Đề cương chi tiết

Bộ môn: An toàn thông tin

Phần II: 14 câu

Mục lục

Lưu ý trước khi đọc 2

Câu 1 (Bùi Tùng): Nêu một số kỹ thuật mã hóa cổ điển, phân tích khả năng áp dụng mô hình cho mã hóa dữ liệu lưu trữ và mã hóa dữ liệu trên đường truyền. 3

Câu 2 (Bùi Tùng): Khác nhau giữa mã hóa cổ điển và các hàm băm. Nguyên lý của hàm băm, khả năng sử dụng hàm băm trong bảo vệ dữ liệu và các hệ thống ứng dụng. 4

Câu 3 (Lệ Hàn Phong): Cơ sở của mã hoá công khai RSA, phân tích khả năng sử dụng mã hoá RSA để lưu trữ dữ liệu trên hệ thống máy tính, truyền dữ liệu trên mạng máy tính. 5

Câu 4 (Lệ Hàn Phong): Phân tích sự khác biệt mã hóa cổ điển và mã công khai, khả năng kết hợp giữa hai loại khóa trong truyền tin? 6

Câu 5 (Haidang Pham): Giới thiệu về mã hóa ECC nguyên lý và ứng dụng. 7

Câu 6 (Nguyễn Đức Thắng): Khác biệt và tương đồng giữa mã hóa cổ điển và mã hóa DES, AES?. Ứng dụng của DES, AES trong thực tế. 8

Câu 7 (Phan Kid): Trình bày mô hình chữ ký số. Sự cần thiết của triển khai mô hình chữ ký số trong giao dịch điện tử ở Việt Nam. Trình bày hiểu biết về hiện trạng mô hình chữ ký số ở Việt Nam. 9

Câu 8 (Haidang Pham): Nguyên lý, khả năng, phương thức phòng chống với các phương thức tấn công mạng máy tính: Port scaning attack, Evesdropping attack, IP spoofing attack 12

Câu 9 (Phan Kid): Nguyên lý, khả năng, phương thức phòng chống với các phương thức tấn công mạng máy tính: Hijacking attack, Replay attack, Man-in-the-middle. 15

Câu 10 (Phan Kid): Tấn công SQL injection, tràn bộ đệm, chéo ngang – cross page attack ? Giải pháp phòng chống ? 16

Câu 11 (Hữu Anh): Tấn công DoS, DdoS nguyên lý và khả năng phòng chống ? 18

Câu 12 (Phan Kid): Khác nhau giữa virus, worm, trojan, backdoor 20

Câu 13 (Tú Cẩm): Khả năng bảo vệ hệ thống của trình quét virus và firewall 21

Câu 14 (Tú Cẩm): IPSec, VPN khả năng bảo vệ thông tin trên đường truyền 22

Lưu ý trước khi đọc

- Đây là những câu trả lời do một số bạn tự soạn thảo dựa trên bài giảng của thầy và tìm hiểu trên mạng. (Tên người làm được để ngay cạnh câu hỏi).
- Những chỗ nào chữ màu nâu là những phần thuộc về cá nhân, mang tính chất kết hợp trên mạng và tổng hợp kiến thức bản thân nên độ tin cậy có thể không cao. Các bạn đọc những phần này tham khảo để tự tìm ra cho mình một cách trả lời khác chính xác và hợp lý hơn.
- Các câu trả lời này nếu có vấn đề, sai sót, thiếu sót gì, xin vui lòng liên hệ qua FB hoặc qua sđt **0167 5894 643** , để t kịp thời chỉnh sửa.
- Mọi vấn đề thắc mắc về câu trả lời, cần giải đáp, các bạn có thể liên hệ với mình hoặc trực tiếp hỏi những bạn chịu trách nhiệm cho câu hỏi đó.
- Chân thành cảm ơn mọi ý kiến đóng góp của các bạn ☺

Chúc các bạn ôn bài tốt !

Câu 1(Bùi Tùng): Nêu một số kỹ thuật mã hóa cổ điển, phân tích khả năng áp dụng mô hình cho mã hóa dữ liệu lưu trữ và mã hóa dữ liệu trên đường truyền.

- Hệ thống mã hóa (Cryptosytem) là một bộ năm (P, C, K, E, D) thỏa mãn các điều kiện sau:
  + Tập nguồn P là tập hữu hạn tất cả các bản tin nguồn cần mã hóa có thể có
  + Tập đích C là tập hữu hạn tất cả các bản tin có thể có sau khi mã hóa
  + Tập khóa K là tập hữu hạn các khóa có thể được sử dụng
  + E, D là tập luật mã hóa và giải mã. Với mỗi khóa k tồn tại 1 luật mã hóa e_k thuộc E và luật giải mã tương ứng d_k thuộc D.
  Luật mã hóa e_k : P -> C và d_k: C -> D thỏa mãn $d_k(e_k(x)) = x$ với mọi x thuộc P
- ***Một số kỹ thuật mã hóa cổ điển:***
  + ***Mã hóa dịch chuyển:*** là một trong những phương pháp lâu đời nhất được sử dụng. Thông điệp được mã hóa bằng cách dịch chuyển xoay vòng từng ký tự đi k vị trí trong bảng chữ cái. Trong trường hợp đặc biệt k = 3, phương pháp mã hóa bằng dịch chuyển được gọi là phương pháp mã hóa Caesar.
    - Cho P = C = K = Z_n với mỗi khóa K định nghĩa $e_k(x) = (x + k) \bmod n$ và $d_k(y) = (y - k) \bmod n$ với x,y thuộc Z_n
    - E = {e_k, k thuộc K} và D = {d_k, k thuộc K}
    - ***Trên thực tế, phương pháp này có thể dễ dàng bị phá vỡ bằng cách thử mọi khả năng khóa k thuộc k, điều này hoàn toàn có thể thực hiện được do không gian khóa K chỉ có n phần tử để chọn lựa. Do có thể dễ dàng bị phá vỡ, không nên áp dụng phương pháp này cho mã hóa dữ liệu lưu trữ và mã hóa dữ liệu trên đường truyền.***

  + ***Mã hóa thay thế :***Phương pháp mã hóa thay thế (Substitution Cipher) là một trong những phương pháp mã hóa nổi tiếng và đã được sử dụng từ hàng trăm năm nay. Phương pháp này thực hiện việc mã hóa thông điệp bằng cách hoán vị các phần tử trong bảng chữ cái hay tổng quát hơn là hoán vị các phần tử trong tập nguồn *P*.
    - Cho P=C = Z_n: K là tập hợp tất cả các hoán vị n phần tử 0, 1, …n-1. Như vậy mỗi khóa thuộc K là 1 hoán vị của n phần tử 0, 1, …n-1. Với mỗi khóa k thuộc K, định nghĩa: $e_k(x) = k(x)$ và $d_k(y) = k^{-1}(y)$ với x, y thuộc Z_n, E = {e_k, k thuộc K} và D = {d_k, k thuộc K}
    - Đây là một phương pháp dơn giản, thao tác mã hóa và giải mã được thực hiện nhanh chóng. Trong phuong pháp mã hóa thay thế có không gian khóa K rất lớn với n! phần tử nên không thể bị giải mã bằng cách "vét cạn" mọi trường hợp khóa k. Tuy nhiên, trên thực tế thông điệp được mã hóa bằng phương pháp này vẫn có thể bị giải mã nếu như có thể thiết lập dược bảng tần số xuất hiện của các ký tự trong thông điệp hay nắm dược một số từ, ngữ trong thông điệp nguồn ban đầu.

Câu 2 (Bùi Tùng): Khác nhau giữa mã hóa cổ điển và các hàm băm. Nguyên lý của hàm băm, khả năng sử dụng hàm băm trong bảo vệ dữ liệu và các hệ thống ứng dụng.

- ***Khác nhau giữa mã hóa cổ điển và các hàm băm***

Mã hóa cổ điển	Hàm băm
Từng ký tự hay nhóm ký tự được thay thế bằng một hay 1 nhóm ký tự khác. Vẫn giữ nguyên độ dài thông tin gốc.	Biến đổi khối thông tin gốc có độ dài bất kỳ thành đoạn thông tin có đội dài cố định gọi là mã băm.

- ***Nguyên lý hàm băm***:

  + Biến đổi khối thông tin gốc có độ dài bất kỳ thành một đoạn thông tin có độ dài cố định gọi là mã băm. Mã băm được dùng để kiểm tra tính chính xác của thông tin nhận được.

  + Một hàm băm H áp dụng cho khối thông tin M tạo ra kết quả m, được ký hiệu là H(M) = m.

  + Thông thường, mã băm được gởi kèm với thông tin gốc, cùng với một cơ chế bảo vệ nào đó giúp mã băm không bị thay đổi hoặc tính lại. Ở phía nhận, hàm băm lại được áp dụng đối với thông tin gốc để tìm ra mã băm mới, giá trị này được so sánh với mã băm đi kèm với thông tin gốc. Nếu hai mã băm giống nhau, nghĩa là thông tin gởi đi không bị thay đổi

- ***Khả năng sử dụng của hàm băm trong việc bảo vệ dữ liệu và các hệ thống ứng dụng: (Phan Kid bổ sung)***

  + Ứng dụng chính của hàm băm là sử dụng với các hệ chữ ký điện tử, trong đó thay vì ký trực tiếp lên các văn bản, thông điệp, người ta sẽ ký lên giá trị băm đại diện cho toàn bộ văn bản đó. Ngoài việc sử dụng với các hệ chữ ký điện tử, hàm băm còn được sử dụng vào các mục đích khác như: xác thực hóa thông điệp, xác thực hóa người dùng.

  + Trong các hệ thống yêu cầu có xác thực người dùng, để lưu mật khẩu người ta cũng sử dụng các hàm băm hoặc các hệ mã trong vai trò của hàm băm.

Câu 3(Lệ Hàn Phong): Cơ sở của mã hoá công khai RSA, phân tích khả năng sử dụng mã hoá RSA để lưu trữ dữ liệu trên hệ thống máy tính, truyền dữ liệu trên mạng máy tính.

- ***Cơ sở của mã hóa công khai RSA:***

  + Trong phương pháp RSA tất cảcác phép tính đều được thực hiện trên Z_n

  n = pq với p và q là hai số nguyên tố phân biệt.

  Cho P = C =Z_n và định nghĩa:

  K= { ((n, p, q, a, b): n = pq, p, q là số nguyên tố, ab ≡1 (mod φ(n)) }

  Với mỗi k = (n, p, q, a, b) ∈ K, định nghĩa: $e_k(x) = x^b \bmod n$ và $d_k(y) = y^a \bmod n$ với x,y∈Z_n

Giá trị n và b được công bố, trong khi giá trị p, q, a được giữ bí mật

- ***Phân tích khả năng sử dụng mã hóa RSA để lưu trữ dữ liệu trên hệ thống máy tính, truyền dữ liệu trên mạng máy tính: (Phan kid bổ sung)***

  + Hệ mã RSA có tính an toàn cao nhưng nhược điểm là tốc độ mã hóa chậm. Bởi vậy nó chỉ được sử dụng với các văn bản ngắn và thường dùng trong giao thức xác nhận chủ thể (chữ ký điện tử)

  + RSA được áp dụng vào quá trình truyền tải dữ liệu như sau:

    - Một khóa riêng sẽ được tạo ra dựa trên các số nguyên tố
    - Một khóa chung sẽ được tạo ra dựa trên khóa riêng này theo hàm một chiều. Tức là việc tìm lại "khóa riêng" từ khóa chung này là một điều gần như không thể. Do đó, khóa chung có thể gửi đi trên mạng
    - Khóa chung sẽ được gửi đi trên mạng trong quá trình truyền dữ liệu
    - Dữ liệu nhận được sẽ được mã hóa dựa theo khóa chung này, và được giải mã bằng mã riêng.

Câu 4(Lệ Hàn Phong): Phân tích sự khác biệt mã hóa cổ điển và mã công khai, khả năng kết hợp giữa hai loại khóa trong truyền tin?

Trong mã hóa cổ điển, thông điệp nguồn được mã hóa với mã khóa k được thống nhất trước giữa người gửi A và người nhận B. Người A sẽ sử dụng mã khóa k để mã hóa thông điệp x thành thông điệp y và gửi y cho người B, người B sẽ sửdụng mã khóa k để giải mã thông điệp y này.

Khóa công khai sử dụng hai loại khóa trong cùng một cặp khóa: khóa công cộng (public key) được công bố rộng rãi và được sửdụng trong mã hóa thông tin, khóa riêng (private key) chỉ do một người nắm giữ và được sử dụng để giải mã thông tin đã được mã hóa bằng khóa công cộng.

Các phương pháp mã hóa cổ điển có ưu điểm xử lý rất nhanh so với các phương pháp mã hóa khóa công khai. Do khóa dùng để mã hóa cũng được dùng để giải mã nên cần phải giữ bí mật nội dung của khóa. Vấn đề khó khăn đặt ra đối với các phương pháp mã hóa này chính là bài toán trao đổi mã khóa.

Ngược lại, các phương pháp mã hóa khóa công khai giúp cho việc trao đổi mã khóa trở nên dễ dàng hơn. Nội dung của public key không cần phải giữ bí mật như đối với khóa bí mật trong các phương pháp mã hóa cổ điển.

Bởi vậy chúng ta có thể sử dụng khóa công khai để mã hóa khóa bí mật, khi đó khóa bí mật có thể được trao đổi an toàn.

Câu 5(Haidang Pham): Giới thiệu về mã hóa ECC nguyên lý và ứng dụng.

- ***Giới thiệu về mã hóa ECC :***

  Hiện nay, hệ mật RSA là giải thuật khoá công khai được sử dụng nhiều nhất, nhưng hệ mật dựa trên đường cong Elliptic (ECC) có thể thay thế cho RSA bởi mức an toàn và tốc độ xử lý cao hơn. Ưu điểm của ECC là hệ mật mã này sử dụng khoá có độ dài nhỏ hơn so với RSA. Từ đó làm tăng tốc độ xử lý một cách đáng kể, do số phép toán dùng để mã hoá và giải mã ít hơn và yêu cầu các thiết bị có khả năng tính toán thấp hơn, nên giúp tăng tốc độ và làm giảm năng lượng cần sử dụng trong quá trình mã hoá và giải mã.

- ***Nguyên lý:***

  + ECC thực hiện việc mã hoá và giải mã dựa trên toạ độ của các điểm dựa trên đường cong Elliptic. Xét đẳng thức Q=kP, (điểm Q là tổng của k điểm P, k < p)

  + Cho trước k và P, việc tính Q thực hiện dễ dàng , nhưng rất khó xác định k nếu biết Q và P. (Phép nhân được xác định bằng cách cộng liên tiếp cùng điểm P.

  Ví dụ: 4P = P+P+P+P ; 9P = 2(2(2P)) + P).

  + Hệ mật dựa trên đường cong Elliptic dựa trên độ khó khi biết được điểm P và Q và phải tìm ra giá trị k. Bên cạnh công thức của đường cong Elliptic, thì một thông số quan trọng khác của đường cong Elliptic là điểm G (còn gọi là điểm cơ sở), điểm G đối với mỗi đường cong elliptic là cố định, trong hệ mật mã ECC thì một số nguyên lớn k đóng vai trò như một khoá riêng, trong khi đó kết quả của phép nhân giữa k với điểm G được coi như là khoá công khai tương ứng.

- ***Ứng dụng:***

  + Việc trao đổi khoá theo Diffie Hellman dựa trên đường cong Elliptic (ECDH – Elliptic Curve Diffie Hellman) và thuật toán chữ ký số dựa trên đường cong Elliptic (ECDSA - Elliptic Curve Digital Signature Algorithm) là những ứng dụng cụ thể của đường cong Elliptic trong lĩnh vực mật mã.

  + Trong trao đổi khoá ECDH, hai bên A và B sử dụng các tham số đường cong Elliptic giống nhau. Mỗi bên tạo ra khoá riêng kA và kB và tạo ra các khoá công khai $Q_A=k_AG$ và $Q_B=k_BG$. hai bên trao đổi khoá công khai và nhân khoá riêng của nó với khoá công khai của bên kia, điều này dẫn đến thông tin mật được chia sẻ $k_AQ_B = k_BQ_A = k_Ak_BG$. Còn ECDSA hoàn toàn tương tự như DSA.

Câu 6(Nguyễn Đức Thắng): Khác biệt và tương đồng giữa mã hóa cổ điển và mã hóa DES, AES?. Ứng dụng của DES, AES trong thực tế.

- ***Mã hóa cổ điển và mã hóa DES, EAS***

- Giống:

  Mã hóa cổ điển :mã dịch vòng, thay thế,vvv Mã hóa DES, EAS: mã hóa theo khối đều là hệ thống mã hóa quy ước(Mã hóa Đối xứng) : quá trình mã hóa và giải mã một thông điệp sửdụng cùng một mã khóa gọi là khóa bí mật(secret key) hay khóa đối xứng. Do đó, vấn đề bảo mật thông tin đã mã hóa hoàn toàn phụ thuộc vào việc giữ bí mật nội dung của mã khóa đã được sử dụng.

- Khác:

  Trong phương pháp DES, kích thước khối là 64 bit. DES thực hiện mã hóa dữ liệu qua 16 vòng lặp mã hóa, mỗi vòng sử dụng một khóa chu kỳ48 bit được tạo ra từ khóa ban đầu có độ dài 56 bit. DES sử dụng 8 bảng hằng số S-box để thao tác. Quá trình mã hóa của DES có thể được tóm tắt như sau: Biểu diễn thông điệp nguồn xP ∈ bằng dãy 64bit. Khóa k có 56 bit. Sử dụng cấu trúc mạng Feistel. Trong phương pháp EAS, kích thước khối là 128 bit. Quá trình mã hóa của EAS có thể được tóm tắt như sau: Biểu diễn thông điệp nguồn xP ∈ bằng dãy 128bit. Khóa k có 128,192 hoặc 256 bit. Khác với với DES sử dụng mạng Feistel, Rijndael sử dụng mạng thay thế-hoán vị. AES có thể dễ dàng thực hiện với tốc độ cao bằng phần mềm hoặc phần cứng và không đòi hỏi nhiều bộ nhớ. Do AES là một tiêu chuẩn mã hóa mới, nó đang được triển khai sử dụng đại trà.

- ***Ứng dụng:***

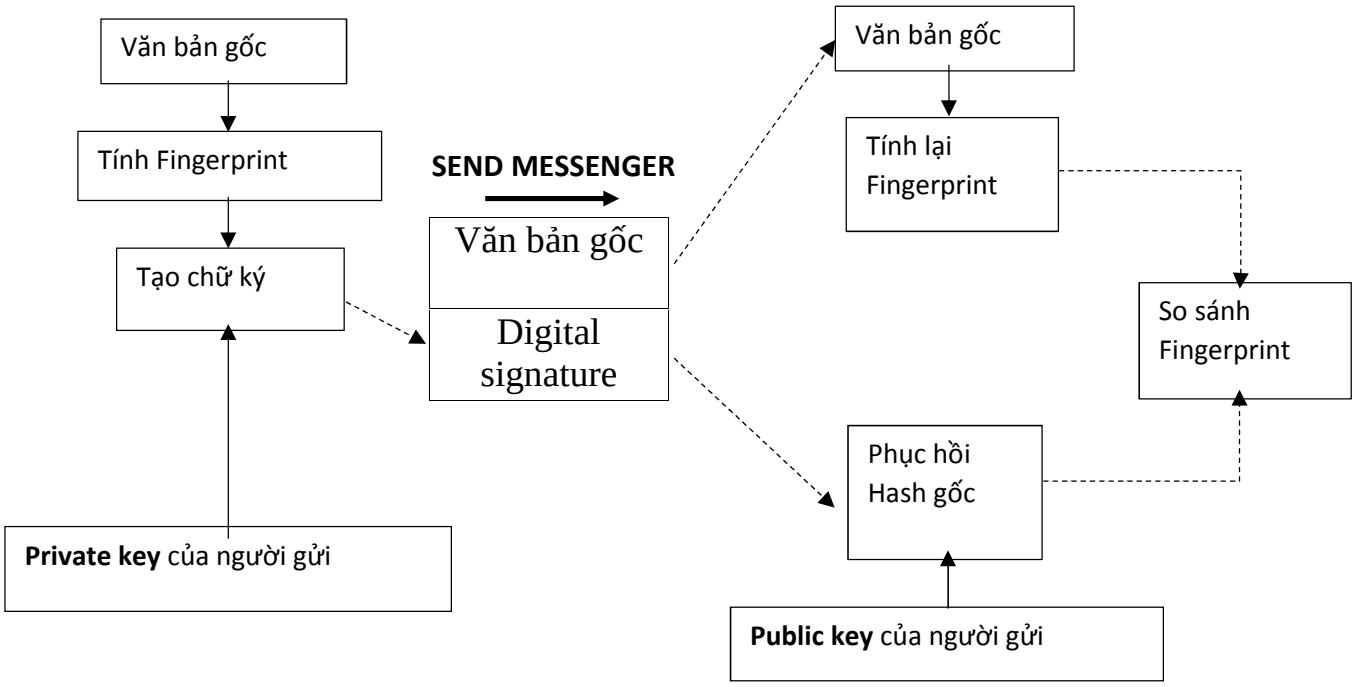
_Bảo mật dữ liệu -bảo vệ tính toàn vẹn của thông điệp(bảo mật thông tin lien lạc trong quân sự và dân sự) - phối hợp tạo ra hàm băm AES-Hash

Câu 7(Phan Kid): Trình bày mô hình chữ ký số. Sự cần thiết của triển khai mô hình chữ ký số trong giao dịch điện tử ở Việt Nam. Trình bày hiểu biết về hiện trạng mô hình chữ ký số ở Việt Nam.

- Khái niệm chữ ký số: Chữ ký số là một công nghệ đảm bảo an toàn thông tin dựa trên mật mã khóa công khai cho phép thay thế chữ ký tay và con dấu trên môi trường điện tử.
- ***Sơ đồ chữ ký số:*** là bộ 5 (P, A, K, S, V) thỏa mãn các điều kiện dưới đây:
  + P là tập hợp hữu hạn các thông điệp
  + A là tập hợp hữu hạn các chữ ký có thể sử dụng
  + Không gian khóa K là tập hợp hữu hạn các khóa có thể sử dụng
  + Với mỗi khóa k ∈ K, tồn tại thuật toán chữ ký $sig_k \in S$ và thuật toán xác nhận chữ ký tương ứng $ver_k \in V$. Mỗi thuật toán sig_k : P -> A và ver_k: P x A -> {True, False} là các hàm thỏa điều kiện:

$$\forall x \in P, \forall y \in A : ver(x,y) = \begin{cases} true & \text{nếu } y = sig(x) \\ false & \text{nếu } y \neq sig(x) \end{cases}$$

- ***Mô hình chữ ký số:***



- ***Sự cần thiết của triển khai mô hình chữ ký số trong giao dịch điện tử ở Việt Nam:***
  + Mỗi ngày, một số lượng lớn giao dịch điện tử được thực hiện thông qua Internet phục vụ cho các hoạt động phát triển kinh tế - xã hội và quan hệ quốc tế, … Đây

là một môi trường giao dịch thuận lợi nhưng cũng có nhiều nguy cơ tiềm ẩn về an toàn thông tin. Do không gặp trực tiếp, đối tác giao dịch khó được xác thực chính xác nên có thể bị mạo danh. Ở dạng điện tử, nội dung các văn bản có thể bị thay đổi bởi người không có thẩm quyền. Do đó, các văn bản điện tử không thể dùng làm bằng chứng để đảm bảo các đối tác không chối bỏ các cam kết của mình. Giao dịch điện tử chỉ có thể thực hiện một cách an toàn và trở thành một phương tiện trao đổi thông tin hiệu quả trong thời đại thông tin số nếu các biện pháp an toàn thông tin cho giao dịch điện tử có thể đảm bảo các tính năng: *Bảo mật*, *Nhất quán*, *Xác thực* và *Chống chối bỏ*.

+ Các biện pháp an toàn thông tin cho giao dịch điện tử được sử dụng trước đây như sử dụng tên định danh/mật khẩu (ID/Password), mật khẩu sử dụng một lần (OTP),… đều có hạn chế riêng về tính năng, mức độ đảm bảo và mô hình giao dịch. Một trong các biện pháp trên là sử dụng mật mã đối xứng để mã hóa tài liệu điện tử khi trao đổi giữa hai hay nhiều đối tác. Mật mã này sử dụng một khóa (thường gọi là mật khẩu) để mã và sử dụng chính khóa đó để mở mã một tài liệu điện tử (tệp máy tính hay thông điệp dữ liệu). Nhiều phần mềm phổ biến hiện nay như MS Word, MS Excel, WinRAR, WinZip,… cho phép người dùng sử dụng biện pháp này để mã hóa nhằm hạn chế người không có thẩm quyền đọc nội dung tài liệu. Tuy nhiên, do mã và mở mã phải dùng cùng một khóa nên các đối tác trao đổi thông tin có sử dụng biện pháp an toàn thông tin này cần biết nhau để thống nhất mật khẩu. Vì thế mật mã đối xứng không hoàn toàn phù hợp với mô hình giao dịch mở như thương mại điện tử, khi các đối tác chưa quen nhau có thể có nhu cầu giao dịch. Ngoài ra, do mật khẩu được chia sẻ giữa các đối tác nên biện pháp an toàn thông tin này không có tính năng *xác thực* và *chống chối bỏ*.

+ Với việc giao dịch điện tử được dùng ngày càng rộng rãi để triển khai các loại hình giao dịch quan trọng như thương mại điện tử, chính phủ điện tử,… chữ ký số đã được công nhận là biện pháp an toàn thông tin phù hợp nhất cho giao dịch điện tử xét từ khía cạnh tính năng và mức độ đảm bảo an toàn thông tin cũng như tính khả dụng.

- ***Hiểu biết về hiện trạng chữ mô hình chữ ký số ở Việt Nam:***

Chữ ký số đem lại nhiều lợi ích cho người dân và cộng đồng doanh nghiệp trong các hoạt động phát triển kinh tế - xã hội. Với chữ ký số, nhiều giao dịch kinh tế, thương mại, hành chính được thực hiện theo cách truyền thống được chuyển sang môi trường điện tử, với độ đảm bảo an toàn cao, giảm bớt thời gian và chi phí thực hiện, thuận lợi và dễ dàng quản lý.

Tại Việt Nam, sau một thời gian triển khai, đến nay người dân và cộng đồng doanh nghiệp có thể xác định *chữ ký số là dạng thể hiện chữ ký tay và con dấu, được công nghệ đảm bảo và được* pháp *luật bảo hộ*. Sau khi Nghị định số 26/2007/NĐ-CP cùng một số văn bản dưới Nghị định ra đời, đến nay khung pháp lý về chữ ký số dần được hình thành và hoàn thiện. Với việc các CA công cộng được Bộ Thông tin và Truyền thông cấp giấy phép và đi vào hoạt động để cung cấp dịch vụ chứng thực chữ ký số, điều kiện để người dân và cộng đồng doanh nghiệp sử dụng chữ ký số tại Việt Nam đã chín được cụ thể hóa hơn.

+ Một ứng dụng điển hình về sử dụng chữ ký số tại nước ta trong thời gian vừa qua là hệ thống kê khai thuế qua mạng do Bộ Tài chính triển khai và đưa và ứng dụng rộng rãi. Phương thức này cho phép doanh nghiệp chỉnh sửa sai sót một cách nhanh chóng, hồ sơ khai thuế có thể được gửi đi từ bất cứ nơi nào có kết nối mạng, vào bất cứ thời điểm nào trước hạn quy định, với chi phí in ấn, đi lại được giảm thiểu, thông tin thuế được nhập và tổng hợp nhanh chóng. Việc ứng dụng chữ ký số cho phép cải cách và hiện đại hóa ngành thuế, giảm tình trạng quá tải, áp lực cho doanh nghiệp và cơ quan thuế trong thủ tục nộp thuế, tiết kiệm nhân lực và nguồn lực xử lý, lưu trữ thông tin về thuế.

+ Tuy nhiên, đối với người dân và cộng đồng doanh nghiệp, trên góc độ chi phí/hiệu quả, lợi ích của việc sử dụng chữ ký số liên quan đến tỷ lệ chi phí sở hữu chứng thư số trên số các ứng dụng chữ ký số. Hiện nay, trung bình giá thuê bao doanh nghiệp phải trả cho để sở hữu một chứng thư số là 1 triệu VNĐ một năm (chứng thư số cho cá nhân có giá thấp hơn). Tuy nhiên, chữ ký số chỉ được sử dụng chủ yếu với mục đích kê khai thuế qua mạng nên đã có ý kiến cho là giá một chứng thư số còn cao trong điều kiện hiện nay. Tuy nhiên, khi số lượng các ứng dụng thiết thực có sử dụng chữ ký số tăng lên, khi đó chi phí sử dụng chữ ký số sẽ giảm và mức giá hiện nay có thể được người dân và doanh nghiệp chấp nhận.

Câu 8(Haidang Pham): Nguyên lý, khả năng, phương thức phòng chống với các phương thức tấn công mạng máy tính: Port scaning attack, Evesdropping attack, IP spoofing attack

a)Port Scanning ATACK:

***Nguyên Lý** :

-Port scanning là quá trình xác định cổng TCP/IP mở và có sẵn trên một hệ thống. Công cụ Port scanning cho phép một hacker tìm hiểu về các dịch vụ có sẵn trên một hệ thống nhất định. Mỗi dịch vụ hay ứng dụng máy tính được kết hợp với một số cổng thông dụng. Ví dụ, một công cụ quét đó là xác định cổng 80 mở cho một web sever đang chạy trên đó. Hacker cần phải biết rõ với số cổng thông dụng.

-TCP scan: Trên gói TCP/UDP có 16 bit dành cho Port Number điều đó có nghĩa nó có từ 1 – 65535 port. Thường chỉ scan từ

-1 Số phương pháp:

+SYN SCAN:Gửi SYN Vơi 1 thông số port,nhận lại được SYN ACK thì client biết port trên sever đã mở

+FIN SCAN:Client gửi gói FIN với số port nhất định,nhận ACK sever sẽ mở port đó,Sever gửi về gói RST Thì client (máy khách) biết sever đóng port đó

+ NULL Scan Sure: Client sẽ gửi tới Server những gói TCP với số port cần Scan mà không chứa thông số Flag nào, nếu Server gửi lại gói RST thì tôi biết port đó trên Server bị đóng.

+XMAS Scan Sorry: Client sẽ gửi những gói TCP với số Port nhất định cần Scan chứa nhiều thông số Flag như: FIN, URG, PSH. Nếu Server trả về gói RST tôi biết port đó trên Server bị đóng.

+TCP CONNECT: gửi đến Server những gói tin yêu cầu kết nối

port cụ thể trên server, Nêu server trả về gói SYN/ACK thì mở cổng

đó

+ACK SCAN: Scan này nhằm mục đích tìm những Access Controll List trên Server, Client cố gắng kết nối tới Server bằng gói ICMP, nhan được gói tin là Host Unreachable thì client se hiểu port đó trên server đã bị lọc.

***Chức năng**:
-Xác định máy đang mở cổng nào.
-Xác định hệ thống đang sử dụng dịch vụ nào.

* **Một số phương pháp phòng chống**:

- Biện pháp đối phó là quá trình hoặc bộ công cụ được sử dụng bởi các quản trị viên an ninh để phát hiện và có thể ngăn chặn port-scanning các máy chủ trên mạng của họ. Danh sách các biện pháp đối phó cần được thực hiện để ngăn chặn một hacker thu thập thông tin từ quá trình quét cổng:

-Kiến trúc an ninh thích hợp, chẳng hạn như thực hiện các IDS và tường lửa nên được đi chung.

-Hacker chân chính sử dụng công cụ của họ thiết lập để kiểm tra việc Scanning, thực hiện các biện pháp đối phó. Khi tường lửa được đặt ra, công cụ aport-scanning nên được chạy cho các máy chủ trên mạng để cho phép tường lửa phát hiện chính xác và dừng các hoạt động của port-scanning.

-Tường lửa có thể phát hiện các hoạt động thăm dò được gửi bởi các công cụ port-scanning. Các tường lửa nên tiến hành lấy *trạng thái kiểm tra (stateful inspections). C*ó nghĩa là nó sẽ kiểm tra không chỉ các tiêu đề TCP mà cả dữ liệu của gói tin để xác định liệu được phép đi qua tường lửa.

-Network IDS nên được sử dụng để phát hiện các phương pháp dò tìm hệ điều hành được sử dụng bởi một số công cụ hacker phổ biến như Nmap.

-Chỉ có các cổng cần thiết nên được giữ ở trạng thái mở. Phần còn lại sẽ được lọc hoặc bị chặn.

-Các nhân viên của tổ chức sử dụng các hệ thống cần được đào tạo thích hợp nhận thức về an ninh. Cũng nên biết chính sách bảo mật khác nhau mà họ đang cần làm theo.

b) Eavesdropping Attack:

*__Nguyên Lý__ :

-Sử dụng các phương pháp vật lý :Nghe trộm qua đường truyền vật lý hoặc sóng vô tuyến

-Nghe lén mạng :

+Tham gia vào mạng

+Nhận các gói tin được truyền tới cổng mạng

+Nếu mạng sử dụng là switch thì dùng phương pháp ‘Man in the midle’

***Chức năng**:

-Tạo ra các gói tin có địa chỉ IP giả

-Vượt qua các kiểm soát nguồn gốc về địa chỉ IP

-Phục vụ các mô hình tấn công khác:kiểu phiên,kiểu phản xạ

*__Một số phương pháp phòng chống:__

- Sử dụng switch thay cho hub

- Giám sát địa chỉ MAC

- Sử dụng cơ chế mã hóa truyền tin và mã hóa theo thời gian

- Sử dụng các dịch vụ mã hóa trong liên kết:SSL,SSH,SFTP

-Sử dụng các phần mềm phát hiện hoạt động nghe lén trên mạng

c) IP spoofing attack(Giả mạo địa chỉ IP)

*__Nguyên Lý__:

-IP Spoofing là một công nghệ nhằm vượt qua sự ngăn chặn truy cập của hệ thống, Attacker có thể gửi các thông điệp đến một máy tính mà dưới danh nghĩa là một host hợp lệ. Ở đây có một vài sự khác nhau trong nhiều cách tấn công theo kiểu này:

+Giả mạo bằng cách bắt gói(Non Blind spoofing):Phân tích số thứ tự cho máy cùng mạng

+Giả mạo địa chỉ IP từ xa(Blind spoofing):khác mạng có được số TCP sequence chính xác là rất khó,tuy nhiên với 1 số kỹ thuật như định tuyến theo địa chỉ nguồn

***Chức năng**:

- Giả mạo IP được thường xuyên nhất được sử dụng trong tấn công từ chối dịch vụ . Trong các cuộc tấn công như vậy, mục tiêu là để làm lụt nạn nhân với lượng truy cập áp đảo, và những kẻ tấn công không quan tâm về việc nhận được câu trả lời cho các gói tin tấn công. Các gói tin với địa chỉ giả mạo là như vậy, thích hợp cho các cuộc tấn công như vậy với mục đích chính là che giấu nguồn gốc thực sự của cuộc tấn công.

- Giả mạo IP còn là một phương pháp tấn công được sử dụng bởi những attacker để đánh bại các biện pháp an ninh mạng, chẳng hạn như xác thực dựa trên địa chỉ IP. Loại tấn công này hiệu quả nhất trong các hệ thống có độ tin cậy giữa các máy cao

*__Một số phương pháp phòng chống:__

-Dùng danh sách kiểm tra truy cập trên các interface của router.Một ACL có thể được dung để loại bỏ những traffic từ bên ngoài mà lại được đóng gói bởi 1địa chỉ trong mạng cục bộ

-Dùng mật mã xác thực

-Mã hóa traffic giữa các thiết bị

Câu 9(Phan Kid): Nguyên lý, khả năng, phương thức phòng chống với các phương thức tấn công mạng máy tính: Hijacking attack, Replay attack, Man-in-the-middle.

- Hijacking attack:
  + Nguyên lý: truy cập trái phép thông tin hoặc dịch vụ trong một hệ thống máy tính. Người tấn công bằng 1 cách nào đó xen vào giữa cuộc giao tiếp giữa 2 người. Người tấn công sẽ chiếm quyền của 1 trong 2 người, hoặc chỉ làm gián điệp để lấy thông tin 2 người gửi cho nhau.
- Replay attack:
  + Nguyên lý: Sử dụng công cụ để ghi nhận tất cả thông tin trao đổi khi một máy tính nào đó truy xuất đến server. Sau đó sử dụng các thông tin bắt được trên mạng để nối kết lại đến server đó. Đây là kỹ thuật mà Attacker khi nắm được một số lượng packet sẽ sử dụng lại những packet này sau đó. Ví dụ Attacker có được packet chứa password của một user. Password này đã được mã hoá và attacker không biết được. Tuy nhiên hệ thống chứng thực không có chức năng kiểm tra Session time hay hệ thống có TCP Sequence number kém. Attacker sẽ thực hiện bỏ qua xác thực (Bypass Authenticate) bằng cách gửi packet một lần nữa hay còn gọi là replay.
- Man – in – the – middle:
  + Nguyên lý: Kẻ tấn công sẽ đứng giữa kênh truyền thông của hai máy tính để xem trộm thông tin và thậm chí có thể thay đổI nộI dung trao đổi giữa hai máy tính. Trong khi đó cả hai máy tính đều nghĩ rằng mình đang kết nối trực tiếp với máy tính kia.
- Phương thức phòng chống cho cả 3 loại này (vì 3 loại này có bản chất giống nhau):
  - Mã hóa lưu lượng truy cập dữ liệu thông qua giữa các bên
  - Tái tạo các phiên ID sau khi đăng nhập thành công
  - Sử dụng khóa phiên
  - Sử dụng firewall và 1 số phần mềm để ngăn chặn việc cướp quyền hoặc nghe lén.

Câu 10(Phan Kid): Tấn công SQL injection, tràn bộ đệm, chéo ngang – cross page attack ? Giải pháp phòng chống ?

- ***Tấn công SQL injection***

  + SQL injection là một kỹ thuật cho phép những kẻ tấn công lợi dụng lỗ hổng của việc kiểm tra dữ liệu đầu vào trong các ứng dụng web và các thông báo lỗi của hệ quản trị cơ sở dữ liệu trả về để inject (tiêm vào) và thi hành các câu lệnh SQL bất hợp pháp, SQL injection có thể cho phép những kẻ tấn công thực hiện các thao tác delete, insert, update,...trên cơ sở dữ liệu của ứng dụng, thậm chí là server mà ứng dụng đó đang chạy, lỗi này thường xảy ra trên các ứng dụng web có dữ liệu được quản lý bằng các hệ quản trị cơ sở dữ liệu như SQL Server, MySQL, DB2,...

  + Giải pháp phòng chống:

    - Làm sạch dữ liệu đầu vào: Mô hình Blacklist và Whitelist. Cấm những giá trị input được cho là nguy hiểm và cho phép những giá trị input cho là an toàn.
    - Xây dựng truy vấn theo mô hình tham số hóa
    - Chuẩn hóa dữ liệu
    - Các biện pháp bảo vệ database: giới hạn phạm vi ảnh hưởng của ứng dụng, giới hạn phạm vi ảnh hưởng của database

- ***Tấn công tràn bộ đệm***

  + Tấn công tràn bộ đệm (Buffer overflow attack): là phương thức tấn công vào các lỗi lập trình của phần mềm. Lỗi này có thể do lập trình viên, do bản chất của ngôn ngữ hoặc do trình biên dịch.

  + Các lỗi tràn bộ đệm có thể làm cho một tiến trình đổ vỡ hoặc cho ra các kết quả sai. Các lỗi này có thể được kích hoạt bởi các dữ liệu vào được thiết kế đặc biệt để thực thi các đoạn mã phá hoại hoặc để làm cho chương trình hoạt động một cách không như mong đợi. Gây ra nhiều lỗ hổng bảo mật đối với phần mềm và tạo cơ sở cho nhiều thủ thuật khai thác.

  + Giải pháp phòng chống:

    - Kiểm tra biên (bounds checking) đầy đủ bởi lập trình viên
    - Sử dụng trình biên dịch với các ngôn ngữ bậc cao ít có khả năng bị tấn công tràn bộ đệm.
    - Sử dụng các thư viện an toàn
    - Chống tràn bộ nhớ đệm trên stack bằng kỹ thuật Stack-smashing protection
    - Bảo vệ không gian thực thi
    - Ngẫu nhiên hóa sơ đồ không gian địa chỉ

- ***Tấn công Cross page attack (XSS):***

  + Là một kỹ thuật tấn công bằng cách chèn vào các website động (ASP, PHP,..) nhưng thẻ HTML hay những đoạn mã script nguy hiểm.

  + Trong đó những đoạn mã nguy hiểm được chèn vào hầu hết được viết bằng Client-Site script như Javascript, Jscript, DHTML và cũng có thể là các thẻ HTML.

  + Giải pháp phòng chống:

    - Mã hóa các ký tự < , > để vô hiệu hóa Script trước khi insert nó vào database, tuy bị mã hóa, nhưng lúc hiển thị ra trang web vẫn là dấu < , >.
    - Luôn luôn lọc các dữ liệu nhập từ phía người dùng bằng cách lọc các kí tự đặc biệt được định nghĩa trong đặc tả của HTML.
    - Lỗi XSS có thể tránh được khi máy chủ web đảm bảo những trang phát sinh được mã hóa thích hợp để ngăn chặn chạy những script mong muốn.

Câu 11(Hữu Anh): Tấn công DoS, DdoS nguyên lý và khả năng phòng chống ?

- ***NGUYÊN LÝ:***

Tấn công DoS(Denial-of-Service_ Tấn công từ chối dịch vụ):

Một cuộc tấn công dạng Từ-chối-Dịch-vụ /Denial-of-Service (DoS) được thiết kế để ngăn trở hoặc chặn đứng các hoạt động thông thường của một trang web, máy chủ hoặc tài nguyên mạng khác. Tin tặc có thể dùng nhiều cách khác nhau để thực hiện các cuộc tấn công này. Một phương pháp phổ biến là gửi đến nhiều yêu cầu liên tục vượt quá khả năng xử lý của máy chủ. Việc này sẽ làm cho máy chủ chạy chậm hơn bình thường (website sẽ mất nhiều thời gian hơn để mở ra hoặc xử lý thông tin) và có thể phá huỷ hoàn toàn máy chủ (dẫn đến tất cả website trên máy chủ đều bị đánh sập)

Tấn công DDoS(Distributed-Denial-of-Service_ Tấn công từ chối dịch vụ phân tán):

Một cuộc tấn công dạng Từ-chối-Dịch-vụ-Phân-tán/ Distributed-Denial-of-Service (DdoS) chỉ khác ở chỗ được thực hiện bằng cách sử dụng nhiều máy tính khác nhau. Hacker thường sử dụng một máy tính đã bị xâm nhập, gọi là "máy chủ", để điều khiển các máy bị xâm nhậm khác, gọi là "zombie" (xác chết biết đi), để thực hiện cuộc tấn công. Cả máy chủ và zombie đều bị hacker xâm nhập bằng cách cài Trojan hay mã độc, thông qua lỗ hổng của một ứng dụng nào đó trên máy.

- ***CÁCH PHÒNG CHỐNG:***

Nguyên tắc chống tấn công DoS là cần phải lọc và gạt bỏ được các luồng tin tấn công và tốt hơn nữa là ngăn chặn được các nguồn tấn công. Để chống DDoS phải vô hiệu hóa được hoạt động của các mạng botnet. Để làm được điều này một cách hiệu quả thường đòi hỏi các biện pháp điều phối ứng cứu sự cố ở quy mô quốc gia hay thậm chí phối hợp nhiều nước. Do đó khi phát hiện có các cuộc tấn công DoS hay DDoS, các đơn vị quản lý cổng/trang TTĐT cần báo cho Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) càng sớm càng tốt. Mặt khác, việc áp dụng các biện pháp và công cụ kỹ thuật tại chỗ để nâng cao năng lực bảo vệ các cổng/trang TTĐT cũng có hiệu quả rõ rệt.

Một số biện pháp kỹ thuật và công cụ phòng chống tấn công từ chối dịch vụ:

-Tăng cường khả năng xử lý của hệ thống:

+ Tối ưu hóa các thuật toán xử lý, mã nguồn của máy chủ web

+ Nâng cấp hệ thống máy chủ

+ Nâng cấp đường truyền và các thiết bị liên quan,

+ Cài đặt đầy đủ các bản vá cho hệ điều hành và các phần mềm khác để phòng ngừa khả năng bị lỗi tràn bộ đệm, cướp quyền điều khiển,v.v…

- Hạn chế số lượng kết nối tại thiết bị tường lửa tới mức an toàn hệ thống cho phép.

- Sử dụng các tường lửa cho phép lọc nội dung thông tin (tầng ứng dụng) để ngăn chặn các kết nối nhằm tấn công hệ thống.

- Phân tích luồng tin (traffic) để phát hiện các dấu hiệu tấn công và cài đặt các tường lửa cho phép lọc nội dung thông tin (tầng ứng dụng) ngăn chặn theo các dấu hiệu đã phát hiện.

- Sử dụng hệ thống thiết bị, phần mềm hoặc dịch vụ giám sát an toàn mạng (đặc biệt về lưu lượng) để phát hiện sớm các tấn công từ chối dịch vụ.

- Sử dụng thiết bị bảo vệ mạng có dịch vụ chống tấn công DDoS chuyên nghiệp kèm theo, ví dụ như: Arbor, Checkpoint, Imperva, Perimeter,…

Câu 12(Phan Kid): Khác nhau giữa virus, worm, trojan, backdoor

Virus	Worm	Trojan	Backdoor
Là một chương trình, hoặc đoạn chương trình kí sinh trên chương trình khác. Virus nằm trên 1 file.	+ Là một file độc lập.	+ Là một chương trình, mã độc nằm chứa trong 1 chương trình hợp pháp, ẩn trong máy tính	+ Là một đoạn chương trình
Thi hành khi file kí sinh được mở, kích hoạt.	Tự thi hành, tấn công qua danh sách địa chỉ.	Ẩn trong máy đến khi 1 chương trình khác kích hoạt thì thi hành	Khi nhận được lệnh từ ngoài, nó được kích hoạt và phá hoại theo mục đích.
Có khả năng tự nhân bản	Có khả năng tự nhân bản	Không tự nhân bản	Không tự nhân bản
Nguy hiểm: Tấn công, phá hoại làm hư hại, hỏng, mất dữ liệu,.v…v	Nguy hiểm: tương đương với virus, nguy hiểm hơn với tấn công và tự lây lan qua hệ thống mạng.	Nguy hiểm: sao chép và khai thác thông tin, dữ liệu của nạn nhân, gửi về cho tin tặc để tin tặc có thể lấy cắp dữ liệu, xóa file,….	Nguy hiểm: Mở một dịch vụ nào đó để tạo cổng sau nhằm mục đích dễ dàng đột nhập vào máy tính nạn nhân một cách kín đáo khi cần.

Câu 13(Tú Cẩm): Khả năng bảo vệ hệ thống của trình quét virus và firewall

Bài làm:

- **Khả năng bảo vệ hệ thống của trình quét virus:**

+ Virus là một phần mã máy tính tự gắn nó với một chương trình hoặc một tệp để nó có thể phát tán từ máy tính tới máy tính, lây nhiễm khi nó di chuyển. Các vi rút có thể phá hủy phần mềm, phần cứng, và các tệp của bạn.

+ Nguyên lý hoạt động của trình diệt virus:

. Dựa trên database có sẵn: lúc này antivirus sẽ quét ổ cứng kiểm tra xem coi có file nào có trùng mã hash (thường là md5) với virus có trong database không? nếu trùng thì nó sẽ delete hoặc cách ly...

. **Dùng các thuật toán thông minh**: lúc này antivirus sẽ dựa trên cách thức hoạt động của một chương trình để kiểm tra xem nó có giống với virus hay không. Ngoài ra, khi quét các file trên một ổ đĩa nào đó, antivirus sẽ không kiểm tra dựa trên database mà dựa trên các dấu hiệu chung của virus để nhận diện. Dĩ nhiên nhận diện thông minh sẽ có một sai số nhất định (tỉ lệ nhận lầm file là virus, hay không nhận diện được virus ...)

- **Khả năng bảo vệ hệ thống của firewall:** .

+ **Tính năng** chính của FireWall là

Chức năng chính của Firewall là kiểm soát luồng thông tin từ giữa Intranet và Internet. Thiết lập cơ chế điều khiển dòng thông tin giữa mạng bên trong (Intranet) và mạng Internet. Cụ thể là:
- Cho phép hoặc cấm những dịch vụ truy nhập ra ngoài (từ Intranet ra Internet).
- Cho phép hoặc cấm những dịch vụ phép truy nhập vào trong (từ Internet vào Intranet).
- Theo dõi luồng dữ liệu mạng giữa Internet và Intranet.
- Kiểm soát địa chỉ truy nhập, cấm địa chỉ truy nhập.
- Kiểm soát người sử dụng và việc truy nhập của người sử dụng.
- Kiểm soát nội dung thông tin thông tin lưu chuyển trên mạng.

Câu 14(Tú Cẩm): IPSec, VPN khả năng bảo vệ thông tin trên đường truyền

- Lý thuyết về VPN khiến người ta liên tưởng VPN với sự an toàn, với tính ẩn danh và sử dụng VPN để giữ bí mật thông tin, để che giấu vị trí địa lý thật của mình.... Nhưng thực tế cho thấy lưu lượng VPN hoàn toàn có khả năng rò rỉ vào mạng truyền thông ở dạng rõ, mà nếu không bị rò rỉ thì vẫn có thể bị giải mã. Bên cạnh đó, nếu VPN hoạt động theo giao thức PPTP thì có thể coi rằng dữ liệu không hề được mã hóa.
- **IPSec** là 1 giao thức của mạng riêng ảo VPN được làm việc tại tầng Network Layer – layer 3 của mô hình OSI , bao gồm những giao thức cung cấp cho mã hoá và xác thực. Cấu trúc của nó gồm:

    1. Sử dụng các giao thức cung cấp mật mã nhằm bảo mật gói tin trong quá trình truyền
    2. Cung cấp phương thức xác thực.
    3. Thiết lập các thông số mã hóa

- Tính năng của IPSec:

    1. Mã hóa quá trình truyền thông tin
    2. Đảm bảo tính nguyên vẹn của dữ liệu
    3. Phải được xác thực giữa các giao tiếp
    4. Chống quá trình replay trong các phiên bảo mật
    5. Modes- các mode

- Nguyên lí hoạt động:

1. Transport Mode (chế độ vận chuyển): cung cấp cơ chế bảo vệ cho dữ liệu của các lớp cao hơn, thêm vào vài bytes cho mỗi packets và nó cũng cho phép các thiết bị trên mạng thấy được địa chỉ đích cuối cùng của gói. Khả năng này cho phép các tác vụ xử lý đặc biệt trên các mạng trung gian dựa trên các thông tin trong IP header.

2. Tunnel Mode (Chế độ đường hầm): Tunnel mode bảo vệ toàn bộ gói dữ liệu. Với tunnel hoạt động giữa hai security gateway, địa chỉ nguồn và đích có thể được mã hóa