công ty quản lý quỹ và quỹ đầu tư; hệ thống CSDL quản lý công ty chứng khoán; hệ thống CSDL quản lý nhà đầu tư nước ngoài; hệ thống công bố thông tin.

23) Đưa ra một hệ thống thông tin hoặc một trang web thực tế ở Việt Nam mà có sử dụng chữ ký điện tử? Nghiệp vụ nào trong hệ thống đó có sử dụng chữ ký số? Trình bày các bước cụ thể để người dùng trong hệ thống này thực hiện nghiệp vụ có sử dụng chữ ký số.

(gợi ý: Website của cơ quan Thuế, Wibsite của cơ quan Hải quan, Website của cơ quan Bảo hiểm xã hội, ...)

+Đưa tra 1 hệ thống thông tin hoặc 1 trang web thực tế ở Việt Nam mà có sử dụng chữ ký điện tử?

Website của cơ quan Thuế Việt Nam Tổng Cục Thuế - Bộ Tài Chính

+Nghiệp vụ nào trong hệ thống đó có sử dụng chữ ký số?

Chữ ký số trong các giao dịch hành chính công như: Kê khai thuế, sử dụng để ký hóa đơn điện tử, nộp tiền thuế và tờ khai,…

+Trình bày các bước cụ thể để người dùng trong hệ thống này thực hiện nghiệp vụ có sử dụng chữ ký số

Bước 1: Đăng nhập vào Trang thông tin điện tử của Tổng cục Thuế

Bước 2: Lập giấy nộp tiền

Bước 3: Khai báo thông tin trên tờ khai

Bước 4: Ký số

24) Chứng thư số là gì? Mục tiêu của chứng thư số? Hiện nay Việt Nam đã có các đơn vị nào có thể cung cập dịch vụ chứng thư số?

- Chứng thư số là gì?

+Là chứng thực để gắn một chìa khóa công khai với một thực thể (cá nhân, máy chủ, cty,…). Hay nói cách khác, CTS giúp xác định chìa khóa công khai thuộc về thực thể nào.

+Một CTS thường gồm chìa khóa công khai và một số thông tin khác về thực thể sở hữu chìa khóa đó.

+Chứng thư số thuộc sở hữu của nhà cung cấp chứng thư số, viết tắt CA (certificate authority).

-Mục tiêu của chứng thư số: Loại chứng thư này được dùng như một công cụ điện tử giúp nhận diện cá nhân, máy chủ hoặc một số đối tượng khác bằng cách gắn định danh đối tượng đó với một "khóa công khai" được cấp bởi tổ chức có thẩm quyền.

-Hiện nay Việt Nam đã có các đơn vị nào có thể cung cập dịch vụ chứng thư số?

-Hiện nay trên thị trường có gần 20 đơn vị cung cấp chữ ký số điện tử, khiến doanh nghiệp tuy có nhiều sự lựa chọn đa dạng hơn nhưng lại gặp khó khăn trong việc đưa ra quyết định mua của đơn vị nào. Có thể kể đến một vài loại chữ ký số được các doanh nghiệp tin dùng hiện nay như:

1. Chữ ký số điện tử MISA eSign của nhà cung cấp MISA
2. Chữ ký số Viettel – CA của nhà cung cấp Viettel
3. Chữ ký số VNPT – CA của nhà cung cấp VNPT
4. Chữ ký số BKAV – CA của nhà cung cấp BKAV

25) Chứng thư số là gì? Nội dung có trong chứng thư số là gồm những nội dung gì?

- Chứng thư số là gì:

+Là chứng thực để gắn một chìa khóa công khai với một thực thể (cá nhân, máy chủ, cty,…). Hay nói cách khác, CTS giúp xác định chìa khóa công khai thuộc về thực thể nào.

+Một CTS thường gồm chìa khóa công khai và một số thông tin khác về thực thể sở hữu chìa khóa đó.

+Chứng thư số thuộc sở hữu của nhà cung cấp chứng thư số, viết tắt CA (certificate authority).

***Nội dung có trong chứng thư số gồm :**

-Tên của tổ chức cung cấp dịch vụ chứng thực chữ ký số.

-Tên của thuê bao.

-Số hiệu chứng thư số.

-Thời hạn có hiệu lực của chứng thư số.

-Khóa công khai của thuê bao.

-Chữ ký số của tổ chức cung cấp dịch vụ chứng thực chữ ký số.

-Các hạn chế về mục đích, phạm vi sử dụng của chứng thư số.

-Các hạn chế về trách nhiệm pháp lý của tổ chức cung cấp dịch vụ chứng thực chữ ký số.

-Thuật toán mật mã.

-Các nội dung cần thiết khác theo quy định của Bộ Thông tin và Truyền thông

26) Chứng thực thực thể là gì? Trình này 2 phương pháp mà bạn biết mà có thể cài đặt để chứng thực thực thể.

-Khái niệm: Chứng thực thực thể là một kĩ thuật cho phép một bên (party) chứng minh sự nhận dạng (identify) của một bên khác

Trong đó thực thực thể(entity)có thể là một người hoặc tiến trình hoặc server. Thực thể mà idenity cần chứng minh được gọi là người thỉnh cầu (claimant)Bên mà cố gắng chứng minh identity của cliamant được gọi là người thẩm định (verifier)

-Xác thực thực thể là tạo ra liên kết giữa định danh và đối tượng, thực thể gồm 2 bước

+Chủ thể cung cấp một định danh trong hệ thống

+Chủ thể cung cấp thông tin xác thực có thể chứng minh sự liên kết giữa định danh và chủ thể

-Trình này 2 phương pháp mà bạn biết mà có thể cài đặt để chứng thực thực thể.

❖ **+Chứng thực password:**

Chứng thực mật khẩu là phương pháp đơn giản và lâu đời nhất, được gọi là Password-based Authentication, password là một thứ mà claimant biết.

+Một Password được dùng khi một người dùng cần truy xuất một hệ thống để sử dụng nguồn tài nguyên của hệ thống.

+Mỗi người dùng có một định danh người dùng (user identification) công khai và một password bí mật.

- Có 2 cơ chế password:

- Fixed password: Là một password được dùng lặp đi lặp lại mỗi lần truy xuất.
- One-time password: Là một password mà được sử dụng chỉ một lần. Loại password này làm cho các tấng công eavesdropping (nghe trộm) và salting vô tác dụng.

Chứng thực bằng Challenge-reponse

- Dùng chứng thực bằng Password, để chứng mnh nhận dạng Claimant cần trình ra password bí mật, tuy nhiên password này có bị tiết lộ
- Với chứng thực bằng Challenge-reponse, ***claimant chứng mình rằng cô ta biết một bí mật (secret) mà không cần gửi chúng đi.*** Nói cách khác, clamant không cần gửi bí mật cho verifier, verifier hoặc có hoặc tự tìm ra chúng
- ***Challege là một giá trị biến đổi theo thời gian được gửi bởi Verifier, Response là kết quả của một hàm được áp dụng trên challenge***

Có 3 hướng chính để tạo nên Challenge-reponse

- Using A Sysmetric-Key Cipher
- Using Keyed-Has Functions
- Using An Asymmetric-Key Cipher
- Using Digital Signature

27) Điều khiển truy cập là gì? Trình bày ít nhất 2 phương pháp mà bạn biết mà có thể cài đặt điều khiển truy cập một hệ thống thông tin.

-Điều khiển truy cập :là quá trình giới hạn *quyền sử dụng* của người dùng đã được chứng thực đối với *tài nguyên hệ thống*, cũng như hạn chế các tác động của người dùng đối với tài nguyên hệ thống và đảm bảo người dùng chỉ tác động được các tài nguyên trong phạm vi được cấp quyền đó.

-Trình bày ít nhất 2 phương pháp mà bạn biết mà có thể cài đặt điều khiển truy cập một hệ thống thông tin.

+Điều khiển truy cập bắt buộc (Mandatory Access Control):

. Việc bảo vệ dữ liệu không được quyết định bởi người dùng thông thường

. Hệ thống yêu cầu phải bảo vệ dữ liệu

. Ví dụ: Thư mục dùng chung trên máy chủ, người dùng không thể thay đổi được

+ Điều khiển truy cập theo người dùng (Role-based Access Control): Quyền truy cập được định nghĩa theo vai trò của người dùng:

* Adminstrator

* Power User

* Dial-up User

28) Mật khẩu (password) là gì? Mật khẩu cố định (fixed password) và mật khẩu dùng một lần (one time password) khác nhau như thế nào? Trình bày điểm mạnh và điểm yếu của 2 loại mật khẩu.

-Mật khẩu (tiếng Anh: Password): thường là một xâu, chuỗi, loạt các ký tự mà dịch vụ internet phần mềm hệ thống máy tính yêu cầu người sử dụng nhập vào bằng bàn phím trước khi có thể tiếp tục sử dụng một số tính năng nhất định.

Mật khẩu có thể đi cặp với tên truy nhập khi hệ thống cần phân biệt các người sử dụng khác nhau. Một mật khẩu thường là khoảng từ 4 đến 16 kí tự, tùy thuộc vào cách các hệ thống máy tính được cấu hình.

-Mật khẩu cố định (fixed password) và mật khẩu dùng một lần (one time password) khác nhau như thế nào?

Mật khẩu cố định (fixed password): là loại mật khẩu được dùng để mở khoá khoá mặc định khi tạo tài khoản người dùng, nó sẽ là mật khẩu đăng nhập lâu dài cho đến khi người dùng thay đổi nó một cách thủ công. Tuy nhiên vì nó được Sử dụng nhiều lần nên Bảo mật thấp, Dễ bị hack và tấn công

Mật khẩu dùng một lần (one time password): là loại mật khẩu sử dụng một lần sẽ mất hiệu lực sau vài phút hay khi người dùng đã thoát khỏi hệ thống. Do đó nó có tính bảo mật cao và sau khi nhập mật khẩu dù mật khẩu có bị lộ cũng không bị xâm nhập

-Trình bày điểm mạnh và điểm yếu của 2 loại mật khẩu.

- **One Time Password:**

- Ưu điểm: bổ sung lớp bảo mật cho tài khoản thanh toán. Cách sử dụng đơn giản, dễ hiểu, tiện lợi. Mức phí dịch vụ thấp. Phổ biến trong nhiều hình thức xác minh chủ thể như tạo tài khoản ngân hàng, mạng xã hội…

- Nhược điểm: mã OTP có thể bị lộ nếu chủ tài khoản giữ thông tin không cẩn thận. Giao dịch thông qua hệ thống internet có thể bị hacker tấn công.

- **Fixed Pasword:**

- Ưu điểm: độ sai lệch ít, thân thiện và dễ sử dụng. Là dạng mật khẩu dự phòng cho các loại bảo mật tân tiến hơn.

- Nhược điểm: đối với những người có nhiều mật khẩu hoặc những người lớn tuổi dễ xảy ra việc quên mật khẩu. Tính bảo mật cao đồng nghĩa với việc sự tiện dụng thấp đi. Bấm nhầm hoặc sai mật khẩu nhiều lần có thể dẫn đến hiện tượng khoá máy.

29) Trình bày các loại mã OPT, nêu ưu điểm và nhược điểm của từng loại?Các loại mã OTP hiện nay và ưu nhược điểm từng loại:

-SMS OTP: Khi bạn thực hiện giao dịch ngân hàng trực tuyến, sau khi xác nhận mã giao dịch trên hệ thống internet banking, sẽ có một mã OTP gởi đến số điện thoại của bạn để bạn xác minh giao dịch trực tuyến này lần thứ 2. Bạn phải nhập mã OTP này để có thể hoàn thành giao dịch.

Ưu điểm: Vừa nhanh, vừa tiện lợi, người dùng có thể copy mã OTP trực tiếp từ tin nhắn sang mục OTP trong tài khoản để thực hiện giao dịch. tạo lớp bảo mật thứ hai cho tài khoản của bạn. Và lớp bảo vệ này sẽ xuất hiện khi phát hiện bất kỳ hoạt động không rõ ràng nào từ tài khoản của bạn.

Nhược điểm: người dùng không thể sử dụng được ở nơi không có sóng di động, hoặc di chuyển ra nước ngoài. Khi đó, buộc bạn phải sử dụng một hình thức nhận OTP khác.

- **Token**: đây là một thiết bị ngân hàng cấp riêng cho bạn khi bạn đăng kí với ngân hàng. Bạn phải trả thêm phí cho thiết bị này. Khi bạn thực hiện giao dịch, đến bước xác minh cuối cùng, thiết bị này sẽ sinh ra mã OTP mặc định để bạn có thể nhập mã và hoàn thành giao dịch.

Ưu điểm: Máy Token có kích thước khá là nhỏ gọn, giúp bạn dễ dàng mang theo bên người cũng như dễ dàng cho vào chùm chìa khóa cá nhân. Giúp bảo vệ các giao dịch của khách hàng, Tránh bị kẻ gian hack thông tin cũng như sử dụng những thông tin để thực hiện giao dịch. Nếu chẳng may bị lộ mã OTP đã sử dụng thì khách hàng cũng không cần quá lo lắng bởi mã đó chỉ có hiệu lực duy nhất một lần. Các sử dụng thiết bị Token khá là đơn giản phù hợp cho rất nhiều đối tượng

Nhược điểm: Bạn có thể dễ dàng nhận ra để sử dụng dịch vụ này thì khách hàng cần phải trả một khoản phí không nhỏ từ 200.000 - 400.000 đồng cho mỗi thiết bị Token. Thời hạn sống của mỗi mã OTP cho có 60s. Bạn cần phải có máy Token thì mới có thể thực hiện giao dịch được

-Smart OTP: đây là một ứng dụng riêng của do từng ngân hàng phát triển. Cho nên, có ngân hàng sẽ có dịch vụ smart OTP và có ngân hàng sẽ không cung cấp dịch vụ này. Đây là ứng dụng được chạy trên 2 hệ điều hành Androi và iOS. Sau khi đăng kí tài khoản và kích hoạt thành công, thì ứng dụng này sẽ hoạt động tương tự các xác thực mã OTP bằng Token.

Ưu điểm: là phương thức xác thực sử dụng công nghệ tiên tiến, bảo mật, thuận tiện cho Doanh nghiệp khi sử dụng các tiện ích của F@st EBank. Nó được coi là hình thức kết hợp hoàn hảo giữa SMS OTP và Token Key. Tự động tạo ra mã xác thực ngẫu nhiên sau một thời gian nhất định. Có thể sử dụng được khắp mọi nơi ngay cả khi bạn di chuyển ra nước ngoài. Cung cấp mã xác thực không cần sóng điện thoại hay mạng Internet.

Nhược điểm: Smart OTP cũng có thể rủi ro đối với những khách hàng sử dụng điện thoại bị bẻ khóa máy hoặc tự ý cài thêm các phần mềm độc hại, không rõ nguồn gốc. Để thực hiện được mọi ứng dụng này để được nhận mã xác nhận OTP bạn cần phải đăng ký dịch vụ với ngân hàng, nhà cung cấp dịch vụ hoặc xác thực thông tin qua SMS OTP. Bên cạnh đó, bạn không thể sử dụng chung trên nhiều thiết bị ứng dụng tạo mã OTP.

30) Đưa ra một hệ thống mà bạn biết có sử dụng mật khẩu cố định (fixed password) và mô tả các bước thực hiện để bạn có thể được chứng thực người dùng trong hệ thống đó. Nêu mục tiêu của việc chứng thực này.

Hệ thống sử dụng mật khẩu một lần là hệ thống Internet Banking

Tình huống : Bạn A muốn sử dụng Internet Banking để chuyển tiền sang tài khoản của người thân thì cần thực hiện các bước sau:

Bước 1: Đăng nhập tên và mật khẩu cố định tài khoản như đã đăng ký với ngân hàng.

Bước 2: Hoàn thành các thông tin giao dịch: tên người nhận, số tiền cần chuyển, hình thức chuyển, phí chuyển khoản, mã khuyến mãi nếu có. Sau khi hoàn thành các bước trên, hệ thống ngân hàng sẽ tự động gửi cho mình một mã gồm 4-6 ký tự qua tin nhắn SMS trên điện thoại đi động.

Bước 3: Vào mục SMS và sao chép mã OTP.

Bước 4: Nhập mã OTP vừa sao chép lên trên ứng dụng. Tiếp đó xác nhận giao dịch lần cuối là bạn có thể chuyển khoản một cách thành công và an toàn cho người thân.

-Mục tiêu của việc chứng thực này: Đảm bảo tính xác *thực* (Authentication): Xác *thực* đúng *thực thể* cần thực hiện giao dịch.

31) Đưa ra một hệ thống mà bạn biết có sử dụng mật khẩu dùng một lần (one time password) và mô tả tình huống mà bạn có sử dụng mật khẩu để chứng thực người dùng/giao dịch. Nêu mục tiêu của việc chứng thực này.

- Mã OTP thường được sử dụng trong dịch vụ giao dịch trực tuyến Emobile Banking của các Ngân Hàng: Mã OTP được sinh ra khi khách hàng sử dụng dịch vụ **Emobile Banking** và đây được xem là một loại hình dịch vụ nhằm tạo sự tiện lợi cho khách hàng trong mỗi lần giao dịch cũng như tăng tính bảo mật cho các lần giao dịch của khách hàng.

- Khi khách hàng thực hiện giao dịch ví dụ như : Chuyển khoản, thanh toán dịch vụ .. Thì khách hàng sẽ nhận được tin nhắn mã OTP từ ngân hàng gửi vào số điện mà khách hàng đã đăng ký với ngân hàng. Và Khách hàng sử dụng mã OTP này để thực hiện bước xác thực cuối cùng cho mỗi lần giao dịch. Ví dụ như khi khách hàng A sử dụng thẻ ATM nội địa để chuyển tiền cho người thân. Sau khi đã hoàn thành tất cả các công đoạn từ chọn số tiền, tài khoản gửi thì ngân hàng sẽ gửi về số điện thoại khách hàng một mã OTP. Và Khách hàng dùng mã này để xác thực giao dịch đang thực hiện

- Mục tiêu: Dùng để bảo mật 2 lớp. Ngoài lớp mật khẩu bạn đăng ký khi sử dụng, thì khi thực hiện giao dịch bạn còn cần phải nhập mã OTP để xác thực. Điều này sẽ đảm bảo an toàn, trong các trường hợp tài khoản bị lộ hoặc bị hack. Nếu bạn bị mất tài khoản, mật khẩu thì kẻ gian cũng không thể thực hiện giao dịch được vì không có mã OTP. Như vậy, bạn không thể thực hiện giao dịch nếu không nhập được mã OTP.

32) Sinh trắc học (biometric) là gì? Nêu các lĩnh vực mà có thể áp dụng sinh trắc học?

-**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. Đây là một công nghệ sử dụng những thuộc tính vật lý hoặc các mẫu hành vi, các đặc điểm sinh học đặc trưng như dấu vân tay, mẫu mống mắt, giọng nói, khuôn mặt, dáng đi,... để nhận diện con người .

- Các lĩnh vực mà có thể áp dụng:

+Ứng Dụng Công Nghệ Sinh Trắc Học Trong Khu Vực Chính Phủ

+ Ứng Dụng Công Nghệ Sinh Trắc Học Trong Tổ Chức Tài Chính Ngân Hàng

+ Ứng Dụng Công Nghệ Sinh Trắc Học Trong Chăm Sóc Sức Khỏe

+Ứng Dụng Công Nghệ Sinh Trắc Học Trong Quản Lý Lực Lượng Lao Động

+Ứng Dụng Công Nghệ Sinh Trắc Học Trong Quản Lý Khách Sạn

+Ứng Dụng Công Nghệ Sinh Trắc Học Trong Ngành Giao Thông Vận Tải

+Ứng Dụng Công Nghệ Sinh Trắc Học Trong Quản Lý Trường Học

33) Nêu ưu điểm và nhược điểm của việc áp dụng chứng thực bằng sinh trắc học.

- Ưu điểm

+Có thể rất chính xác

+Nhanh: thời gian chứng thực nhỏ hơn 1s

+Sự tác động của người dùng thấp, Không cần phải nhớ khóa

+Kết hợp nhiều yếu tố: vân tay, võng mạc, giọng nói,…→ Tính bảo mật cao

- Nhược điểm

+Giá thành cao: triển khai hệ thống sinh trắc học đòi hỏi chi phí cho phần cứng và phần mềm .Hiện tại máy nhận dạng sinh trắc học trên thị trường khá đắt tiền

+Có thể nhận diện sai: mặc dù đúng người nhưng hệ thống không chấp nhận, Chỉ chấp nhận hình ảnh xác thực rõ ràng, nên khi tay bẩn, trầy hoặc xây xước thì sẽ không được hệ thống chấp nhận

34) Hệ thống quản lý an toàn thông tin là gì? Mục tiêu của hệ thống an toàn toàn thông tin?

-Hệ thống quản lý an toàn thông tin là gì?

+Hệ thống quản lý an toàn thông tin (Information Security Management System - ISMS) là công cụ để các nhà lãnh đạo quản lý thực hiện việc giám sát, quản lý hệ thống thông tin, tăng cường mức độ an toàn, bảo mật, giảm thiểu rủi ro cho hệ thống thông tin, đáp ứng được mục tiêu của doanh nghiệp, tổ chức.

+Hệ thống quản lý an toàn thông tin là một hệ thống đưa ra các phương pháp đánh giá việc theo dõi; bảo vệ và quản lý hệ thống thông tin, dữ liệu. Việc mất thông tin trong bất cứ trường hợp nào; dù ít hay nhiều cũng gây ra thiệt hại cho tổ chức. Thậm chí có thể khiến tổ chức sụp đổ.

- Mục tiêu xây dựng hệ thống an toàn thông tin

-Đảm bảo ATTT của tổ chức, đối tác và khách hàng, giúp cho hoạt động của tổ chức luôn thông suốt và an toàn.

-Giúp nhân viên tuân thủ việc đảm bảo ATTT trong hoạt động nghiệp vụ thường ngày; Các sự cố ATTT do người dùng dây ra sẽ được hạn chế tối đa khi nhân viên được đào tạo, nâng cao nhận thức ATTT.

-Giúp hoạt động đảm bảo ATTT luôn được duy trì và cải tiến. Các biện pháp kỹ thuật và chính sách tuân thủ được xem xét, đánh giá, đo lường hiệu quả và cập nhật định kỳ.

-Đảm bảo hoạt động nghiệp vụ của tổ chức không bị gián đoạn bởi các sự cố liên quan đến ATTT.

-Nâng cao uy tín của tổ chức, sự tin tưởng của khách hàng, đối tác, cổ đông vì thông tin của họ được bảo mật an toàn. Tăng sức cạnh tranh, tạo lòng tin với khách hàng, đối tác, thúc đẩy quá trình toàn cầu hóa và tăng cơ hội hợp tác quốc tế.

-Đảm bảo thông tin không bị đánh cắp, mất mất và giúp khôi phục thông tin khi xảy ra sự cố.

-Cung cấp đủ thông tin khi cần.

-Khai thác và tận dụng được tối đa nguồn thông tin.

-Đảm bảo những thông tin quan trọng không bị phát tán ra bên ngoài.