MỤC LỤC

LỜI MỞ ĐẦU **1**
TÓM TẮT NỘI DUNG **2**
Chương 1. **CÁC KHÁI NIỆM CƠ BẢN** **3**
1.1. MỘT SỐ KHÁI NIỆM TOÁN HỌC **3**
1.1.1. Ước chung lớn nhất, bội chung nhỏ nhất **3**
1.1.2. Quan hệ " Đồng dư " **4**
1.1.3. Số nguyên tố **5**
1.1.4. Khái niệm nhóm, nhóm con, nhóm Cyclic **5**
1.1.5. Phần tử nghịch đảo **7**
1.1.6. Các phép tính cơ bản trong không gian modulo **7**
1.1.7. Độ phức tạp của thuật toán **8**
1.2. TỔNG QUAN VỀ AN TOÀN THÔNG TIN **9**
1.2.1. Khái niệm về thông tin dữ liệu **9**
1.2.2. An toàn thông tin **10**
1.2.3. Các chiến lược an toàn thông tin hệ thống **11**
1.2.4. Các mức bảo vệ trên mạng **13**
1.2.5. An toàn thông tin bằng mã hóa **15**
1.2.6. Hệ mã hóa **16**
1.2.6.1 Tổng quan về mã hóa dữ liệu **16**
1.2.6.2. Hệ mã hóa khóa công khai **19**
1.2.6.3. Hệ mã hóa khóa đối xứng cổ điển **22**
1.2.6.4. Hệ mã hóa khóa đối xứng DES **26**
1.2.7. Chữ ký số **29**
1.2.7.1. Giới thiệu **29**
1.2.7.2. Phân loại chữ ký số **31**
1.2.7.3.Một số loại chữ ký số **32**
1.3. TỔNG QUAN VỀ MẠNG RIÊNG ẢO **36**
1.3.1. Khái niệm mạng riêng ảo **36**
1.3.2. Mục đích **38**
1.3.3. Chức năng **39**
1.3.4. Lợi ích của công nghệ VPN **39**

1.3.5. Các dạng kết nối mạng riêng ảo 42
1.3.5.1. VPN truy nhập từ xa (Remote Access VPNs) 42
1.3.5.2. Site – To – Site VPN 44
1.3.6. Giới thiệu một số giao thức đường hầm trong VPN 48
***Chương 2* 52**
MỘT SỐ BÀI TOÁN AN TOÀN THÔNG TIN TRONG MẠNG RIÊNG ẢO 52
2.1. KIỂM SOÁT TRUY NHẬP MẠNG RIÊNG ẢO 52
2.1.1. Bài toán kiểm soát truy nhập trong Mạng riêng ảo 52
2.1.2. Phương pháp giải quyết 52
2.1.2.1. Kiểm soát truy nhập bằng mật khẩu 52
2.1.2.2.Kiểm soát truy nhập bằng chữ ký số 53
2.2. BẢO MẬT THÔNG TIN TRONG MẠNG RIÊNG ẢO 55
2.2.1. Bài toán bảo mật thông tin trong Mạng riêng ảo 55
2.2.2. Bảo mật thông tin bằng phương pháp mã hóa 56
2.3. BẢO TOÀN THÔNG TIN TRONG MẠNG RIÊNG ẢO 59
2.3.1. Bài toán bảo toàn thông tin trong Mạng riêng ảo 59
2.3.2. Phương pháp giải quyết 60
2.3.2.1. Bảo toàn bằng phương pháp mã hóa 60
2.3.2.2. Bảo toàn sử dụng kỹ thuật chữ ký số 61
***Chương 3.* THỬ NGHIỆM CHƯƠNG TRÌNH 62**
3.1. THỬ NGHIỆM CHƯƠNG TRÌNH 62
3.1.1. Chương trình mã hóa dịch chuyển 62
3.1.2. Chương trình chữ ký số RSA 62
3.2. CẤU HÌNH HỆ THỐNG 63
3.3. CÁC THÀNH PHẦN CỦA CHƯƠNG TRÌNH 64
3.3.1. Chương trình mã hóa dịch chuyển 64
3.3.2. Chương trình ký số RSA 64
3.4. HƯỚNG DẪN SỬ DỤNG CHƯƠNG TRÌNH 65
3.4.1. Chương trình mã hóa dịch chuyển 65
3.4.2. Chương trình ký số RSA 67
KẾT LUẬN 69
PHỤ LỤC 70

LỜI CẢM ƠN

Lời đầu em gửi lời cảm ơn chân thành tới thầy **PGS.TS Trịnh Nhật Tiến** Khoa Công nghệ thông tin trường Đại học Công Nghệ, ĐHQG HN đã tận tình hướng dẫn em và tạo điều kiện tốt nhất để em hoàn thành đề tài tốt nghiệp này.

Em cũng xin cảm ơn các thầy các cô giáo trong khoa Công nghệ thông tin – Trường Đại học dân lập Hải Phòng đã giúp đỡ em trong suốt khóa học tại trường. Cũng như sự đóng góp quý báu của các thầy cô với đề tài tốt nghiệp này của em.

LỜI MỞ ĐẦU

Ngày nay, công nghệ viễn thông đang phát triển rất nhanh. Trong đó công nghệ mạng đóng vai trò hết sức quan trọng trong việc thông tin dữ liệu. Chỉ xét về góc độ kinh doanh, nhu cầu truyền thông của các công ty, tổ chức là rất lớn. Một công ty có một mạng riêng cho phép chia sẻ tài nguyên giữa các máy tính nội bộ. Nhưng cũng muốn chi nhánh, văn phòng, nhân viên di động hay các đối tác từ xa có thể truy cập vào mạng công ty. Có nhiều dịch vụ được cung cấp như Modem quay số, ISDN server hay các đường truyền WAN thuê riêng đắt tiền. Nhưng với sự phát triển rộng rãi của mạng Internet, một số công ty có thể kết nối với nhân viên, đối tác từ xa ở bất cứ đâu, thậm chí trên toàn thế giới mà không cần sử dụng các dịch vụ đắt tiền trên.

Nhưng có một vấn đề là mạng nội bộ công ty chứa tài nguyên, dữ liệu quan trọng mà chỉ cho phép người dùng có quyền hạn, được cấp phép mới được truy cập vào mạng. Trong khi Internet là mạng công cộng và không bảo mật. Do đó, Internet có thể là mối nguy hiểm cho hệ thống mạng, cơ sở dữ liệu quan trọng của công ty. Sự thông tin qua môi trường Internet có thể bị làm sai lệch hoặc bị đánh cắp. Và đây chính là chỗ để mạng riêng ảo (VPN – Virtual Private Network) chứng tỏ khả năng. VPN cung cấp giải pháp thông tin dữ liệu riêng tư an toàn thông qua môi trường mạng Internet công cộng với chi phí thấp, hiệu quả mà vẫn rất bảo mật.

Sau thời gian được học ở trường với sự dạy dỗ và định hướng của các thầy cô giáo trong khoa, em đã trọn đề tài "NGHIÊN CỨU MỘT SỐ BÀI TOÁN AN TOÀN THÔNG TIN TRONG MẠNG RIÊNG ẢO" để làm đồ án tốt nghiệp cũng như học hỏi thêm kiến thức để sau này áp dụng vào thực tế công việc của chúng em. Do thời gian và kiến thức còn nhiều hạn chế, nên quyển đồ án này sẽ còn nhiều thiếu sót. Kính mong sự hướng dẫn, góp ý thêm của thầy cô và bạn bè.

Em xin chân thành cảm ơn!

TÓM TẮT NỘI DUNG

Nhu cầu truy cập từ xa (ngoài văn phòng) mạng nội bộ để trao đổi dữ liệu hay sử dụng ứng dụng ngày càng phổ biến. Đây là nhu cầu thiết thực, tuy nhiên do vấn đề bảo mật và an toàn thông tin nên các công ty ngại "mở" hệ thống mạng nội bộ của mình để cho phép nhân viên truy cập từ xa.

Mục đích và ý nghĩa thực tiễn:

- Nhằm đáp ứng nhu cầu chia sẻ thông tin, truy cập từ xa và tiết kiệm chi phí.
- Cho phép các máy tính truyền thông với nhau thông qua một môi trường chia sẻ như mạng Internet nhưng vẫn đảm bảo được tính riêng tư và bảo mật dữ liệu.
- Cung cấp kết nối giữa các máy tính, cho phép dữ liệu có thể gửi từ máy truyền qua môi trường mạng chia sẻ và đến được máy nhận.
- Bảo đảm tính riêng tư và bảo mật trên môi trường chia sẻ này, các gói tin được mã hóa và chỉ có thể giải mã với những khóa thích hợp, ngăn ngừa trường hợp "trộm" gói tin trên đường truyền.

Cách tiếp cận và phương pháp giải quyết: do các vấn đề bảo mật và an toàn thông tin được trao đổi từ các máy trong mạng riêng ảo nên cần phải có cơ chế bảo đảm an toàn thông tin. Từ các khái niệm tổng quan về bảo đảm an toàn thông tin đến các chương trình mã hóa dữ liệu, và các chương trình ký số giúp giải quyết việc che giấu thông tin được trao đổi qua mạng riêng ảo. Bảo đảm dư liệu được nguyên vẹn từ nơi gửi đi thì nơi nhận cũng phải nhận được nguyên vẹn và chính xác về nội dung.

Kết quả mong muốn: cung cấp kết nối an toàn và hiệu quả để truy cập tài nguyên nôi bộ công ty từ bên ngoài thông qua mạng Internet. Mặc dù sử dụng hạ tầng mạng chia sẻ nhưng chúng ta vẫn đảm bảo được tính riêng tư của dữ liệu giống như đang truyền thông trên một hệ thống mạng riêng.

Chương 1. CÁC KHÁI NIỆM CƠ BẢN

1.1. MỘT SỐ KHÁI NIỆM TOÁN HỌC

1.1.1. Ước chung lớn nhất, bội chung nhỏ nhất

1.1.1.1. Ước số và bội số

Cho hai số nguyên a và b, b ≠ 0. Nếu có một số nguyên q sao cho a = b*q, thì ta nói rằng a ***chia hết*** cho b, kí hiệu b\a. Ta nói b là ước của a, và a là bội của b.

Ví dụ:

Cho a = 6, b = 2, ta có 6 = 2*3, ký hiệu 2\6. Ở đây 2 là ước của 6 và 6 là bội của 2.

Cho các số nguyên a, b ≠ 0, tồn tại cặp số nguyên (q, r) (0≤ r ≤ /b/) duy nhất sao cho **a = b*q + r.** Khi đó q gọi là ***thương nguyên,*** **r** gọi là *số dư* của phép chia a cho b. Nếu r = 0 thì ta có phép chia hết.

***Ví dụ*:**

Cho a = 13, b = 5, ta có 12 = 5*2 + 3. Ở đây thương q=2, số dư là r = 3.

1.1.1.2. Ước chung lớn nhất, bội chung nhỏ nhất.

Số nguyên d được gọi là *ước chung* của các số nguyên $a_1,a_2,\ldots,a_n$, nếu nó là *ước* của tất cả các số đó.

Số nguyên m được gọi là *bội chung* của các số nguyên $a_1,a_2,\ldots,a_n$, nếu nó là *bội* của tất cả các số đó.

Một ước chung d >0 của các số nguyên $a_1,a_2,\ldots,a_n$, trong đó mọi ước chung của $a_1,a_2,\ldots,a_n$, đều là ước của d, thì d được gọi là *ước chung lớn nhất* (UCLN) của $a_1,a_2,\ldots,a_n$. Ký hiệu d = gcd($a_1,a_2,\ldots,a_n$) hay d = UCLN($a_1,a_2,\ldots,a_n$).

Nếu gcd($a_1,a_2,\ldots,a_n$) = 1, thì các số $a_1,a_2,\ldots,a_n$ được gọi là *nguyên tố cùng nhau.*

Một bội chung m >0 của các số nguyên $a_1,a_2,\ldots,a_n$, trong đó mọi bội chung của $a_1,a_2,\ldots,a_n$ đều là bội của m, thì m được gọi là *bội chung nhỏ nhất* (BCNN) của $a_1,a_2,\ldots,a_n$. Ký hiệu m = lcm($a_1,a_2,\ldots,a_n$) hay m = BCNN($a_1,a_2,\ldots,a_n$).

Ví dụ:

Cho a =12, b=15, gcd(12,15) = 3, lcm(12,15) = 60.

Hai số 8 và 13 là *nguyên tố cùng nhau*, vì gcd(8, 13) =1.

Ký hiệu :

Z_n = {0, 1, 2, … , n-1} là tập các số nguyên không âm < n.

Z_n^* = {e ∈ Z_n , e là nguyên tố cùng nhau với n}. Tức là e # 0.

1.1.2. Quan hệ " Đồng dư "

1.1.2.1. Khái niệm

Cho các số nguyên a, b, m (m >0). Ta nói rằng a và b ***"đồng dư" với nhau*** theo modulo m, nếu chia a và b cho m, ta nhận được cùng một số dư.

Ký hiệu : a ≡ b(mod m).

Ví dụ : 17 ≡ 5 (mod 3) vì 17 và 5 chia cho 3 được cùng số dư là 2.

1.1.2.2. Các tính chất của quan hệ "Đồng dư"

1). Quan hệ "đồng dư" là quan hệ tương đương trong Z.

Với mọi số nguyên dương m ta có :

a ≡ a (mod m) với mọi a ∈ Z;

a ≡ b (mod m) thì b ≡ a (mod m);

a ≡ b (mod m) và b ≡ c (mod m) thì a ≡ c (mod m);

2). Tổng hay hiệu các "đồng dư" :

(a + b) (mod n) = [(a mod n) + (b mod n)] (mod n)

(a - b) (mod n) = [(a mod n) - (b mod n)] (mod n)

3). Tích các "đồng dư":

(a * b) (mod n) = [(a mod n) * (b mod n)] (mod n)

1.1.3. Số nguyên tố

1.1.3.1. Khái niệm

Số nguyên tố là số tự nhiên lớn hơn 1 và chỉ có hai ước là 1 và chính nó.

Ví dụ :

Các số 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31 là các số nguyên tố.

1.1.3.2. Định lý về số nguyên tố

1). Định lý : Về số nguyên dương > 1.

Mọi số nguyên dương n >1 đều có thể biểu diễn được *duy nhất* dưới dạng :

$n=P_1^{n_1}.P_1^{n_2}\ldots P_1^{n_k}$, trong đó :

k, n_i (i = 1,2,…,k) là các số tự nhiên, P_i là các số nguyên tố, từng đôi một khác nhau.

2). Định lý : Mersenne.

Cho $p = 2^k - 1$, nếu p là số nguyên tố, thì k phải là số nguyên tố.

3). Hàm Euler.

Cho số nguyên dương n, số lượng các số nguyên dương bé hơn n và *nguyên tố cùng nhau* với n được ký hiệu ø(n) và gọi là hàm *Euler.*

Nhận xét : Nếu p là số nguyên tố, thì ø(p) = p-1.

Định lý về Hàm Euler : Nếu n là tích của hai số nguyên tố n = p.q,

Thì ø(n) = ø(p).ø(q) = (p-1)(q-1)

1.1.4. Khái niệm nhóm, nhóm con, nhóm Cyclic

a) Nhóm là bộ các phần tử (G, *) thỏa mãn các tính chất sau:

+ Tính chất kết hợp: (x * y) * z = x * (y * z)

+ Tính chất tồn tại phần tử trung gian e ∈ G: e * x = x * e = x, ∀x ∈G

+ Tính chất tồn tại phần tử nghịch đảo x’ ∈G: x’ * x = x * x’ = e

b) Nhóm con của G là tập $S \subset G$, $S \neq \emptyset$, và thỏa mãn các tính chất sau:

+ Phần tử trung lập e của G nằm trong S.

+ S khép kín đối với phép tính (*) trong, tức là $x * y \in S$ với mọi $x, y \in S$.

+ S khép kín đối với phép lấy nghịch đảo trong G, tức $x^{-1} \in S$ với mọi $x \in S$.

c) Nhóm cyclic:

(G, *) là nhóm được sinh ra bởi một trong các phần tử của nó. Tức là có phần tử $g \in G$ mà với mỗi $a \in G$, đều tồn tại số $n \in N$ để $g^n = a$. Khi đó g là phần tử sinh hay phần tử nguyên thủy của nhóm G.

Ví dụ:

$(Z^+, *)$ gồm các số nguyên dương là một nhóm cyclic có phần tử sinh là 1.

d) Nhóm (Z_n^*, phép nhân mod n)

+ Kí hiệu $Z_n = \{0, 1, 2, \ldots, n-1\}$ là tập các số nguyên không âm < n.

Z_n và phép cộng (+) lập thành nhóm Cyclic có phần tử sinh là 1, phần tử trung lập e = 0.

$(Z_n, +)$ gọi là nhóm cộng, đó là nhóm hữu hạn có cấp n.

+ Kí hiệu $Z_n^* = \{x \in Z_n$, x là nguyên tố cùng nhau với n}. Tức là x phải $\neq 0$.

Z_n^* được gọi là Tập thặng dư thu gọn theo mod n, có phần tử là ø(n).

Z_n^* với phép nhân mod n, lập thành một nhóm (nhóm nhân), phần tử trung lập e = 1.

Tổng quát (Z_n^*, phép nhân mod n) không phải là nhóm Cyclic.

Nhóm nhân Z_n^* là Cyclic chỉ khi n có dạng: 2, 4, p^k, hay $2p^k$ với p là nguyên tố lẻ.

1.1.5. Phần tử nghịch đảo

1). Khái niệm.

Cho a ∈ Z_n. Nếu tồn tại b ∈ Z_n sao cho a*b ≡ 1 (mod n), ta nói b là phần tử nghịch đảo của a trong $Z_n$và ký hiệu a^{-1}. Một phần tử có phần tử nghịch đảo, gọi là khả nghịch.

2). Tính chất:

+ Cho a, b ∈Z_n. Phép chia của a cho b theo modulo n là tích của a và b^{-1} theo modulo n và chỉ được xác định khi b khả nghịch theo modulo n.

+ Cho a ∈ Z_n, a khả nghịch khi và chỉ khi UCLN(a, n) = 1.

+ Giả sử d = UCLN (a, n). Phương trình đồng dư ax ≡ b mod n có nghiệm x nếu và chỉ nếu d chia hết cho b, trong trường hợp các nghiệm d nằm trong khoảng [0, n-1] thì các nghiệm đồng dư theo modulo $\frac{n}{d}$.

Ví dụ: 4^{-1}= 7 mod 9 vì 4 . 7 ≡ 1 mod 9

1.1.6. Các phép tính cơ bản trong không gian modulo

Cho n là số nguyên dương. Các phần tử trong Z_n được thể hiện bởi các số nguyên {0, 1, 2, ..., n-1}. Nếu a, b ∈ $Z_n$thì:

$$(a + b) \bmod n = \begin{cases} a + b \; nu \;\; a + b < n \\ a + b - n \; nu \; a + b \geq n \end{cases}$$

Vì vậy, phép cộng modulo (và phép trừ modulo) có thể được thực hiện mà không cần thực hiện các phép chia dài. Phép nhân modulo của a và b được thực hiện bằng phép nhân thông thường a với b như các số nguyên bình thường, sau đó lấy phần dư của kết quả sau khi chia cho n.

1.1.7. Độ phức tạp của thuật toán

1). Chi phí của thuật toán.

Chi phí phải trả cho một quá trình tính toán gồm chi phí thời gian và bộ nhớ.

+ Chi phí thời gian của một quá trình tính toán là thời gian cần thiết để thực hiện một quá trình tính toán.

+ Chi phí bộ nhớ của một quá trình tính toán là số ô nhớ cần thiết để thực hiện một quá trình tính toán.

Gọi A là một thuật toán, e là dữ liệu vào của bài toán đã được mã hóa.

Thuật toán A tính trên dữ liệu vào e phải trả một giá nhất định.

Ký hiệu: $t_A(e)$ là giá thời gian và $l_A(e)$ là giá bộ nhớ.

2). Độ phức tạp về bộ nhớ:

$t_A(n) = \max \{ l_A(e)$, với $|e| \leq n\}$, n là "kích thước" đầu vào của thuật toán.

3). Độ phức tạp về thời gian:

$l_A(n) = \max \{ t_A(e)$, với $|e| \leq n\}$.

4). Độ phức tạp tiệm cận:

Độ phức tạp PT(n) được gọi là tiệm cận tới hàm f(n), ký hiệu O(f(n)) nếu tồn tại các số n_0, c mà $PT(n) \leq c.f(n)$, $\forall n \leq n_0$.

5). Độ phức tạp đa thức:

Độ phức tạp PT(n) được gọi là đa thức, nếu nó tiệm cận tới đa thức p(n).

6).Thuật toán đa thức:

Thuật toán được gọi là đa thức, nếu độ phức tạp về thời gian là đa thức.

1.2. TỔNG QUAN VỀ AN TOÀN THÔNG TIN

1.2.1. Khái niệm về thông tin dữ liệu

Dữ liệu (data) là những dữ kiện thô chưa qua xử lý. Có nhiều kiểu dữ liệu có thể được sử dụng để biểu diễn các dữ kiện này. Khi các yếu tố này được tổ chức hoặc sắp xếp theo một cách có nghĩa thì chúng trở thành thông tin. Dữ kiện trên các hóa đơn bán hàng là ví dụ về dữ liệu trong HTTT quản lí bán hàng.

Thông tin (information) là một bộ các dữ liệu được tổ chức theo một cách sao cho chúng mang lại một giá trị tăng so với giá trị vốn có cuả bản thân dữ kiện đó.

Để có giá trị sử dụng đối với những người làm công tác quản lý và ra quyết định, thông tin cần phải có những thuộc tính sau:

- Tính chính xác: Thông tin chính xác là những thông tin không chứa lỗi. Thông tin không chính xác thường được tạo ra từ những dữ liệu không chính xác được nhập vào hệ thống trước đó.
- Tính đầy đủ: Thông tin đầy đủ là thông tin chứa mọi dữ kiện quan trọng. Một báo cáo đầu tư bị xem là không đầy đủ nếu nó không đề cập tới tất cả chi phí liên quan.
- Tính kinh tế: Thông tin được xem là kinh tế khi giá trị mà nó mang lại phải vượt chi phí tạo ra nó.
- Tính mềm dẻo: Thông tin được coi là có tính mềm dẻo khi nó có thể được sử dụng cho nhiều mục đích khác nhau, ví dụ thông tin về hàng tồn kho có thể được sử dụng cho nhân viên quản lí bán hàng, đồng thời cũng có giá trị sử dụng cho nhân viên quản lí sản xuất và nhà quản lí tài chính.
- Tính tin cậy: Tính tin cậy của thông tin phụ thuộc vào nhiều yếu tố. Nó có thể phụ thuộc vào phương pháp thu thập dữ liệu, cũng có thể phụ thuộc vào nguồn gốc của thông tin.
- Tính liên quan: Tính liên quan của thông tin đối với người ra quyết định là rất quan trọng. Tính liên quan của thông tin thể hiện ở chỗ nó có đến đúng đối tượng nhận tin hay không? Nó có mang lại giá trị sử dụng cho đối tượng nhận tin hay không?

- Tính đơn giản: Thông tin đến tay người sử dụng cần đơn giản, không quá phức tạp. Nhiều khi quá nhiều thông tin sẽ gây khó khăn cho người sử dụng trong việc lựa chọn thông tin.
- Tính kịp thời: Thông tin được coi là kịp thời khi nó đến với người sử dụng và đúng thời điểm cần thiết.
- Tính kiểm tra được: Đó là thông tin cho phép người ta kiểm định để chắc chắn rằng nó hoàn toàn chính xác (bằng cách kiểm tra nhiều nguồn cho cùng một thông tin).
- Tính dễ khai thác: Đó là những thông tin có thể tra cứu dễ dàng đối với những người sử dụng có thẩm quyền theo đúng dạng vài đúng thời điểm mà họ cần.
- Tính an toàn: Thông tin cần được bảo vệ trước người sử dụng không có thẩm quyền.

1.2.2. An toàn thông tin

1.2.2.1. Khái niệm an toàn thông tin

An toàn thông tin có mục đích là phải tổ chức việc xử lý, ghi nhớ và trao đổi thông tin sao cho bảo đảm tính bí mật, toàn vẹn, xác thực, và sẵn sàng được bảo đảm ở mức đầy đủ.

An toàn thông tin bao gồm các nội dung sau:

- Tính bí mật: Tính kín đáo riêng tư của thông tin.
- Tính toàn vẹn: Bảo vệ thông tin, không cho phép sửa đổi thông tin trái phép.
- Tính xác thực: Tính xác thực của thông tin, bao gồm xác thực đối tác (bài toán nhận danh), xác thực thông tin trao đổi.
- Bảo đảm sẵn sàng: Thông tin sẵn sàng cho người dùng hợp pháp.

1.2.2.2. Các nhóm trong an toàn thông tin

An toàn thông tin được chia thành 11 nhóm:

- Chính sách an toàn thông tin (Infomaton security policy): chỉ thị và hướng dẫn về an toàn thông tin.
- Tổ chức an toàn thông tin (Organization of information security): tổ chức biện pháp an toàn và quy trình quản lý.
- Quản lý tài sản (Asset management): trách nhiệm và phân loại giá trị thông tin.
- An toàn tài nguyên con người (Human resource security): bảo đảm an toàn.
- An toàn vật lý và môi trường (Physical and environmental security)
- Quản lý vận hành và trao đổi thông tin (Communicstions and operations management).
- Kiểm soát truy nhập (Access control).
- Thu nhận, phát triển và bảo quản các hệ thống thông tin (Information system acquisition, development and maintenance).
- Quản lý sự cố mất an toàn thông tin (Information security incident management).
- Quản lý duy trì khả năng tồn tại của doanh nghiệp (Business continuity management)
- Tuân thủ các qui định của pháp luật (Compliance).

1.2.3. Các chiến lược an toàn thông tin hệ thống

1.2.3.1. Giới hạn quyền hạn tối thiểu (Last Privilege)

Đây là chiến lược cơ bản nhất, theo nguyên tắc này bất kỳ một đối tượng nào cũng chỉ có những quyền hạn nhất định đối với tài nguyên mạng, khi thâm nhập vào mạng đối tượng đó chỉ được sử dụng một số tài nguyên nhất định.

1.2.3.2. Bảo vệ theo chiều sâu (Defence In Depth)

Nguyên tắc này nhắc nhở chúng ta: không nên dựa vào một chế độ an toàn nào dù cho chúng rất mạnh, mà nên tạo nhiều cơ chế an toàn tương hỗ lẫn nhau.

1.2.3.3. Nút thắt (Choke Point)

Tạo ra một "cửa khẩu" hẹp, và chỉ cho phép thông tin đi vào hệ thống của mình bằng con đường duy nhất chính là "cửa khẩu" này => phải tổ chức một cơ cấu kiểm soát và điều khiển thông tin đi qua cửa này.

1.2.3.4. Điểm nối yếu nhất (Weakes Link)

Chiến lược này dựa trên nguyên tắc: " Một dây xích chỉ chắc tại mắt duy nhất, một bức tường chỉ cứng tại điểm yếu nhất".

Kẻ phá hoại thường tìm chỗ yếu nhất của hệ thống để tấn công, do đó ta cần phải gia cố các điểm yếu của hệ thống. Thông thường chúng ta chỉ quan tâm đến kẻ tấn công trên mạng hơn là kẻ tiếp cận hệ thống, do đó an toàn vật lý được coi là điểm yếu nhất trong hệ thống của chúng ta.

1.2.3.5. Tính toàn cục

Các hệ thống an toàn đòi hỏi phải có tính toàn cục của các hệ thống cục bộ. Nếu có một kẻ nào đó có thể bẻ gãy một cơ chế an toàn thì chúng có thể thành công bằng cách tấn công hệ thống tự do của ai đó và sau đó tấn công hệ thống từ nội bộ bên trong.

1.2.3.6. Tính đa dạng bảo vệ

Cần phải sử dụng nhiều biện pháp bảo vệ khác nhau cho hệ thống khác nhau, nếu không có kẻ tấn công vào được một hệ thống thì chúng cũng dễ dàng tấn công vào hệ thống khác.

1.2.4. Các mức bảo vệ trên mạng

Vì không thể có một giải pháp an toàn tuyệt đối, nên người ta thường phải sử dụng đồng thời nhiều mức bảo vệ khác nhau tạo thành nhiều hàng rào chắn đối với các hoạt động xâm phạm. Việc bảo vệ thông tin trên mạng chủ yếu là bảo vệ thông tin cất giữ trong máy tính, đặc biệt là các server trên mạng. Bởi thế, ngoài một số biện pháp nhằm chống thất thoát thông tin trên đường truyền, mọi cố gắng tập trung vào việc xây dựng các mức rào chắn từ ngoài vào trong cho các hệ thống kết nối vào mạng. Thông thường bao gồm các mức bảo vệ sau:

1.2.4.1. Quyền truy nhập

Lớp bảo vệ trong cùng là quyền truy nhập, nhằm kiểm soát các tài nguyên của mạng và quyền hạn trên tài nguyên đó. Dĩ nhiên là kiểm soát được các cấu trúc dữ liệu càng chi tiết càng tốt. Hiện tại việc kiểm soát thường ở mức tệp.

1.2.4.2. Đăng ký tên/ mật khẩu

Thực ra đây cũng là kiểm soát quyền truy nhập, nhưng không phải truy nhập ở mức thông tin mà ở mức hệ thống. Đây là phương pháp bảo vệ phổ biến nất vì nó đơn giản ít phí tổn và cũng rất hiệu quả.

Mỗi người sử dụng muốn được tham gia vào mạng để sử dụng tài nguyên đều phải có đăng ký tên và mật khẩu trước.

Người quản trị mạng có trách nhiệm quản lý, kiểm soát mọi hoạt động của mạng và xác định quyền truy nhập của những người sử dụng khác theo thời gian và không gian (nghĩa là người sử dụng chỉ được truy nhập trong một khoảng thời gian nào đó, tại một vị trí nhất định nào đó).

Về lý thuyết nếu mọi người đều giữ kín được mật khẩu và tên đăng ký của mình thì sẽ không xảy ra các truy nhập trái phép. Song điều đó khó đảm bảo trong thực tế vì nhiều nguyên nhân rất đời thường làm giảm hiệu quả của lớp bảo vệ này. Có thể khắc phục bằng cách người quản trị mạng chịu trách nhiệm đặt mật khẩu hoặc thay đổi mật khẩu theo thời gian.

1.2.4.3. Mã hóa dữ liệu

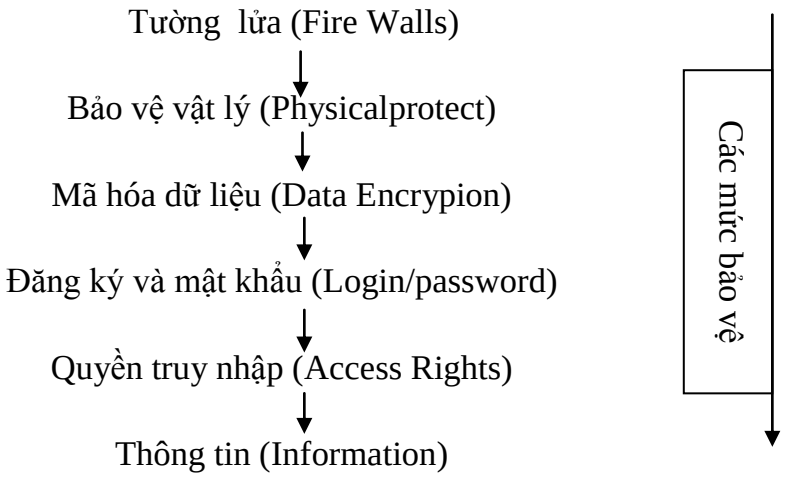
Để bảo mật thông tin trên đường truyền người ta sử dụng các phương pháp mã hóa. Dữ liệu bị biến đổi từ dạng nhận thức được sang dạng không nhận thức được theo một thuật toán nào đó và sẽ được biến đổi ngược lại ở trạm nhận (giải mã). Đây là lớp bảo vệ thông tin rất quan trọng.

1.2.4.4. Bảo vệ vật lý

Ngăn cản các truy nhập vật lý vào hệ thống. Thường dùng các biện pháp truyền thống như ngăn cấm tuyệt đối người không phận sự vào phòng đặt máy mạng, dùng ổ khóa trên máy tính hoặc các máy trạm không có ổ mềm.

1.2.4.5. Tường lửa

Ngăn chặn thâm nhập trái phép và lọc bỏ các gói tin không muốn gửi hoặc nhận vì các lý do nào đó để bảo vệ một máy tính hoặc cả mạng nội bộ (Intranet).



1.2.4.6. Quản trị mạng

Trong thời đại phát triển của công nghệ thông tin, mạng máy tính quyết định toàn bộ hoạt động của một cơ quan, hay một công ty xí nghiệp. Vì vậy việc bảo đảm cho hệ thống mạng máy tính hoạt động một cách an toàn, không xảy ra sự cố là một công việc cấp thiết hàng đầu. Công tác quản trị mạng máy tính phải được thực hiện một cách khoa học đảm bảo các yêu cầu sau:

- Toàn bộ hệ thống hoạt động bình thường trong giờ làm việc.
- Có hệ thống dự phòng khi có sự cố về phần cứng hoặc phần mềm xảy ra.
- Sao lưu dữ liệu quan trọng theo định kỳ.
- Bảo dưỡng mạch theo định kỳ.
- Bảo mật dữ liệu, phân quyền truy cập, tổ chức nhóm làm việc trên mạng.

1.2.5. An toàn thông tin bằng mã hóa

Để bảo vệ thông tin trên đường truyền người ta thường biến đổi nó từ dạng nhận thức được sang dạng không nhận thức được trước khi truyền đi trên mạng, quá trình này gọi là mã hóa thông tin (Encryption).

Tai trạm nhận thông tin phải thực hiện quá trình ngược lại, tức là biến đổi thông tin từ dạng không nhận thức được (dữ liệu đã được mã hóa) về dạng nhận thức được (dạng gốc), quá trình này được gọi là giải mã. Đây là một lớp bảo vệ thông tin rất quan trọng và được sử dụng rộng rãi trong môi trường mạng.

Để bảo vệ thông tin bằng mã hóa người ta thường tiếp cận theo hai hướng:

+ Theo đường truyền (Link_Oriented_Security).

+ Từ nút đến nút (End_to_End)

Theo cách thứ nhất, thông tin được mã hóa để bảo vệ trên đường truyền giữa hai nút mà không quan tâm đến nguồn và đích của thông tin đó. Ở đây ta lưu ý rằng thông tin chỉ được bảo vệ trên đường truyền, tức là ở mỗi nút đều có quá trình giải mã, sau đó mã hóa để truyền đi tiếp. Do đó các nút cần phải được bảo vệ tốt.

Theo cách thứ hai, thông tin trên mạng được bảo vệ trên toàn đường truyền từ nguồn tới đích. Thông tin sẽ được mã hóa ngay sau khi mới tạo ra và chỉ được giải mã khi về đến đích. Cách này mắc phải nhược điểm chỉ có dữ liệu của người dùng thì mới có thể mã hóa được, còn dữ liệu điều khiển thì giữ nguyên để có thể xử lí tại các nút.

1.2.6. Hệ mã hóa

1.2.6.1. Tổng quan về mã hóa dữ liệu

1/. Khái niệm mã hóa dữ liệu

Để đảm bảo An toàn thông tin lưu trữ trong máy tính hay đảm bảo An toàn thông tin trên đường truyền tin người ta phải "***Che giấu***" các thông tin này.

"***Che***" thông tin (dữ liệu) hay "***Mã hóa***" thông tin là ***thay đổi hình dạng*** thông tin gốc, và người khác ***khó*** nhận ra.

"***Giấu***" thông tin (dữ liệu) là ***cất giấu*** thông tin trong bản tin khác, và người khác cũng ***khó*** nhận ra.

Thuật toán mã hóa là thủ tục tính toán để thực hiện mã hóa hay giải mã.

Khóa mã hóa là một giá trị làm cho thuật toán mã hóa thực hiện một cách riêng biệt và sinh bản rõ riêng.Thông thường khóa càng lớn thì bản mã càng an toàn. Phạm vi các giá trị có thể có của khóa gọi là ***không gian khóa.***

Hệ mã hóa là tập các thuật toán, các khóa nhằm che giấu thông tin, cũng như làm rõ nó.

Việc mã hóa phải theo các quy tắc nhất định, quy tắc đó gọi là ***Hệ mã hóa.***

Hệ mã hóa được định nghĩa là bộ năm (P, C, K, E, D), trong đó:

P là tập hữu hạn các bản rõ có thể.

C là tập hữu hạn các bản mã có thể.

K là tập hữu hạn các khoá có thể.

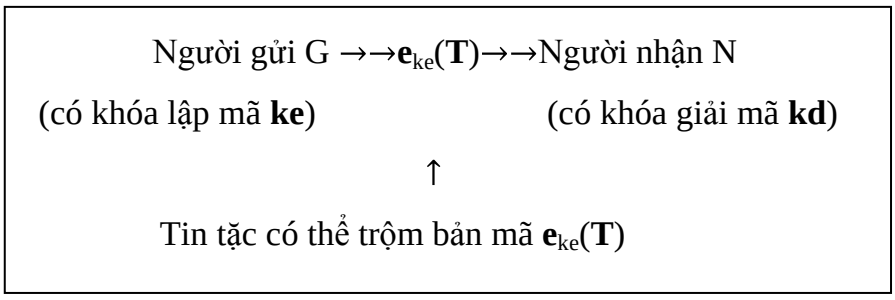
E là tập các hàm lập mã.

D là tập các hàm giải mã.

Với khóa lập mã $\mathbf{ke} \in \mathbf{K}$, có hàm lập mã $\mathbf{e}_{ke} \in \mathbf{E}$, $\mathbf{e}_{ke}$: $\mathbf{P} \rightarrow \mathbf{C}$,
Với khóa giải mã $\mathbf{kd} \in \mathbf{K}$, có hàm giải mã $\mathbf{d}_{kd} \in \mathbf{D}$, $\mathbf{d}_{kd}$: $\mathbf{C} \rightarrow P$,
Sao cho $\mathbf{d}_{kd}(\mathbf{e}_{ke}(x)) = \mathbf{x}, \quad \forall \mathbf{x} \in \mathbf{P}$.

Ở đây **x** được gọi là ***bản rõ***, $\mathbf{e}_{ke}(x)$ được gọi là ***bản mã***.

Mã hóa và giải mã



2/. Phân loại hệ mã hóa

Có nhiều cách để phân loại hệ mã hóa. Dựa vào tính chất "đối xứng" của khóa, có thể phân các hệ mã hóa thành hai loại:

- Hệ mã hóa khóa đối xứng (hay còn gọi là mã hóa khóa bí mật): là những hệ mã hóa dùng chung một khóa cả trong quá trình mã hóa dữ liệu và giải mã dữ liệu. Do đó khóa phải được giữ bí mật tuyệt đối.

- Hệ mã hóa khóa bất đối xứng (hay còn gọi là mã khóa công khai): Hệ mật này dùng một khóa để mã hóa, dùng một khóa khác để giải mã, nghĩa là khóa để mã hóa và giải mã là khác nhau. Các khóa này tạo nên từng cặp chuyển đổi ngược nhau và không có khóa nào có thể "dễ" suy được từ khóa kia. Khóa để mã hóa có thể công khai, nhưng khóa để giải mã phải giữ bí mật.

Ngoài ra nếu dựa vào thời gian đưa ra hệ mã hóa, ta còn có thể phân làm hai loại: Mã hóa cổ điển (là hệ mật mã ra đời trước năm 1970) và mã hóa hiện đại (ra đời sau năm 1970).

Còn nếu dựa vào cách thức tiến hành mã thì hệ mã hóa còn được chia làm hai loại là mã dòng (tiến hành mã từng khối dữ liệu, mỗi khối lại dựa vào các khóa khác nhau, các khóa này được sinh ra từ hàm sinh khóa, được gọi là dòng khóa) và mã khối (tiến hành mã từng khối dữ liệu với khóa như nhau).

1.2.6.2. Hệ mã hóa khóa công khai

1/. Hệ mã hóa RSA

Sơ đồ (Rivest, Shamir, Adleman đề xuất năm 1977)

* Tạo cặp khóa (bí mật, công khai) (a, b) :

Chọn bí mật số nguyên tố lớn p, q, tính n = p * q, công khai n, đặt P = C = Z_n

Tính bí mật Ø(**n**) = (**p-1**).(**q-1**).

Chọn khóa công khai b <Ø(n), nguyên tố cùng nhau với Ø(n).

Khóa bí mật a là phần tử nghịch đảo của b theo mod Ø(n): a*b ≡ 1(mod Ø(n)).

Tập cặp khóa (bí mật, công khai) K = {(a, b)/ a, b ∈Z_n, a*b ≡ 1(mod Ø(n)).

Với ***Bản rõ*** x ∈ P và ***Bản mã*** y ∈ C, định nghĩa:

Hàm Mã hoá: y = $\mathbf{e}_k(x) = x^b \bmod n$

Hàm Giải mã: x = $d_k(y) = y^a \bmod n$

Ví dụ:

Bản rõ chữ: R E N A I S S A N C E

* Sinh khóa:

Chọn bí mật số nguyên tố p= 53, q= 61, tính n = p * q = 3233, công khai n.

Đặt P = C = Z_n, tính bí mật Ø(n) = (p-1). (q-1) = 52 * 60 = 3120.

+ Chọn khóa công khai b là nguyên tố với Ø(n), tức là ƯCLN(b, Ø(n)) = 1.

Ví dụ chọn b = 71.

+ Khóa bí mật a là phần tử nghịch đảo của b theo mod Ø(n): a*b ≡1(mod Ø(n)).

Từ a*b ≡ 1 (mod Ø(n)), ta nhận được khóa bí mật a = 791.

* Bản rõ số:

R	E	N	A	I	S	S	A	N	C	E	(Dấu cách)
17	04	13	00	08	18	18	00	13	02	04	26
m_1		m_2		m_3		m_4		m_5		m_6	

* Theo phép lập mã: $\mathbf{c}_i = m_i^b \bmod n = m_i^{71} \bmod 3233$, ta nhận được:

* Bản mã số:

c_1	c_2	c_3	c_4	c_5	c_6
3106	0100	0931	2691	1984	2927

* Theo phép giải mã: $m_i = c_i^a \bmod n = c_i^{791} \bmod 3233$, ta nhận lại bản rõ.

Độ an toàn :

- Hệ mã hóa RSA là tất định, tức là với một bản rõ x và một khóa bí mật a, thì chỉ có một bản mã y.

- Hệ mật RSA an toàn, khi giữ được bí mật khoá giải mã a, p, q, $\phi(n)$.

Nếu biết được p và q, thì thám mã dễ dàng tính được $\phi(n) = (q-1)*(p-1)$.

Nếu biết được $\phi(n)$, thì thám mã sẽ tính được a theo thuật toán Euclide mở rộng.

Nhưng phân tích n thành tích của p và q là bài toán "khó".

Độ an toàn của Hệ mật RSA dựa vào khả năng giải bài toán phân tích số nguyên dương n thành tích của 2 số nguyên tố lớn p và q.

2/. Hệ mã hóa Elgamal

Sơ đồ:(Elgamal đề xuất năm 1985)

* ***Tạo cặp khóa (bí mật, công khai) (a,b):***

Chọn số nguyên tố **p** sao cho bài toán logarit rời rạc trong Z_p là "khó" giải.

Chọn phần tử nguyên thủy **g** $\in Z_p^*$. Tính khóa công khai $h \equiv g^a \bmod \mathbf{p}$.

Định nghĩa tập khóa: $K = \{(p, g, a, h): h \equiv g^a \bmod \mathbf{p}\}$.

Các giá trị p, g, h được công khai, phải giữ bí mật **a**.

Với *bản rõ* x ∈ P và *bản mã* y ∈ **C**, với khóa k ∈ K định nghĩa :

* ***Lập mã*** :

Chọn ngẫu nhiên bí mật $r \in Z_{p-1}$, bản mã là $y = e_k(x, r) = (y_1, y_2)$

Trong đó : $y_1 = g^r \bmod p$ và $y_2 = x * h^r \bmod p$

**** Giải mã*** :

$d_k (y_1, y_2) = y_2(y_1^a)^{-1} \bmod p$.

Ví dụ: Bản rõ x = 1299.

Chọn p = 2579, g = 2, a = 765. Tính khóa công khai $h = 2^{765} \bmod 2579 = 949$.

* ***Lập mã*** : Chọn ngẫu nhiên r = 853. Bản mã là y = (435, 2369),

Trong đó: $y_1 = 2^{852} \bmod 2579 = 435$ và $y_2 = 1299 * 949^{853} \bmod 2579 = 2396$

**** Giải mã :*** $x = y_2(y_1^a)^{-1} \bmod p = 2369 * (435^{765})^{-1} \bmod 2579 = 1299$.

Độ an toàn :

- Hệ mã hóa Elgamal là không tất định, tức là với một bản rõ **x** và 1 khóa bí mật **a**, thì có thể có nhiều hơn một bản mã y, vì trong công thức lập mã còn có thành phần
ngẫu nhiên r.

- Độ an toàn của Hệ mật mã Elgamal dựa vào khả năng giải bài toán logarit rời rạc trong Z_p. Theo giả thiết trong sơ đồ, thì bài toán này phải là "khó" giải.

Cụ thể là: Theo công thức lập mã : $y = e_k(x, r) = (y_1, y_2)$, trong đó $y_1 = g^r \bmod p$ và $y_2 = x * h^r \bmod p$. Như vậy muốn xác định bản rõ **x** từ công thức y_2, thám mã phải biết được **r**, Giá trị này có thể tính được từ công thức y_1, nhưng lại gặp bài toán logarit rời rạc.

1.2.6.3. Hệ mã hóa khóa đối xứng cổ điển

Khái niệm

- Hệ mã hóa khóa đối xứng đã được dùng từ rất sớm, nên còn được gọi là ***Hệ mã hóa đối xứng – cổ điển***. Bản mã hay bản rõ là dãy các ký tự Latin.

- ***Lập mã***: thực hiện theo các bước sau:

Bước 1: nhập bản rõ ký tự: RÕ_CHỮ.

Bước 2: chuyển RÕ_CHỮ ==> RÕ_SỐ.

Bước 3: chuyển RÕ_SỐ ==> MÃ_SỐ.

Bước 4: chuyển MÃ _SỐ ==> MÃ_CHỮ

- ***Giải mã***: thực hiện theo các bước sau:

Bước 1: nhập bản mã ký tự: MÃ_CHỮ.

Bước 2: chuyển MÃ_CHỮ ==> MÃ_SỐ

Bước 3: chuyển MÃ_SỐ ==> RÕ_SỐ.

Bước 4: chuyển RÕ_SỐ ==> RÕ_CHỮ

Các hệ mã hóa cổ điển

- Hệ mã hóa dịch chuyển: khóa có 1 "chìa".
- Hệ mã hóa Affine: khóa có 2 "chìa".
- Hệ mã hóa thay thế: khóa có 26 "chìa".
- Hệ mã hóa VIGENERE: khóa có m "chìa".
- Hệ mã hóa HILL: khóa có ma trận "chìa".

a. Hệ mã hóa dịch chuyển

Sơ đồ :

Đặt P = C = K = Z_{26}. Bản mã y và bản rõ x $\in Z_{26}$.

Với khóa k $\in$K, ta định nghĩa:

Hàm mã hóa: $y=e_k(x) = (x+k) \bmod 26$

Hàm giải mã: $x=d_k(y) = (y-k) \bmod 26$

Độ an toàn :

Độ an toàn của mã dịch chuyển là rất thấp.

Tập khóa K chỉ có 26 khóa, nên việc phá khóa có thể thực hiện dễ dàng bằng cách thử kiểm tra từng khóa: k=1,2,3, …,26.

b.Hệ mã hóa thay thế (Hoán vị toàn cục)

Sơ đồ :

Đặt P = C = Z_{26} . Bản mã y và bản rõ x $\in Z_{26}$.

Tập khóa K là tập mọi hoán vị trên Z_{26}.

Với khóa k = $\pi \in$ K, tức là 1 hoán vị trên Z_{26}, ta định nghĩa:

Mã hóa: $y=e_\pi(x)= \pi(x)$

Giải mã: $x=d_\pi(y)= \pi^{-1}(y)$

Độ an toàn:

Độ an toàn của mã thay thế thuộc loại cao

Tập khóa K có 26! Khóa ($>4.10^{26}$), nên việc phá khóa có thể thực hiện bằng cách duyệt tuần tự 26! Hoán vị của 26 chữ cái. Để kiểm tra tất cả 26! khóa, tốn rất nhiều thời gian.

Hiện nay với hệ mã này, người ta có phương pháp thám mã khác nhanh hơn.

c. Hệ mã hóa AFFINE

Sơ đồ :

Đặt P = C = Z_{26}. Bản mã y và bản rõ x ∈ Z_{26}.

Tập khóa K = {(a,b), với a,b ∈ Z_{26}, UCLN(a,26)=1}

Với khóa k=(a,b) ∈ K, ta định nghĩa:

Phép mã hóa : $y=e_k(x)= (ax + b) \bmod 26$

Phép giải mã : $x=d_k(y)= a^{-1}(y-b) \bmod 26$

Độ an toàn:

Độ an toàn của Hệ mã hóa Affine: Rất thấp

- Điều kiện UCLN(a,26)=1 để bảo đảm a có phần tử nghịch đảo $a^{-1} \bmod 26$, tức là thuật toán giải mã d_k luôn thực hiện được.

- Số lượng a ∈ Z_{26} nguyên tố với 26 là ∅(26)=12, đó là :

1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25

- Các số nghịch đảo theo (mod 26) tương ứng là:

1, 9, 21, 15, 3, 19, 7, 23, 11, 5, 17, 25

- Số lượng b ∈ Z_{26} là 26.

- Số các khóa (a,b) có thể là 12*26 = 312. Rất ít !

- Như vậy việc dò tìm khóa mật khá dễ dàng.

d. Hệ mã hóa VIGENERE

Sơ đồ:

Đặt P =C=K=$(Z_{26})^m$, m là số nguyên dương, các phép toán thực hiện trong (Z_{26}).

Bản mã Y và bản rõ X ∈ $(Z_{26})^m$. Khóa k = (k_1, k_2, …,k_m) gồm m phần tử.

Mã hóa Y = (y_1, y_2, …,y_m) = $e_k(x_1,x_2, …, x_m)= (x_1+ k1,x_2 + k_2,…, x_m+ k_m) \bmod 26$.

Giải mã X = (x_1,x_2,…, x_m) = $d_k(y_1,y_2, …,y_m) = (y_1- k_1,y_2 - k_2,…, y_m- k_m) \bmod 26$.

Độ an toàn:

Độ an toàn của mã VIGENERE là tương đối cao

Nếu khóa gồm m ký tự khác nhau, mỗi ký tự có thể được ánh xạ vào trong m ký tự có thể, do đó hệ mật mã này được gọi là thay thế đa biểu. Như vậy số khóa có thể có trong Vigenere là 26^m.

Nếu dùng phương pháp "tấn công vét cạn", thám mã phải kiểm tra 26^m khóa. Hiện nay với hệ mã này, người ta có phương pháp thám mã khác nhanh hơn.

e. Hệ mã hóa hoán vị cục bộ

Sơ đồ :

Đặt P = C = K = $(Z_{26})^m$, m là số nguyên dương. Bản mã Y và bản rõ X∈Z_{26}.

- Tập khóa K là tập tất cả các hoán vị của {1, 2, …, m}
- Với mỗi khóa k =π ∈ K, k = (k_1, k_2, …,k_m) gồm m phần tử, ta định nghĩa:

* Mã hóa Y = (y_1,y_2, …,y_m) = e_k(x_1,x_2,…, x_m) = ($x_{k(1)}$, $x_{k(2)}$, …, $x_{k(m)}$)

* Giải mã X = (x_1,x_2,…, x_m) = d_k(y_1,y_2, …,y_m) =($y_{k(1)}^{-1}$,$y_{k(2)}^{-1}$,…, $y_{k(m)}^{-1}$)

- Trong đó k^{-1} =π^{-1} là hoán vị ngược của π .

Độ an toàn :

- Nếu dùng phương pháp "tấn công vét cạn", thám mã phải kiểm tra số khóa có thể là: 1! + 2! + 3! + …+ m! trong đó m ≤ 26.
- Hiện nay với hệ mã này, người ta có phương pháp thám mã khác nhanh hơn.

f. Hệ mã hóa HILL

Sơ đồ :

Đặt P = C = $(Z_{26})^m$, m là số nguyên dương. Bản mã Y và bản rõ X ∈$(Z_{26})^m$.

Tập khóa K={ k ∈$(Z_{26})^{m*n}$/det(K,26)=1}. (K phải có K^{-1})

Mỗi khóa K là một "***chùm chìa khóa***" :

Với mỗi k ∈K, định nghĩa:

* Hàm lập mã: Y = (y_1,y_2, …,y_m) = e_k(x_1,x_2,…, x_m) = (x_1,x_2,…, x_m) * k

* Hàm giải mã: X = (x_1,x_2,…, x_m) = d_k(y_1,y_2, …,y_m) = (y_1,y_2, …,y_m) * k^{-1}

Độ an toàn:

Nếu dùng phương pháp "tấn công vét cạn", thám mã phải kiểm tra số khóa có thể với m lần lượt là 2, 3, 4, …, trong đó m lớn nhất là bằng độ dài bản rõ.

1.2.6.4. Hệ mã hóa khóa đối xứng DES

a. Hệ mã hóa khóa đối xứng DES

15/05/1973, Ủy ban tiêu chuẩn quốc gia Mỹ đã công bố một khuyến nghị về hệ mã hóa chuẩn.

- Hệ mã hóa phải có độ an toàn cao.
- Hệ mã hóa phải được định nghĩa đầy đủ và dễ hiểu.
- Độ an toàn của hệ mã hóa phải nằm ở khóa, không nằm ở thuật toán.
- Hệ mã hóa phải sẵn sàng cho mọi người dùng ở các lĩnh vực khác nhau.
- Hệ mã hóa phải xuất khẩu được.

DES được IBM phát triển, là một cải biên của hệ mật LUCIPHER DES, nó được công bố lần đầu tiên vào ngày 17/03/1975. Sau nhiều cuộc tranh luận công khai, cuối cùng DES được công nhận như một chuẩn liên bang vào ngày 23/11/1976 và được công bố vào ngày15/01/1977.

Năm 1980, "cách dùng DES" được công bố. Từ đó chu kỳ 5 năm DES được xem xét lại một lần bởi Ủy ban tiêu chuẩn quốc gia Mỹ.

Quy trình mã hóa theo DES :

Giai đoạn 1: Bản rõ chữ → Bản rõ số (Dạng nhị phân)

Chia thành

Giai đ oạn 2: Bản rõ số → Các đoạn 64 bit rõ số

Giai đoạn 3: 64 bit rõ số → 64 bit mã số

Kết nối

Giai đoạn 4: Các đoạn 64 bit mã số → Bản mã số (Dạng nhị phân)

Giai đoạn 5: Bản mã số → Bản mã chữ

b. Lập mã và giải mã

Lập mã DES :

Bản rõ là xâu x, bản mã là xâu y, khóa là xâu K, đều có độ dài 64 bit

Thuật toán mã hóa DES thực hiện qua 3 bước chính như sau:

Bước 1: Bản rõ x được hoán vị theo phép hoán vị IP, thành IP (x).

IP(x) = L_0R_0, trong đó L_0 là 32 bit đầu (Left), R_0 là 32 bit cuối (Right).

(IP(x) tách thành L_0R_0).

Bước 2 : Thực hiện 16 vòng mã hóa với những phép toán giống nhau

Dữ liệu được kết hợp với khóa thông qua hàm **f**:

$L_l = R_{l-1}$, $R_l = L_{l-1} \oplus f(R_{l-1},k_1)$ trong đó:

$\oplus$ là phép toán hoặc loại trừ của hai xâu bit (cộng theo modulo 2).

$k_1, k_2, \ldots, k_{16}$ là các khóa con (48 bit) được tính từ khóa gốc K.

Bước 3: Thực hiện phép hoán vị ngược IP^{-1}cho xâu $L_{16}R_{16}$, thu được bản mã y.

$y = IP^{-1}(L_{16}, R_{16})$

Quy trình giải mã :

Quy trình giải mã của DES tương tự như quy trình lập mã, nhưng theo dùng các khóa thứ tự ngược lại: k_{16},k_{15}, …, k_1.

Xuất phát (đầu vào) từ bản mã y, kết quả (đầu ra) là bản rõ x.

c. Độ an toàn của hệ mã hóa DES

- Độ an toàn của hệ mã hóa DES có liên quan đến các bảng S_j :

Ngoại trừ các bảng S, mọi tính toán trong DES đều tuyến tính, tức là việc tính phép hoặc loại trừ của hai đầu ra cũng giống như phép hoặc loại trừ của hai đầu vào, rồi tính toán đầu ra.

Các bảng S chứa đựng nhiều thành phần phi tuyến của hệ mật, là yếu tố quan trọng nhất đối với độ mật của hệ thống.

Khi mới xây dựng hệ mật DES, thì tiêu chuẩn xây dựng các hộp S không được biết đầy đủ. Và có thể các hộp S này có thể chứa các "cửa sập" được giấu kín. Và đó cũng là một điểm đảm bảo tính bảo mật của hệ DES

- Hạn chế của DES chính là kích thước không gian khóa:

Số khóa có thể là 2^{56}, không gian này là nhỏ để đảm bảo an toàn thực sự. Nhiều thiết bị chuyên dụng đã được đề xuất nhằm phục vụ cho phép tấn công với bản rõ đã biết. Phép tấn công này chủ yếu thực hiện theo phương pháp "vét cạn".

Tức là với bản rõ x và bản mã y tương ứng (64 bit), mỗi khóa có thể đều được kiểm tra cho tới khi tìm được một khóa K thỏa mãn $e_K(x) = y$.

1.2.7. Chữ ký số

1.2.7.1. Giới thiệu

Để chứng thực nguồn gốc hay hiệu lực của một tài liệu (ví dụ: đơn xin nhập học, giấy báo nhập học,…) lâu nay người ta dùng chữ ký "tay", ghi vào phía dưới của mỗi tài liệu. Như vậy người ký phải trực tiếp "ký tay" vào tài liệu.

Ngày nay các tài liệu được số hóa, người ta cũng có nhu cầu chứng thực nguồn gốc tài liệu. Rõ ràng không thể "ký tay" vào tài liệu vì chúng không được in ấn trên giấy. Tài liệu "số" là một xâu các bit (0 hay 1), xâu bít có thể rất dài, "Chữ ký" để chứng thực một xâu bít tài liệu cũng không thể là một xâu bit nhỏ đặt phía dưới xâu bit tài liệu. Một "Chữ ký" như vậy chắc chắn sẽ bị kẻ gian sao chép để đặt dưới một tài liệu khác một cách bất hợp pháp.

Những năm 80 của thế kỷ 20, các nhà khoa học đã phát minh ra "chữ ký số" để chứng thực một "tài liệu số" . Đó chính là bản mã của xâu bit tài liệu.

Người ta tạo ra "chữ ký số" trên "tài liệu số" giống như tạo ra "bản mã" của tài liệu với "khóa lập mã".

Như vậy "ký số" trên "tài liệu số" là "ký" trên từng bit tài liệu. Kẻ gian khó có thể giả mạo "chữ ký số" nếu nó không biết "khóa lập mã".

Để kiểm tra một "chữ ký số" thuộc về một "tài liệu số", người ta giải mã "chữ ký số" bằng "khóa giải mã", và so sánh với tài liệu gốc.

Ngoài ý nghĩa để chứng thực nguồn gốc hay hiêu lực của các tài liệu số hóa, Mặt mạnh của "Chữ ký số" hơn "Chữ ký tay" là ở chỗ người ta có thể "ký" vào tài liệu từ rất xa trên mạng công khai. Hơn thế nữa, có thể "ký" bằng các thiết bị cầm tay như Điện thoại di động, laptop,… tại khắp mọi nơi miễn là kết nối được vào mạng. Đỡ tốn thời gian, công sức, chi phí…

"Ký số" thực hiện trên từng bit tài liệu, nên độ dài của "chữ ký số" ít nhất cũng bằng độ dài của tài liệu. Do đó thay vì ký trên tài liệu dài, người ta thường dùng "hàm băm" để tạo "đại diện" cho tài liệu, sau đó mới "ký số" lên "đại diện" này.

Sơ đồ chữ ký số :

Một sơ đồ chữ ký số thường bao gồm hai thành phần chủ chốt là thuật toán ký và thuật toán xác minh.

Một sơ đồ chữ ký số là một bộ 5 (P, A, K, S, V) thỏa mãn các điều kiện sau :

P là một tập hợp các bản rõ có thể.

A là tập hữu hạn các chữ ký có thể.

K là tập hữu hạn các khóa có thể.

S là tập các thuật toán ký.

V là tập các thuật toán xác minh.

Với mỗi k ∈ K, tồn tại một thuật toán ký $Sig_k \in S$, Sig_k: P → A,

có thuật toán kiểm tra chữ ký $Ver_k \in V$, Ver_k : P x A → {đúng, sai},

thỏa mãn điều kiện sau với mọi x ∈ P, y ∈ A :

$Ver_k(x, y)$ = Đúng, nếu y = Sig_k (x) hoặc Sai, nếu y ≠ Sig_k (x).

Chú ý:

Người ta thường dùng hệ mã hóa khóa công khai để lập: "Sơ đồ chữ ký số".

Ở đây khóa bí mật a dùng làm khóa "ký", khóa công khai b dùng làm khóa kiểm tra "chữ ký".

Ngược lại với việc mã hóa, dùng khóa công khai b để lập mã, dùng khóa bí mật a để giải mã.

Điều này là hoàn toàn tự nhiên, vì "ký" cần giữ bí mật nên phải dùng khóa bí mật a để "ký". Còn "chữ ký" là công khai cho mọi người biết, nên họ dùng khóa công khai b để kiểm tra.

1.2.7.2. Phân loại chữ ký số

Có nhiều loại chữ ký tùy theo cách phân loại, sau đây xin giới thiệu một số cách.

Cách 1: Phân loại chữ ký theo khả năng khôi phục thông điệp gốc

1). Chữ ký có thể khôi phục thông điệp gốc:

Là loại chữ ký, trong đó người gửi chỉ cần gửi "chữ ký", người nhận có thể khôi phục lại được thông điệp gốc, đã được "ký" bởi "chữ ký" này.

2). Chữ ký không thể khôi phục thông điệp gốc:

Ví dụ: Chữ ký Elgamal là chữ ký đi kèm thông điệp.

Cách 2: Phân loại chữ ký theo mức an toàn.

1). Chữ ký "không thể phủ nhận":

Nhằm tránh việc nhân bản chữ ký để sử dụng nhiều lần, tốt nhất là người gửi tham gia trực tiếp vào việc kiểm thử chữ ký. Điều đó được thực hiện bằng một giao thức kiểm thử, dưới dạng một giao thức mời hỏi và trả lời.

Ví dụ: Chữ ký không phủ định (Chaum-van Antverpen).

2). Chữ ký "một lần":

Chữ ký dùng một lần (one-time signature) là một khái niệm vẫn còn khá mới mẻ song rất quan trọng, đặc biệt là trong một số mô hình về bỏ phiếu điện tử và tiền điện tử.

Để đảm bảo an toàn, "khóa ký" chỉ dùng 1 lần (one-time) trên 1 tài liệu.

Ví dụ: Chữ ký một lần Lamport. Chữ ký Fail-Stop (Van Heyst & Pedersen).

Cách 3: Phân loại chữ ký theo ứng dụng đặc trưng.

Chữ ký "mù" (Blind Signature).

Chữ ký "nhóm" (Group Signature).

Chữ ký "bội" (Multy Signature).

Chữ ký "mù nhóm" (Blind Group Signature).

Chữ ký "mù bội" (Blind Multy Signature).

1.2.7.3. Một số loại chữ ký số

1/. Chữ ký RSA

Sơ đồ : (đề xuất năm 1978)

1) *Tạo cặp khóa (bí mật, công khai) (a,b):*

Chọn bí mật nguyên tố lớn p, q, tính n=p*q, công khai n đặt $P=C=Z_n^*$

Tính bí mật $\emptyset(n)$ = (q-1)(p-1).

Chọn khóa công khai b <$\emptyset(n)$, nguyên tố cùng nhau với $\emptyset(n)$.

Khóa bí mật a là phần tử nghịch đảo của b theo mod $\emptyset(n)$: a*b=1(mod $\emptyset(n)$).

2) Ký số:

Chữ ký trên x ∈P là $y = Sig_k(x) = x^a \pmod n$, y ∈ A (R1).

3) Kiểm tra chữ ký:

$Ver_k(x,y)$ = đúng ⇔ $x= y^b \pmod n$ (R2).

Chú ý: Với một số chữ ký:

Việc "ký số" vào x tương ứng với việc "mã hóa" tài liệu x.

Kiểm thử chính là việc giải mã "chữ ký", để kiểm tra xem tài liệu đã giải mã có đúng với tài liệu trước khi ký hay không. Thuật toán và kiểm thử "chữ ký" là công khai, ai cũng có thể kiểm thử chữ ký được.

Ví dụ: chữ ký trên x = 2

Tạo cặp khóa (bí mật, công khai) (a,b):

Chọn bí mật số nguyên tố p=3, q=5, tính n=p*q=3*5=15, công khai n.

Đặt P=C=Z_n^*. Tính bí mật $\emptyset(n)$ = (q-1)(p-1)= (3-1)(5-1) =8

Chọn khóa công khai b= 3< $\emptyset(n)$, nguyên tố cùng nhau với $\emptyset(n)$ =8.

Khóa bí mật a =3, là phần tử nghịch đảo của b theo mod $\emptyset\ (n)$: a*b=1(mod $\emptyset(n)$)

Ký số: chữ ký trên x=2 $\in$ P là

$y = Sig_k(x) = x^a \pmod n = 2^3 \pmod{15} = 8$, y $\in$ A.

Kiểm tra chữ ký :

$Ver_k(x,y)$ = đúng $\Leftrightarrow x = y^b \pmod n \Leftrightarrow 2 = 8^b \pmod{15}$

2/. Chữ ký Elgamal

Sơ đồ : (Elgamal đề xuất năm 1985)

Tạo cặp khóa (bí mật, công khai) (a, h):

Chọn số nguyên tố **p** sao cho bài toán logarit rời rạc trong Z_p là "khó" giải.

Chọn phần tử nguyên thủy $g \in Z_p^*$. Đặt $P = Z_p^*$, $A = Z_p^* \times Z_{p-1}$.

Chọn khóa bí mật là $a \in Z_p^*$. Tính khóa công khai $h \equiv g^a \bmod \mathbf{p}$.

Định nghĩa tập khóa : $K = \{(p, g, a, h): h \equiv g^a \bmod \mathbf{p}\}$.

Các giá trị p, g, h được công khai, phải giữ bí mật a.

* ***Ký số***:

Dùng 2 khóa ký: khóa **a** và khóa ngẫu nhiên bí mật $r \in Z_{p-1}^*$.

(Vì $r \in Z_{p-1}^*$, nên nguyên tố cùng p-1, do đó tồn tại $r^{-1} \bmod (p-1)$).

Chữ ký trên $x \in P$ là $y = Sig_k(x, r) = (\gamma, \delta)$, $y \in A$ (E1)

Trong đó $\gamma \in Z_p^*$, $\delta \in Z_{p-1}$:

$\gamma = g^r \bmod \mathbf{p}$ và $\delta = (x - a * \gamma) * r^{-1} \bmod (p-1)$

**** Kiểm tra chữ ký :***

$Ver_k(x, \gamma, \delta) =$ đúng $\leftrightarrow h^{\gamma} * \gamma^{\delta} \equiv g^x \bmod p$. (E2)

Chú ý: Nếu chữ ký được tính đúng, kiểm thử sẽ thành công vì

$h^{\gamma} * \gamma^{\delta} \equiv g^{a\gamma} * g^{r*\delta} \bmod p \equiv g^{(a\gamma + r*\delta)} \bmod p \equiv g^x \bmod p$.

Do $\delta = (x - a * \gamma) * r^{-1} \bmod (p - 1)$ nên $(a * \gamma + r * \delta) \equiv x \bmod (p-1)$

3/. Chữ ký Schnoor

**** Sinh khóa***:

Cho $\mathbf{Z}_n^*$, **q** là số nguyên tố, cho **G** là nhóm con cấp **q** của $\mathbf{Z}_n^*$.

Chọn phần tử sinh $\mathbf{g} \in \mathbf{G}$, sao cho bài toán logarit rời rạc trên **G** là "khó giải".

Chọn hàm băm H: $\{0, 1\}^* \rightarrow \mathbf{Z}_q$.

Chọn khóa bí mật là $a \in \mathbf{Z}_n^*$, khóa công khai là $\mathbf{h} = \mathbf{g}^a \bmod n$.

**** Ký số***:

Chữ ký Schnorr trên $\mathbf{m} \in \{0, 1\}^*$ được định nghĩa là cặp (**c**, **s**), nếu thỏa mãn điều kiện $c = H(\mathbf{m}, \mathbf{g}^s\mathbf{h}^c)$.

Chú ý: Ký hiệu $(\mathbf{m}, \mathbf{g}^s\mathbf{h}^c)$ là phép "ghép nối" **m** và $\mathbf{g}^s\mathbf{h}^c$.

Ví dụ: $\mathbf{m} = 0110$, $\mathbf{g}^s\mathbf{h}^c = 01010$, thì $(\mathbf{m}, \mathbf{g}^s\mathbf{h}^c) = 011001010$.

Tạo chữ ký Schnorr: Chữ ký là cặp (**c**, **s**).

+ Chọn ngẫu nhiên $\mathbf{r} \in \mathbf{Z}_q^*$. Tính $\mathbf{c} = H(\mathbf{m}, \mathbf{g}^r)$, $\mathbf{s} = \mathbf{r} - \mathbf{ca} \pmod{\mathbf{q}}$.

**** Kiểm tra chữ ký:***

Cặp (**c**, **s**) là chữ ký Schnorr, vì thỏa mãn điều kiện$c = H(\mathbf{m}, \mathbf{g}^s\mathbf{h}^c)$.

Vì $\mathbf{g}^s\mathbf{h}^c = \mathbf{g}^{r - ca}(\mathbf{g}^a)^c = \mathbf{g}^r \pmod n$, do đó $H(\mathbf{m}, \mathbf{g}^s\mathbf{h}^c) = H(\mathbf{m}, \mathbf{g}^r) = c$.

1.3. TỔNG QUAN VỀ MẠNG RIÊNG ẢO

1.3.1. Khái niệm mạng riêng ảo

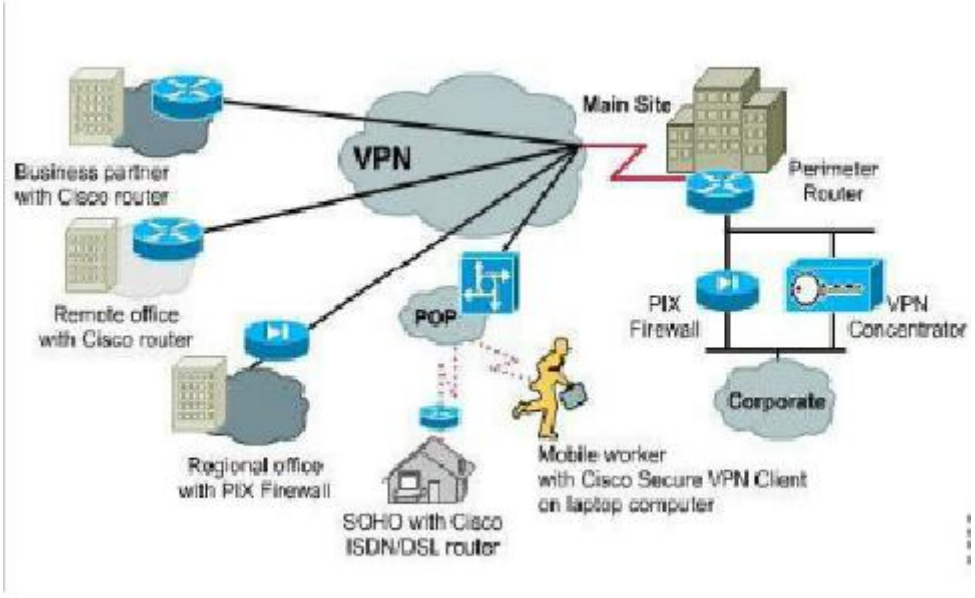
Mạng riêng ảo (Virtual Private Network: VPN). Có nhiều định nghĩa khác nhau về Mạng riêng ảo:

- Theo VPN Consortium, VPN là mạng sử dụng mạng công cộng (như Internet, ATM/Frame Relay của các nhà cung cấp dịch vụ) làm cơ sở hạ tầng để truyền thông tin, nhưng vẫn đảm bảo là một mạng riêng và kiểm soát được truy nhập. Nói cách khác, VPN được định nghĩa là liên kết của khách hàng được triển khai trên một hạ tầng công cộng với các chính sách như trong một mạng riêng. Hạ tầng công cộng này có thể là mạng IP, Frame Relay, ATM hay Internet.
- Theo tài liệu của IBM, VPN là sự mở rộng một mạng Internet riêng của một doanh nghiệp qua một mạng công cộng như Internet, tạo ra một kết nối an toàn, thực chất là qua một đường hầm riêng. VPN truyền thông tin một cách an toàn qua Internet kết nối người dùng từ xa, nhánh văn phòng và các đối tác thương mại thành mạng công ty mở rộng.
- Theo cách nói đơn giản, VPN là sự mở rộng của mạng Intranet qua một mạng công cộng (như Internet) mà đảm bảo sự bảo mật và hiệu quả kết nối giữa hai điểm truyền thông cuối. Mạng Intranet riêng được mở rộng nhờ sự trợ giúp của các "đường hầm". Các đường hầm này cho phép các thực thể cuối trao đổi dữ liệu theo cách tương tự như truyền thông điểm – điểm.

Mạng riêng ảo đã thực sự chinh phục cuộc sống. Việc kết nối các mạng máy tính của các doanh nghiệp lâu nay vẫn được thực hiện trên các đường truyền thuê riêng, cũng có thể là kết nối Frame Relay hay ATM. Nhưng rào cản lớn nhất với các doanh nghiệp, tổ chức đó là chi phí. Chi phí từ nhà cung cấp dịch vụ, chi phí từ việc duy trì, vận hành hạ tầng mạng, thiết bị riêng của doanh nghiệp…rất lớn. Vì vậy, điều dễ hiểu là trong thời gian dài, chúng ta gần như không thấy được nhiều ứng dụng, giải pháp hữu ích trên mạng diện rộng WAN.

Rõ ràng, sự ra đời của công nghệ mạng riêng ảo đã cho phép các tổ chức, doanh nghiệp có thêm sự lựa chọn mới. Không phải vô cớ mà các chuyên gia viễn thông nhận định: "Mạng riêng ảo chính là công nghệ mạng WAN thế hệ mới".

Ví dụ về mô hình kết nối mạng riêng ảo:



Hình 1 Mô hình Mạng riêng ảo

Về căn bản, mỗi VPN là một mạng riêng rẽ sử dụng một mạng chung (Internet) để kết nối cùng với các site (các mạng riêng lẻ) hay nhiều người dùng từ xa. Thay cho việc sử dụng kết nối thực, chuyên dùng như đường leased- line, mỗi VPN sử dụng các kết nối ảo được dẫn qua đường Internet từ mạng riêng của các công ty tới các site hay các nhân viên từ xa. Để có thể gửi và nhận dữ liệu thông qua mạng công cộng, mà vẫn bảo đảm tính an toàn và bảo mật, VPN cung cấp các cơ chế mã hóa dữ liệu trên đường truyền tạo ra một đường ống bảo mật giữa nơi nhận và nơi gửi (Tunnel), giống như một kết nối point- to- point trên mạng riêng. Để có thể tạo ra đường ống bảo mật đó, dữ liệu phải được mã hóa hay che giấu đi, chỉ cung cấp phần đầu gói dữ liệu (header) là thông tin về đường đi cho phép nó có thể đi đến đích thông qua mạng công cộng một cách nhanh chóng.

Dữ liệu được mã hóa một cách cẩn thận, do đó nếu các packet bị bắt lại trên đường truyền công cộng, cũng không thể đọc được nội dung vì không có khóa giải mã.

1.3.2. Mục đích

Đáp ứng nhu cầu khai thác dữ liệu, dịch vụ CSDL, dịch vụ được cung cấp trong mạng nội bộ của công ty để đáp ứng cho các công việc, hoạt động sản xuất kinh doanh của từng doanh nghiệp ở bất cứ nơi đâu mà không cần ngồi trong văn phòng.

Áp dụng cho các tổ chức có nhiều văn phòng chi nhánh, giữa các văn phòng cần trao đổi dữ liệu với nhau. Ví dụ: một công ty đa quốc gia có nhu cầu chia sẻ thông tin giữa các chi nhánh đặt tại nhiều nước khác nhau, có thể xây dựng một hệ thống VPN Site-to-Site kết nối hai văn phòng tạo một đường truyền riêng trên mạng Internet phục vụ quá trình truyền thông an toàn hiệu quả.

Trong một số tổ chức, quá trình truyền dữ liệu giữa một số bộ phận cần đảm bảo tính riêng tư, không cho phép các bộ phận khác truy cập. Hệ thống Intranet VPN có thể đáp ứng tình huống này.

Quản lý văn phòng một cách hiệu quả, giám sát công việc từ xa.

Tích hợp các hệ thống công nghệ cao như Camera quan sát, điện thoại trên nền tảng Internet, voice chat…

Đẩy mạnh hiệu quả kinh doanh, bộ phận quản lý muốn các nhân viên kinh doanh trong quá trình công tác ở bên ngoài có thể truy cập báo cáo bán hàng (Sale Reports) chia sẻ trên File Server và có thể tương tác với máy tính của họ trong văn phòng khi cần thiết. Ngoài ra đối với các dữ liệu mật, nhạy cảm như báo cáo doanh số, trong quá trình truyền có thể áp dụng cơ chế mã hóa chặt chẽ để nâng cao độ an toàn của dữ liệu.

1.3.3. Chức năng

VPN cung cấp ba chức năng chính đó là: tính xác thực (Authentication), tính toàn vẹn (Integrity) và tính bảo mật (Confidentiality).

a) ***Tính xác thực*** : Để thiết lập một kết nối VPN thì trước hết cả hai phía phải xác thực lẫn nhau để khẳng định rằng mình đang trao đổi thông tin với người mình mong muốn chứ không phải là một người khác.

b) ***Tính toàn vẹn*** : Đảm bảo dữ liệu không bị thay đổi hay đảm bảo không có bất kỳ sự xáo trộn nào trong quá trình truyền dẫn.

c) ***Tính bảo mật*** : Người gửi có thể mã hoá các gói dữ liệu trước khi truyền qua mạng công cộng và dữ liệu sẽ được giải mã ở phía thu. Bằng cách làm như vậy, không một ai có thể truy nhập thông tin mà không được phép. Thậm chí nếu có lấy được thì cũng không đọc được.

1.3.4. Lợi ích của công nghệ VPN

VPN mang lại lợi ích thực sự và tức thời cho các công ty. Có thể dùng VPN không chỉ để đơn giản hoá việc thông tin giữa các nhân viên làm việc ở xa, người dùng lưu động, mở rộng Intranet đến từng văn phòng, chi nhánh, thậm chí triển khai Extranet đến tận khách hàng và các đối tác chủ chốt mà còn làm giảm chi phí cho công việc trên thấp hơn nhiều so với việc mua thiết bị và đường dây cho mạng WAN riêng. Những lợi ích này dù trực tiếp hay gián tiếp đều bao gồm: Tiết kiệm chi phí (cost saving), tính mềm dẻo (flexibility), khả năng mở rộng (scalability) và một số ưu điểm khác.

a) Tiết kiệm chi phí

Việc sử dụng một VPN sẽ giúp các công ty giảm được chi phí đầu tư và chi phí thường xuyên.

Tổng giá thành của việc sở hữu một mạng VPN sẽ được thu nhỏ, do chỉ phải trả ít hơn cho việc thuê băng thông đường truyền, các thiết bị mạng đường trục và duy trì hoạt động của hệ thống. Giá thành cho việc kết nối LAN-to-LAN giảm từ 20% tới 30% so với việc sử dụng đường thuê riêng truyền thống. Còn đối với việc truy cập từ xa giảm từ 60% tới 80%.

b) Tính linh hoạt

Tính linh hoạt ở đây không chỉ là linh hoạt trong quá trình vận hành và khai thác mà nó còn thực sự mềm dẻo đối với yêu cầu sử dụng. Khách hàng có thể sử dụng kết nối T1, T3 giữa các văn phòng và nhiều kiểu kết nối khác cũng có thể được sử dụng để kết nối các văn phòng nhỏ, các đối tượng di động.

c) Khả năng mở rộng

Do VPN được xây dựng dựa trên cơ sở hạ tầng mạng công cộng (Internet), bất cứ ở nơi nào có mạng công cộng là đều có thể triển khai VPN. Mà mạng công cộng có mặt ở khắp mọi nơi nên khả năng mở rộng của VPN là rất linh động.

Một cơ quan ở xa có thể kết nối một cách dễ dàng đến mạng của công ty bằng cách sử dụng đường dây điện thoại hay DSL…Và mạng VPN dễ dàng gỡ bỏ khi có nhu cầu.

Khả năng mở rộng băng thông là khi một văn phòng, chi nhánh yêu cầu băng thông lớn hơn thì nó có thể được nâng cấp dễ dàng.

d) Giảm thiểu các hỗ trợ kỹ thuật

Việc chuẩn hoá trên một kiểu kết nối từ đối tượng di động đến ISP và việc chuẩn hoá các yêu cầu về bảo mật đã làm giảm thiểu nhu cầu về nguồn hỗ trợ kỹ thuật cho mạng VPN. Và ngày nay, khi mà các nhà cung cấp dịch vụ đảm nhiệm các nhiệm vụ hỗ trợ mạng nhiều hơn thì những yêu cầu hỗ trợ kỹ thuật đối với người sử dụng ngày càng giảm.

e) Đáp ứng các nhu cầu thương mại

Các sản phẩm dịch vụ VPN tuân theo chuẩn chung hiện nay, một phần để đảm bảo khả năng làm việc của sản phẩm, nhưng có lẽ quan trọng hơn là để sản phẩm của nhiều nhà cung cấp khác nhau có thể làm việc với nhau.

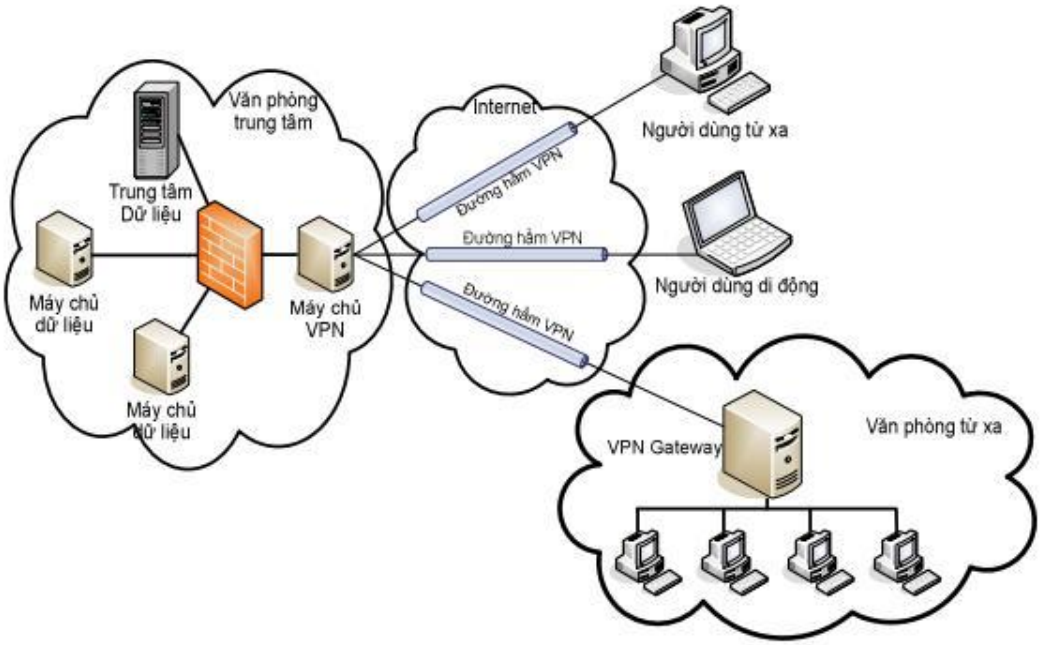
Đối với các thiết bị và Công nghệ Viễn thông mới thì vấn đề cần quan tâm là chuẩn hoá, khả năng quản trị, khả năng mở rộng, khả năng tích hợp mạng, tính kế thừa, độ tin cậy và hiệu suất hoạt động, đặc biệt là khả năng thương mại của sản phẩm.

1.3.5. Các dạng kết nối mạng riêng ảo

1.3.5.1. VPN truy nhập từ xa (Remote Access VPNs)

VPN truy nhập từ xa cung cấp cho các nhân viên, chi nhánh văn phòng di động có khả năng trao đổi, truy nhập từ xa vào mạng của công ty tại mọi thời điểm tại bất cứ đâu có mạng Internet.

VPN truy nhập từ xa cho phép mở rộng mạng công ty tới những người sử dụng thông qua cơ sở hạ tầng chia sẻ chung, trong khi những chính sách mạng công ty vẫn duy trì. Loại VPN này có thể dùng để cung cấp truy nhập an toàn cho các thiết bị di động, những người sử dụng di động, các chi nhánh và những bạn hàng của công ty. Những kiểu VPN này được thực hiện thông qua cơ sở hạ tầng công cộng bằng cách sử dụng công nghệ ISDN, quay số, IP di động, DSL và công nghệ cáp và thường yêu cầu một vài kiểu phần mềm client chạy trên máy tính của người sử dụng.



Hình 2 Remote Access VPN

VPN truy nhập từ xa có các ưu điểm sau:

- Loại bỏ chi phí cho kết nối khoảng cách xa từ người sử dụng đến mạng của tổ chức bởi vì tất cả kết nối xa bây giờ được thay thế bằng kết nối Internet
- Khoảng cách kết nối rộng và chi phí giảm xuống do người sử dụng IP-VPN chỉ cần quay số tới số của nhà cung cấp dịch vụ Internet ISP hoặc trực tiếp kết nối qua mạng băng rộng luôn hiện hành.
- Bởi vì các kết nối truy nhập là nội bộ nên các Modem kết nối hoạt động ở tốc độ cao hơn so với các truy nhập khoảng cách xa.
- Cung cấp dịch vụ kết nối giá rẻ cho những người sử dụng ở xa.
- Triển khai thêm người sử dụng đơn giản và sự tăng lên nhanh chóng của VPN cho phép thêm vào người dùng mới mà không tăng chi phí cho cơ sở hạ tầng.
- Vấn đề quản lí và bảo dưỡng mạng quay số đơn giản khi thêm người sử dụng mới sẽ giúp các công ty có thể dễ dàng chuyển hướng kinh doanh hơn.
- VPN cung cấp khả năng truy nhập tốt hơn đến các site của công ty bởi vì chúng hỗ trợ mức thấp nhất của dịch vụ kết nối.

Tuy nhiên bên cạnh đó VPN truy cập từ xa cũng có một số hạn chế cần khắc phục sau:

- Mạng VPN truy nhập từ xa không hỗ trợ các dịch vụ đảm bảo QoS.
- Nguy cơ bị mất dữ liệu cao. Hơn nữa, nguy cơ các gói có thể bị phân phát không đến nơi hoặc mất gói.
- Bởi vì thuật toán mã hoá phức tạp, nên tiêu đề giao thức tăng một cách đáng kể.

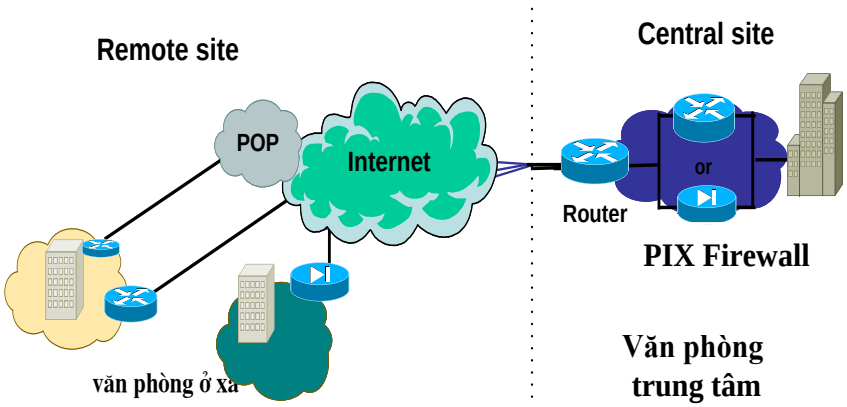
1.3.5.2. Site – To – Site VPN

Site-to-Site VPN được sử dụng để nối các site của các hãng phân tán về mặt địa lý, trong đó mỗi site có các địa chỉ mạng riêng được quản lý sao cho bình thường không xảy ra va chạm.

1/. **Intranet VPN (Mạng VPN cục bộ)**

Các VPN cục bộ được sử dụng để bảo mật các kết nối giữa các địa điểm khác nhau của một công ty. Mạng VPN liên kết trụ sở chính, các văn phòng, chi nhánh trên một cơ sở hạ tầng chung sử dụng các kết nối luôn được mã hoá bảo mật. Điều này cho phép tất cả các địa điểm có thể truy nhập an toàn các nguồn dữ liệu được phép trong toàn bộ mạng của công ty.

Những VPN này vẫn cung cấp những đặc tính của mạng WAN như khả năng mở rộng, tính tin cậy và hỗ trợ cho nhiều kiểu giao thức khác nhau với chi phí thấp nhưng vẫn đảm bảo tính mềm dẻo. Kiểu VPN này thường được cấu hình như là một VPN Site- to- Site.



Hình 3 Intranet VPN

Những ưu điểm chính của mạng cục bộ dựa trên giải pháp VPN bao gồm:

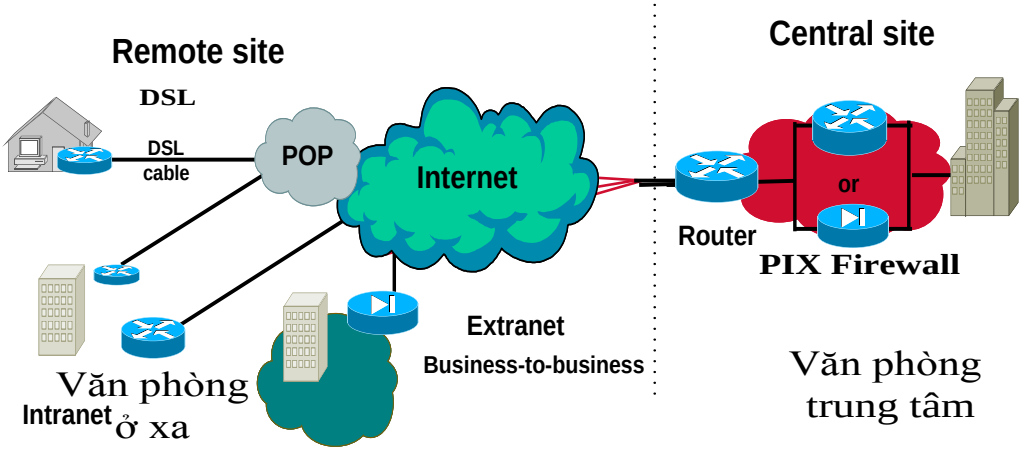
- Các mạng lưới cục bộ hay toàn bộ có thể được thiết lập (với điều kiện mạng thông qua một hay nhiều nhà cung cấp dịch vụ).
- Giảm được số nhân viên kỹ thuật hỗ trợ trên mạng đối với những nơi xa.
- Bởi vì những kết nối trung gian được thực hiện thông qua mạng Internet, nên nó có thể dễ dàng thiết lập thêm một liên kết ngang cấp mới.
- Tiết kiệm chi phí thu được từ những lợi ích đạt được bằng cách sử dụng đường ngầm VPN thông qua Internet kết hợp với công nghệ chuyển mạch tốc độ cao. Ví dụ: như công nghệ Frame Relay, ATM.

Tuy nhiên nó cũng mang một số nhược điểm cần khắc phục sau:

- Bởi vì dữ liệu được truyền "ngầm" qua mạng công cộng – mạng Internet – cho nên vẫn còn những mối "đe dọa" về mức độ bảo mật dữ liệu và mức độ chất lượng dịch vụ (QoS).
- Khả năng các gói dữ liệu bị mất trong khi truyền dẫn vẫn còn khá cao.
- Trường hợp truyền dẫn khối lượng lớn dữ liệu, như là đa phương tiện, với yêu cầu truyền dẫn tốc độ cao và đảm bảo thời gian thực là thách thức lớn trong môi trường Internet.

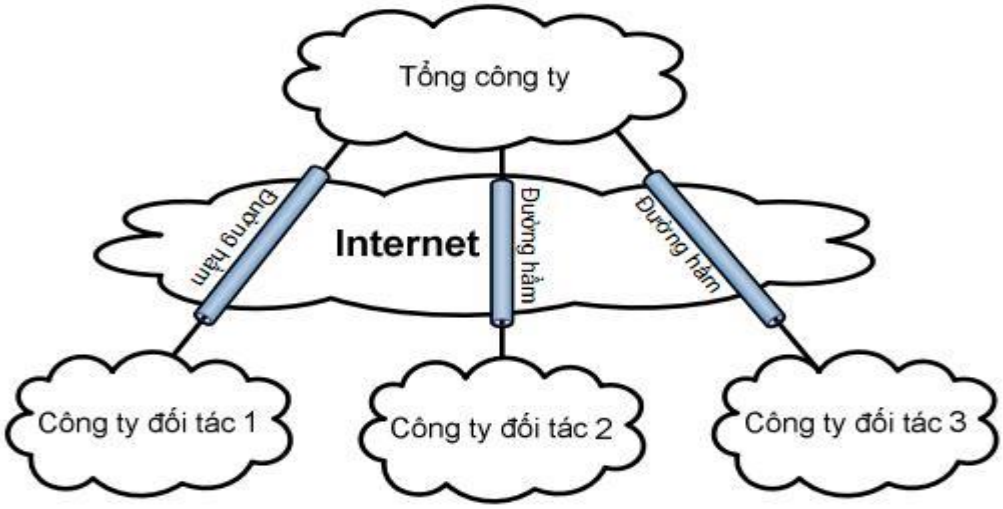
2/. **Extranet VPNs (VPN mở rộng)**

Không giống như mạng VPN cục bộ và mạng VPN truy nhập từ xa, mạng VPN mở rộng không bị cô lập với "thế giới bên ngoài". Thực tế mạng VPN mở rộng cung cấp khả năng điều khiển truy nhập tới những nguồn tài nguyên mạng cần thiết để mở rộng những đối tượng kinh doanh như là các đối tác, khách hàng, và các nhà cung cấp…



Hình 4 Extranet VPN

Các VPN mở rộng cung cấp một đường hầm bảo mật giữa các khách hàng, các nhà cung cấp và các đối tác qua một cơ sở hạ tầng công cộng. Kiểu VPN này sử dụng các kết nối luôn luôn được bảo mật và được cấu hình như một VPN Site–to–Site. Sự khác nhau giữa một VPN cục bộ và một VPN mở rộng đó là sự truy cập mạng được công nhận ở một trong hai đầu cuối của VPN.



Hình 5 Đường hầm bảo mật trong Extranet VPN

Mạng VPN mở rộng có những ưu điểm cơ bản sau:

- Chi phí cho mạng VPN mở rộng thấp hơn rất nhiều so với mạng truyền thống.
- Dễ dàng thiết lập, bảo trì và dễ dàng thay đổi đối với mạng đang hoạt động.
- Vì mạng VPN mở rộng được xây dựng dựa trên mạng Internet nên có nhiều cơ hội trong việc cung cấp dịch vụ và chọn lựa giải pháp phù hợp với các nhu cầu của mỗi công ty hơn.
- Vì tận dụng kết nối Internet nên việc bảo trì chủ yếu do ISP đảm nhiệm nên giảm đáng kể chi phí cho thuê nhân viên bảo trì hệ thống.

Tuy nhiên mạng VPN mở rộng cũng vẫn tồn tại một số nhược điểm sau:

- Nguy cơ bảo mật như tấn công từ chối dịch vụ vẫn còn tồn tại.
- Tăng rủi ro cho sự xâm nhập vào Intranet của tổ chức.
- Trong trường hợp truyền tải các dữ liệu đa phương tiện thì gây quá tải, chậm hệ thống và tốc độ truyền sẽ rất chậm do phụ thuộc vào mạng Internet.
- Do truyền dữ liệu dựa trên kết nối Internet nên chất lượng có thể không ổn định và QoS không thể đảm bảo.

Mặc dù vẫn tồn tại nhiều nhược điểm nhưng nó không đủ để làm lu mờ đi những ưu điểm và lợi ích mang lại cho người sử dụng, vì thế VPN luôn được các nhà quản trị mạng yêu thích, sử dụng. Và các doanh nghiệp thì cũng không phải là ngoại lệ, thậm chí họ còn cảm thấy rất thích thú với công nghệ này.

1.3.6. Giới thiệu một số giao thức đường hầm trong VPN

a) Giao thức định hướng L2F (Layer 2 Forwarding).

Giao thức định hướng lớp 2 L2F do Cisco phát triển độc lập và được phát triển dựa trên giao thức PPP (Point-to-Point Protocol). L2F cung cấp giải pháp cho dịch vụ quay số ảo bằng cách thiết lập một đường hầm bảo mật thông qua cơ sở hạ tầng công cộng như Internet. L2F là giao thức được phát triển sớm nhất, là phương pháp truyền thống để cho những người sử dụng ở xa truy cập vào một mạng công ty thông qua thiết bị truy cập từ xa.

L2F cho phép đóng gói các gói PPP trong L2F, định đường hầm ở lớp liên kết dữ liệu.

Ưu nhược điểm của L2F

Ưu điểm:

- Cho phép thiết lập đường hầm đa giao thức.
- Được cung cấp bởi nhiều nhà cung cấp.

Nhược điểm:

- Không có mã hoá.
- Yếu trong việc xác thực người dùng.
- Không có điều khiển luồng cho đường hầm.

b) Giao thức PPTP (Point –to- Point Tunneling Protocol).

Giao thức đường hầm điểm–điểm PPTP được đưa ra đầu tiên bởi một nhóm các công ty được gọi là PPTP Forum. Nhóm này bao gồm 3 công ty: Ascend comm., Microsoft, ECI Telematicsunication và US Robotic. Ý tưởng cơ sở của giao thức này là tách các chức năng chung và riêng của truy cập từ xa, lợi dụng cơ sở hạ tầng Internet sẵn có để tạo kết nối bảo mật giữa người dùng ở xa (client) và mạng riêng. Người dùng ở xa chỉ việc quay số tới nhà cung cấp dịch vụ Internet địa phương là có thể tạo đường hầm bảo mật tới mạng riêng của họ.

Giao thức PPTP được xây dựng dựa trên chức năng của PPP, cung cấp khả năng quay số truy cập tạo ra một đường hầm bảo mật thông qua Internet đến site đích. PPTP sử dụng giao thức bọc gói định tuyến chung GRE (Generic Routing Encapsulation) được mô tả lại để đóng gói và tách gói PPP, giao thức này cho phép PPTP mềm dẻo xử lý các giao thức khác không phải IP như: IPX, NETBEUI.

Do PPTP dựa trên PPP nên nó cũng sử dụng PAP, CHAP để xác thực. PPTP có thể sử dụng PPP để mã hoá dữ liệu nhưng Microsoft đã đưa ra phương thức mã hoá khác mạnh hơn đó là mã hoá điểm - điểm MPPE (Microsoft Point- to- Point Encryption) để sử dụng cho PPTP.

Một ưu điểm của PPTP là được thiết kế để hoạt động ở lớp 2 (lớp liên kết dữ liệu) trong khi IPSec chạy ở lớp 3 của mô hình OSI. Bằng cách hỗ trợ việc truyền dữ liệu ở lớp thứ 2, PPTP có thể truyền trong đường hầm bằng các giao thức khác IP trong khi IPSec chỉ có thể truyền các gói IP trong đường hầm.

c) Giao thức L2TP (Layer 2 Tunneling Protocol).

Giao thức đường hầm lớp 2 L2TP là sự kết hợp giữa hai giao thức PPTP và L2F- chuyển tiếp lớp 2. PPTP do Microsoft đưa ra còn L2F do Cisco khởi xướng. Hai công ty này đã hợp tác cùng kết hợp 2 giao thức lại và đăng ký chuẩn hoá tại IETF.

Giống như PPTP, L2TP là giao thức đường hầm, nó sử dụng tiêu đề đóng gói riêng cho việc truyền các gói ở lớp 2. Một điểm khác biệt chính giữa L2F và PPTP là L2F không phụ thuộc vào IP và GRE, cho phép nó có thể làm việc ở môi trường vật lý khác. Bởi vì GRE không sử dụng như giao thức đóng gói, nên L2F định nghĩa riêng cách thức các gói được điều khiển trong môi trường khác. Nhưng nó cũng hỗ trợ TACACS+ và RADIUS cho việc xác thực. Có hai mức xác thực người dùng: Đầu tiên ở ISP trước khi thiết lập đường hầm, sau đó là ở cổng nối của mạng riêng sau khi kết nối được thiết lập.

L2TP mang đặc tính của PPTP và L2F. Tuy nhiên, L2TP định nghĩa riêng một giao thức đường hầm dựa trên hoạt động của L2F. Nó cho phép L2TP truyền thông qua nhiều môi trường gói khác nhau như X.25, Frame Relay, ATM. Mặc dù nhiều công cụ chủ yếu của L2TP tập trung cho UDP của mạng IP, nhưng có thể thiết lập một hệ thống L2TP mà không cần phải sử dụng IP làm giao thức đường hầm. Một mạng ATM hay frame Relay có thể áp dụng cho đường hầm L2TP.

Do L2TP là giao thức ở lớp 2 nên nó cho phép người dùng sử dụng các giao thức điều khiển một cách mềm dẻo không chỉ là IP mà có thể là IPX hoặc NETBEUI. Cũng giống như PPTP, L2TP cũng có cơ chế xác thực PAP, CHAP hay RADIUS.

Mặc dù Microsoft đã làm cho PPTP trở nên cách chọn lựa phổ biến khi xây dựng VPN bằng cách hỗ trợ giao thức này sẵn có trong hệ điều hành Windows nhưng công ty cũng có kế hoạch hỗ trợ thêm L2TP trong Windows NT 4.0 và Windows 98.

d) Giao thức IPSec (IP Security).

Các giao thức nguyên thuỷ TCP/IP không bao gồm các đặc tính bảo mật vốn có. Trong giai đoạn đầu của Internet khi mà người dùng thuộc các trường đại học và các viện nghiên cứu thì vấn đề bảo mật dữ liệu không phải là vấn đề quan trọng như bây giờ khi mà Internet trở nên phổ biến, các ứng dụng thương mại có mặt khắp nơi trên Internet và đối tượng sử dụng Internet rộng hơn bao gồm cả các Hacker.

Để thiết lập tính bảo mật trong IP ở cấp độ gói, IETF đã đưa ra họ giao thức IPSec. Họ giao thức IPSec đầu tiên được dùng cho xác thực, mã hoá các gói dữ liệu IP, được chuẩn hoá thành các RFC từ 1825 đến 1829 vào năm 1995. Họ giao thức này mô tả kiến trúc cơ bản của IPSec bao gồm hai loại tiêu đề được sử dụng trong gói IP, gói IP là đơn vị dữ liệu cơ sở trong mạng IP. IPSec định nghĩa 2 loại tiêu đề cho các gói IP để điều khiển quá trình xác thực và mã hoá: một là xác thực tiêu đề IP – AH (IP Authentication Header) điều khiển việc xác thực và hai là đóng gói tải tin an toàn ESP (Encapsulation Security Payload) cho mục đích mã hoá.

IPSec không phải là một giao thức. Nó là một khung của các tập giao thức chuẩn mở cho phép những nhà quản trị mạng lựa chọn thuật toán, các khoá và phương pháp nhận thực để cung cấp sự xác thực dữ liệu, tính toàn vẹn dữ liệu, và sự tin cậy dữ liệu. IPSec là sự lựa chọn cho bảo mật tổng thể các VPN, là phương án tối ưu cho mạng của công ty. Nó đảm bảo truyền thông tin cậy trên mạng IP công cộng đối với các ứng dụng.

IPsec tạo những đường hầm bảo mật xuyên qua mạng Internet để truyền những luồng dữ liệu. Mỗi đường hầm bảo mật là một cặp những kết hợp an ninh để bảo vệ luồng dữ liệu giữa hai Host.

IPSec được phát triển nhắm vào họ giao thức IP kế tiếp là IPv6, nhưng do việc triển khai IPv6 còn chậm và sự cần thiết phải bảo mật các gói IP nên IPSec đã được thay đổi cho phù hợp với IPv4. Việc hỗ trợ cho IPSec chỉ là tuỳ chọn của IPv4 nhưng đối với IPv6 thì có sẵn IPSec.

Chương 2.

MỘT SỐ BÀI TOÁN AN TOÀN THÔNG TIN TRONG MẠNG RIÊNG ẢO

2.1. KIỂM SOÁT TRUY NHẬP MẠNG RIÊNG ẢO

2.1.1. Bài toán kiểm soát truy nhập trong Mạng riêng ảo

Bài toán 1: Kiểm soát một thực thể truy nhập vào VPN.

Khi một thực thể truy nhập vào VPN, phải cung cấp được thông tin để chứng minh rằng thực thể đó là thành viên trong mạng VPN. Nếu là thành viên thì thực thể có thể truy nhập và sử dụng tài nguyên của hệ thống với quyền hạn đã được cho phép. Còn ngược lại, nếu thực thể không là thành viên thì sẽ không thể truy nhập vào bên trong VPN.

Bài toán 2: Hai nút mạng cùng trong VPN cần giao tiếp với nhau cũng cần kiểm soát.

Hai nút mạng cùng trong VPN trước khi giao tiếp cũng vậy. Phải kiểm soát chắc chắn rằng đây là hai nút mạng trong cùng VPN mới thực hiện các giao tiếp kết nối tiếp theo. Kiểm soát nhằm xác thực thông tin tin cậy giữa hai nút mạng để tạo ra một kết nối an toàn.

2.1.2. Phương pháp giải quyết

Xác thực là một phần không thể thiếu được trong kiến trúc bảo vệ của một mạng VPN. Xác thực dựa trên ba thuộc tính: Cái gì ta có (một khóa hay một card token); cái gì ta biết (một mật khẩu, chữ ký số); hay cái gì ta nhận dạng (giọng nói, dấu vân tay).

2.1.2.1. Kiểm soát truy nhập bằng mật khẩu

Thực tế cho thấy, các loại xác thực đơn giản, như số nhận dạng ID của người dùng, mật khẩu không đủ mạnh cho việc bảo vệ truy cập mạng. Mật khẩu có thể bị đón bắt và giữ lấy trong suốt quá trình truyền dữ liệu của mạng.

** Hệ thống mật khẩu một lần*

Để ngăn chặn việc sử dụng trái phép, các mật khẩu bị giữ lại và ngăn không cho chúng không được dùng trở lại, bằng cách cần một mật khẩu mới cho phiên làm việc mới.

Những hệ thống này, thì mỗi khi người dùng đăng nhập vào mạng thì luôn luôn phải chọn một mật khẩu mới cho mỗi phiên làm việc kế tiếp. Do đó để khắc phục khó khăn này bằng cách tạo ra một cách tự động một danh sách mật khẩu có thể chấp nhận được cho người dùng. Nhược điểm của các hệ thống này là khó có thể quản trị những danh sách mật khẩu cho một số lượng lớn người dùng.

2.1.2.2. Kiểm soát truy nhập bằng chữ ký số

Người dùng có thể xác thực truy nhập vào hệ thống bằng việc sử dụng "chữ ký số" để đăng ký truy nhập vào mạng riêng ảo.

Một sơ đồ chữ ký số là một bộ 5 (P, A, K, S, V) trong đó :
P là một tập hợp các bản rõ có thể.
A là tập hữu hạn các chữ ký có thể.
K là tập hữu hạn các khóa có thể.
S là tập các thuật toán ký.
V là tập các thuật toán xác minh.
Với mỗi k ∈ K, tồn tại một thuật toán ký $Sig_k \in S$, Sig_k: P → A,
có thuật toán kiểm tra chữ ký $Ver_k \in V$, Ver_k : P x A → {đúng, sai},
thỏa mãn điều kiện sau với mọi x ∈ P, y ∈ A :
$Ver_k(x, y)$ = Đúng, nếu y = Sig_k (x) hoặc Sai, nếu y ≠ Sig_k (x).
Chú ý:
Người ta thường dùng hệ mã hóa khóa công khai để lập: "Sơ đồ chữ ký số".
Ở đây khóa bí mật a dùng làm khóa "ký", khóa công khai b dùng làm khóa kiểm tra "chữ ký".

Người dùng trong mạng VPN tạo "chữ ký" cho mình và đăng ký "chữ ký" với hệ thống. Thông báo khóa kiểm thử (khóa công khai b). Khóa công khai b sẽ được chứng thực là khóa để kiểm thử chữ ký của chính người dùng.

Người dùng sử dụng chữ ký của mình để truy nhập vào VPN. Có 2 cách để kiểm tra chữ ký số:

Cách 1:

+ Bước 1: Người kiểm tra chữ ký, gửi tài liệu cho người ký.

+ Bước 2: Người ký, ký trên tài liệu và gửi tài liệu có chữ ký cho người kiểm tra.

+ Bước 3: Người kiểm tra nhận tài liệu và kiểm tra chữ ký.

Cách 2:

+ Bước 1: Người ký, ký lên khóa công khai của 1 trong 2 người.

+ Bước 2: Người nhận kiểm tra chữ ký.

Công việc kiểm tra chữ ký, nếu chữ ký đúng thì người dùng có thể tham gia kết nối VPN, còn nếu chữ ký là không chính xác thì sẽ không thể truy nhập vào hệ thống.

2.2. BẢO MẬT THÔNG TIN TRONG MẠNG RIÊNG ẢO

2.2.1. Bài toán bảo mật thông tin trong Mạng riêng ảo

Bài toán: Hai nút mạng trong VPN truyền tin cho nhau cần bảo mật (tránh xem trộm thông tin).

Bảo mật thông tin là làm cho thông tin trở thành bí mật, những người ngoài cuộc không thể xem được hay không hiểu được nội dung thông tin. Bài toán bảo mật thông tin bao gồm 3 phương pháp:

1) Nén thông tin.
2) Mã hóa thông tin.
3) Giấu thông tin.

Để bảo vệ thông tin bên trong máy tính hay đang trên đường truyền tin, phải nghiên cứu về An toàn máy tính và An toàn truyền tin.

* An toàn máy tính (Computer Security):

Là sự bảo vệ các thông tin cố định bên trong máy tính (Static Informations)

Là khoa học về bảo đảm an toàn thông tin trong máy tính.

* An toàn truyền tin (Communication Security):

Là sự bảo vệ thông tin trên đường truyền tin (Dynamic Informations).

Là khoa học về bảo đảm an toàn thông tin trên đường truyền tin.

2.2.2. Bảo mật thông tin bằng phương pháp mã hóa

Để bảo đảm an toàn thông tin lưu trữ trong các máy tính hay bảo đảm an toàn thông tin trên đường truyền tin (mạng máy tính) người ta có thể sử dụng các phương pháp mã hóa để che dấu các thông tin này.

Mã hóa dữ liệu là thực hiện công việc che thông tin và giấu thông tin.

Che thông tin (dữ liệu) hay mã hóa thông tin là thay đổi hình dạng thông tin gốc và người khác khó nhận ra hay đọc được nội dung thông tin gốc.

Giấu thông tin (dữ liệu) là cất giấu thông tin trong bản tin khác, và người khác cũng khó nhận ra.

Sử dụng phương pháp mã hóa là quá trình mật mã dữ liệu truyền đi khỏi máy tính theo một quy tắc nhất định và máy tính đầu xa có thể giải mã được. Hầu hết các hệ thống mã hóa máy tính thuộc về một trong hai loại sau:

- Mã hóa khóa đối xứng (Symmetric-key encryption)
- Mã hóa khóa công khai (Public-key encryption)

a) Mã hóa khóa đối xứng (Symmetric-key encryption)

Thuật toán đối xứng được định nghĩa là một thuật toán khoá chia sẻ sử dụng để mã hoá và giải mã một bản tin. Các thuật toán mã hoá khóa đối xứng sử dụng chung một khoá để mã hoá và giải mã bản tin, điều đó có nghĩa là cả bên gửi và bên nhận đã thoả thuận, đồng ý sử dụng cùng một khoá bí mật để mã hoá và giải mã.

Ưu điểm của mã hoá khoá đối xứng:

- Thuật toán này mã hoá và giải mã rất nhanh, phù hợp với một khối lượng lớn thông tin
- Chiều dài khoá từ 40÷168 bit.
- Các tính toán toán học dễ triển khai trong phần cứng.
- Người gửi và người nhận chia sẻ chung một mật khẩu.

Ví dụ: Khi tạo một bức thư mã hóa mà trong nội dung thư mỗi ký tự được thay thế bằng ký tự ở sau nó hai vị trí trong bảng ký tự. Như vậy ký tự "A" sẽ được thay thế bằng ký tự "C" , ký tự "B" sẽ được thay thế bằng ký tự "D"… Giữa hai người đã có quy ước khóa riêng là dịch đi hai vị trí (Shif by 2). Người nhận được thư sẽ giải mã sử dụng khóa riêng đó và đọc được nội dung thư gốc. Còn người khác sẽ không đọc được nội dung thư gốc vì không biết khóa riêng.

Ở đây cần có sự trao đổi khóa bí mật. Máy tính gửi mã hóa dữ liệu cần gửi khóa bí mật (symmetric key), sau đó mã hóa chính khóa bí mật bằng khóa công khai của người nhận (public key). Máy tính của người nhận sử dụng khóa riêng của nó (private key) tương ứng với khóa public key để giải mã nhận được khóa bí mật (symmetric key). Sau đó dùng chính khóa bí mật này để giải mã dữ liệu đã đươc mã hóa.

Nơi sử dụng hệ mã hóa khóa đối xứng (khóa bí mật): Thường được sử dụng trong môi trường khóa chung có thể dễ dàng trao chuyển bí mật, chẳng hạn trong cùng một mạng nội bộ. Hệ mã hóa khóa đối xứng thường dùng để mã hóa những bản tin lớn, vì tốc độ mã hóa và giải mã nhanh hơn hệ mã hóa khóa công khai. Thuật toán mã hóa DES là thuật toán mã hóa khóa bí mật.

b) Mã hóa khóa công khai (Public-key encryption)

Thuật toán mã hoá khoá công khai được định nghĩa là một thuật toán sử dụng một cặp khoá để mã hoá và giải mã bảo mật một bản tin. Theo thuật toán này thì sử dụng một khoá để mã hoá và một khoá khác để giải mã nhưng hai khoá này có liên quan với nhau tạo thành một cặp khoá duy nhất của một bản tin, chỉ có hai khoá này mới có thể mã hoá và giải mã cho nhau.

Ưu điểm của thuật toán mã hoá khoá công khai:

- Khoá công khai của khoá đôi có thể được phân phát một cách sẵn sàng mà không sợ rằng điều này làm ảnh hưởng đến việc sử dụng các khoá riêng. Không cần phải gửi một bản sao chép khoá công khai cho tất cả các đáp ứng mà chúng ta có thể lấy nó từ một máy chủ được duy trì bởi một công ty hay là nhà cung cấp dịch vụ.
- Cho phép xác thực nguồn phát của bản tin.

Nơi sử dụng hệ mã hóa công khai: Thường được sử dụng chủ yếu trên các đường truyền mạng công cộng, khi mà việc trao chuyển khóa bí mật là tương đối khó khăn. Đặc trưng nổi bật của hệ mã hóa công khai là khóa công khai (public key) và bản mã (ciphertext) đều có thể gửi đi trên một kênh truyền tin không an toàn. Có biết cả khóa công khai và bản mã thì thám mã cũng không dễ khám phá được bản rõ. Nhưng vì tốc độ mã hóa và giải mã chậm, nên hệ mã hóa công khai chỉ dùng để mã hóa những bản tin ngắn, ví dụ như mã hóa khóa bí mật gửi đi. Một số thuật toán sử dụng mã hoá khoá công khai như RSA, Diffie-Hellman.

2.3. BẢO TOÀN THÔNG TIN TRONG MẠNG RIÊNG ẢO

2.3.1. Bài toán bảo toàn thông tin trong Mạng riêng ảo

Bài toán: Hai nút mạng trong VPN truyền tin cho nhau, thì thông tin đó cần được bảo toàn (tránh sửa đổi thông tin trái phép).

Bảo toàn thông tin hay bảo đảm tính toàn vẹn của thông tin: Người ngoài cuộc khó có thể thay đổi được (sửa chữa lại nội dung) thông tin. Là đặc tính khi thông tin trên mạng chưa được ủy quyền thì không thể tiến hành biến đổi được, tức là thông tin trên mạng khi đang lưu giữ hoặc trong quá trình truyền dẫn đảm bảo không bị xóa bỏ, sửa đổi, giả mạo làm rối loạn trật tự, phát lại, xen vào một cách ngẫu nhiên hoặc cố ý và những sự phá hoại khác.

Mục tiêu của việc kết nối mạng là để nhiều người sử dụng, từ những vị trí địa lý khác nhau có thể sử dụng chung tài nguyên, trao đổi thông tin với nhau. Do đặc điểm nhiều người sử dụng lại phân tán về mặt vật lý nên việc bảo vệ các tài nguyên thông tin trên mạng, tránh sự mất mát, xâm phạm là cần thiết và cấp bách.

Công việc truyền tin giữa hai nút mạng được thực hiện qua mạng Internet nên có thể xảy ra trường hợp một "bên thứ ba" có thể gây ra hành động mất mát an toàn thông tin trong giao dịch. Một số vấn đề an toàn thông tin hiện nay:

- Nghe trộm (Eavasdropping): Thông tin không hề bị thay đổi, nhưng sự bí mật của nó thì không còn. Ví dụ, một ai đó có thể biết được số thẻ tín dụng, hay các thông tin cần bảo mật của bạn.
- Giả mạo (tampering): Các thông tin trong khi truyền trên mạng bị thay đổi hay bị thay đổi trước khi đến người nhận. Ví dụ, một ai đó có thể sửa đổi nội dung của một đơn đặt hàng hoặc thay đổi lý lịch của một cá nhân trước khi các thông tin đó đến đích.
- Mạo danh (Impersonation): Một cá nhân có thể dựa vào thông tin của người khác để trao đổi với một đối tượng. Bao gồm 2 hình thức: mạo danh bắt trước, và mạo danh xuyên tạc.

Để vừa đảm bảo tính bảo toàn của thông tin lại không làm giảm sự phát triển của việc trao đổi thông tin thì chúng ta cần có các giải pháp phù hợp. Hiện tại có rất nhiều giải pháp cho vấn đề an toàn tông tin trên mạng như mã hóa thông tin, chữ ký điện tử (chứng chỉ khóa khóa công khai)… Sau đây chúng ta lần lượt tìm hiểu các giải pháp cho bài toán bảo toàn thông tin trong mạng riêng ảo.

2.3.2. Phương pháp giải quyết

Để giải quyết bài toán bảo toàn thông tin, hiện nay có nhiều phương pháp để giải quyết bài toán trên. Ở đây ta nghiên cứu hai phương pháp cơ bản mà được ứng dụng phổ biến trong công nghệ mạng riêng ảo hiện nay:

- Phương pháp 1: Bảo toàn thông tin bằng mã hóa thông tin.
- Phương pháp 2: Bảo toàn thông tin bằng kỹ thuật chữ ký số (Digital Signature).

2.3.2.1. Bảo toàn bằng phương pháp mã hóa

Để đảm bảo thông tin trên đường truyền tin khó có thể bị sửa đổi làm sai lệch thông tin từ bên ngoài. Mã hóa là một công cụ an toàn được ứng dụng rộng dãi trong vấn đề an toàn và bảo mật thông tin trong thời buổi công nghệ hiện nay. Mã hóa đảm bảo các nhiệm vụ chính nhằm che giấu thông tin một cách an toàn, với các thuật toán mã hóa mới hiện nay thì độ phức tạp của bài toán thám mã là rất khó.

Sử dụng các phương pháp mã hóa đối xứng (Hệ mã hóa DES), hay phương pháp mã hóa công khai (Hệ mã hóa RSA, Engamal) để thực hiện mã hóa các bản tin trước khi được truyền đi giữa hai nút mạng. Đảm bảo bản tin khó bị bắt trên đường truyền tin, nếu có bắt được thì đó là một bản mã nên khó có thể giải mã được bản tin để sửa đổi.

Mã hóa thông tin trước khi truyền thông tin đó cho người nhận đảm bảo rằng thông tin đó sẽ không ai có thể đọc, hiểu được nội dung, ngoài người nhận đã nắm giữ khóa giải mã. Chính vì vậy, dù có bắt được gói tin mã hóa trên đường truyền tin thì người khác cũng khó có thể vào đó sửa đổi nội dung của bản tin theo mục đích của mình. Như vậy nội dung của thông tin sẽ được toàn vẹn khi đến người nhận.

2.3.2.2. Bảo toàn sử dụng kỹ thuật chữ ký số

Chữ ký điện tử (digital signature) là đoạn dữ liệu ngắn đính kèm với văn bản gốc để chứng thực tác giả của văn bản và giúp người nhận kiểm tra tính toàn vẹn của nội dung văn bản gốc.

Chữ ký điện tử được tạo ra bằng cách áp dụng thuật toán băm một chiều trên văn bản gốc để tạo ra bản phân tích văn bản (message digest) hay còn gọi là fingerprint, sau đó mã hóa bằng private key tạo ra chữ ký số đính kèm với văn bản gốc để gửi đi. Khi nhận, văn bản được tách làm 2 phần, phần văn bản gốc được tính lại fingerprint để so sánh với fingerprint cũ cũng được phục hồi từ việc giải mã chữ ký số.

Các bước mã hóa:

1) Dùng giải thuật băm để thay đổi thông điệp cần truyền đi. Kết quả ta được một message digest. Dùng giải thuật MD5 (Message Digest 5) ta được digest có chiều dài 128-bit, dùng giải thuật SHA (Secure Hash Algorithm) ta có chiều dài 160-bit.

2) Sử dụng khóa private key của người gửi để ký số message digest thu được ở bước 1. Thông thường ở bước này ta dùng giải thuật RSA. Kết quả thu được gọi là digital signature của message ban đầu.

3) Gộp digital signature vào message ban đầu. Công việc này gọi là "ký nhận" vào message. Sau khi đã ký nhận vào message, mọi sự thay đổi trên message sẽ bị phát hiện trong giai đoạn kiểm tra. Ngoài ra, việc ký nhận này đảm bảo người nhận tin tưởng message này xuất phát từ người gửi chứ không phải là ai khác.

Các bước kiểm tra:

1) Dùng public key của người gửi (khóa này được thông báo đến mọi người) để giải mã chữ ký số của message.

2) Dùng giải thuật (MD5 hoặc SHA) băm message đính kèm.

3) So sánh kết quả thu được ở bước 1 và 2. Nếu trùng nhau, ta kết luận message này không bị thay đổi trong quá trình truyền và message này là của người gửi.

Chương 3. THỬ NGHIỆM CHƯƠNG TRÌNH

3.1. THỬ NGHIỆM CHƯƠNG TRÌNH

3.1.1. Chương trình mã hóa dịch chuyển

Sơ đồ :

Đặt P = C = K = Z_{26}. Bản mã y và bản rõ x ∈ Z_{26}.

Với khóa k ∈ K, ta định nghĩa:

Hàm mã hóa: $y=e_k(x) = (x+k) \bmod 26$

Hàm giải mã: $x=d_k(y) = (y-k) \bmod 26$

3.1.2. Chương trình chữ ký số RSA

Sơ đồ

Tạo cặp khóa (bí mật, công khai) (a,b):

Chọn bí mật nguyên tố lớn p, q, tính n=p*q, công khai n đặt $P=C=Z_n$

Tính bí mật $\emptyset(n)$ = (q-1)(p-1).

Chọn khóa công khai b <$\emptyset(n)$, nguyên tố cùng nhau với $\emptyset(n)$.

Khóa bí mật a là phần tử nghịch đảo của b theo mod $\emptyset(n)$: $a*b=1 \pmod{\emptyset(n)}$.

Ký số:

Chữ ký trên x ∈P là $y = Sig_k(x) = x^a \pmod n$, y ∈ A (R1).

Kiểm tra chữ ký:

$Ver_k(x,y)$ = đúng ⇔ $x= y^b \pmod n$ (R2).

3.2. CẤU HÌNH HỆ THỐNG

1/. **Phần cứng**

- Ram: 4GB
- CPU: Intel Core i5-3230M @ 2.60GHz

2/. **Phần mềm**

- Hệ điều hành (OS): Windows 7
- Visual Studio 2010
- Ngôn ngữ lập trình: Viết bằng C# trên nền .NET 4.0

3.3. CÁC THÀNH PHẦN CỦA CHƯƠNG TRÌNH

3.3.1. Chương trình mã hóa dịch chuyển

Chương trình mã hóa dịch chuyển để thực hiện quá trình mã hóa và giải mã dữ liệu. Dữ liệu được mã hóa trước khi truyền tin cho người nhận để đảm bảo việc dữ liệu an toàn theo đúng nghĩa mà chỉ có người nhận mới có thể đọc được nội dung của tài liệu được gửi.

Chương trình có 2 phần chính:

- Mã hóa xâu dữ liệu.
- Giải mã xâu dữ liệu.

Mỗi phần đều bao gồm các thông tin:

- Bản rõ: là nơi chứa nội dung dữ liệu cần mã hóa.
- Khóa k: dùng để mã hóa và giải mã.
- Bản mã: là nơi chưa nội dung đã được mã hóa.
- Nút mã hóa, nút giải mã: để thực hiện 2 quá trình mã hóa dữ liệu và giải mã.

3.3.2. Chương trình ký số RSA

Chương trình ký số RSA được sử dụng để tạo một chữ ký trên một chữ số x, và sử dụng để kiểm tra một chữ ký.

Chương trình gồm 2 phần chính:

- Ký số trên một chữ số.
- Kiểm tra chữ ký.

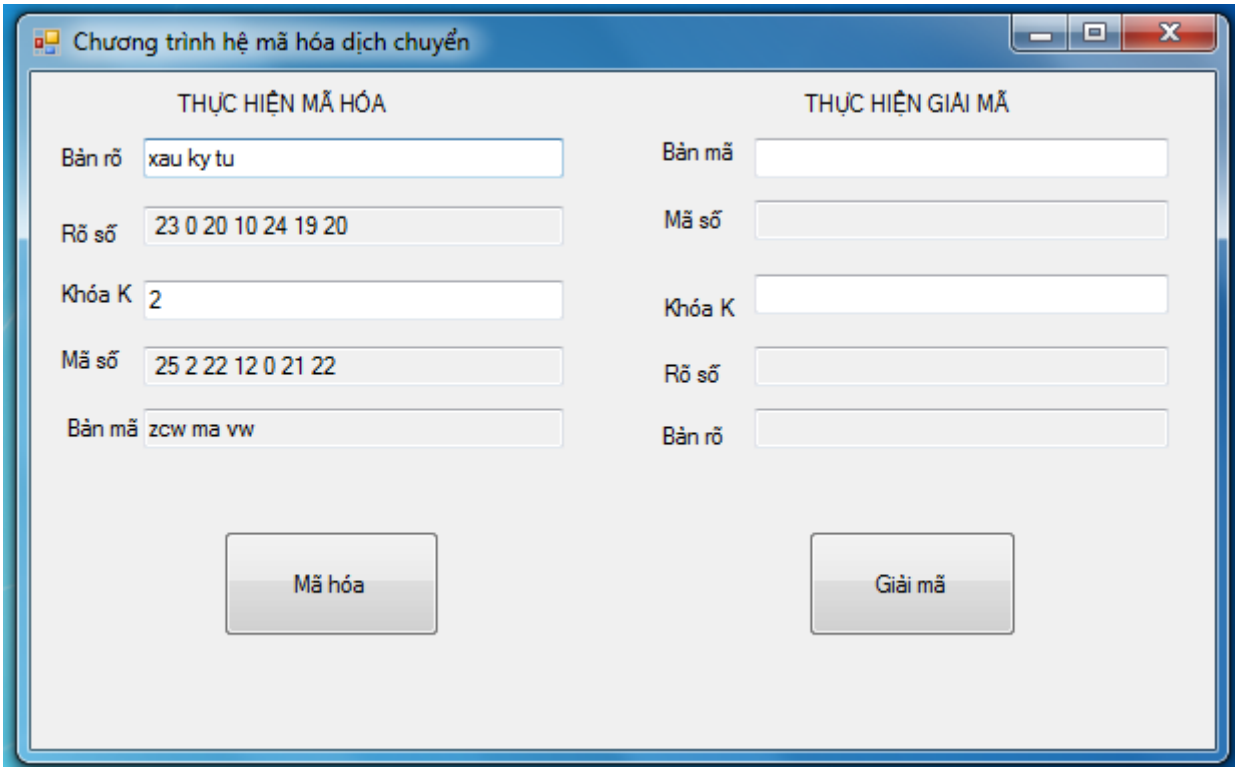
Chương trình bao gồm các thẻ:

- Ký số, kiểm thử.
- Thẻ nhập số nguyên tố p, q, khóa công khai b.

3.4. HƯỚNG DẪN SỬ DỤNG CHƯƠNG TRÌNH

3.4.1. Chương trình mã hóa dịch chuyển

1/. **Thực hiện mã hóa**

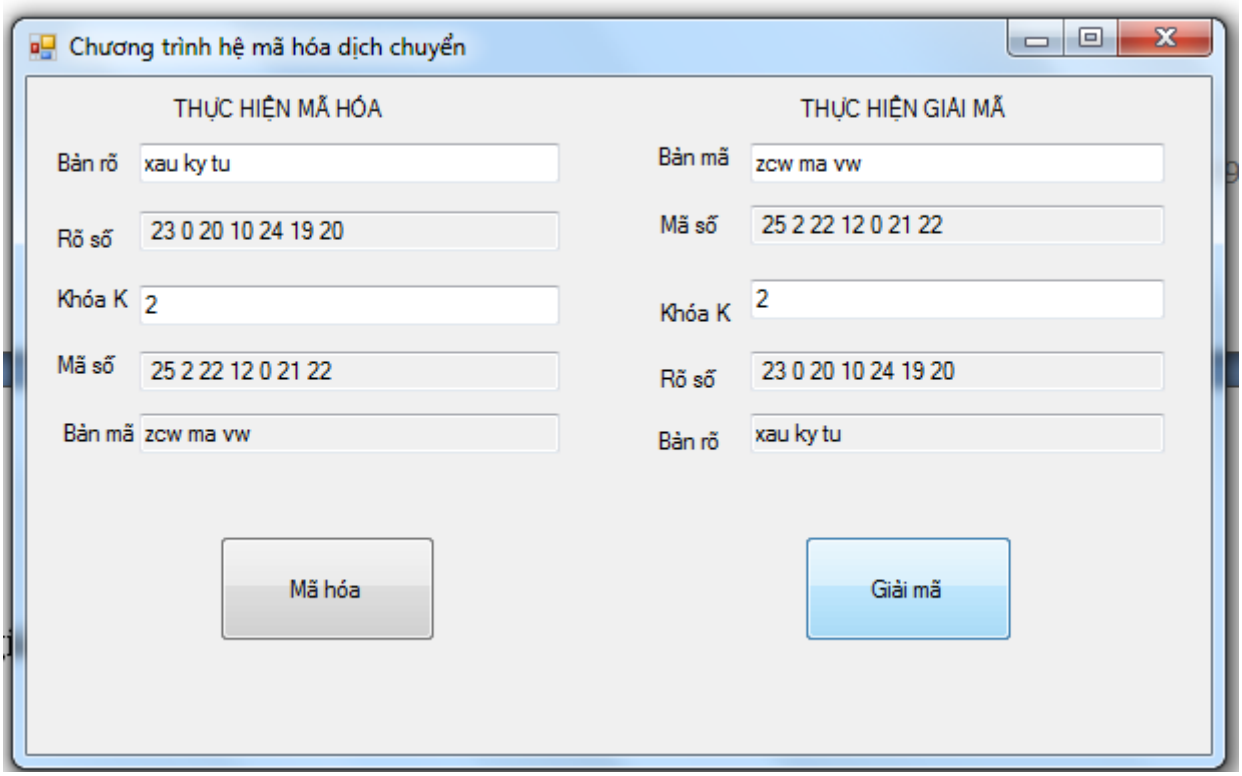


Các bước thực hiện:

- Bước 1: Nhập xâu ký tự cần mã hóa.
- Bước 2: Nhập khóa k để mã hóa (k>=1; k<=26)
- Bước 3: Click nút "Mã hóa" để thực hiện quá trình mã hóa.

Quá trình mã hóa thành công sẽ hiện thị thông tin đã được mã hóa trong ô "Bản mã".

2/. **Thực hiện giải mã**



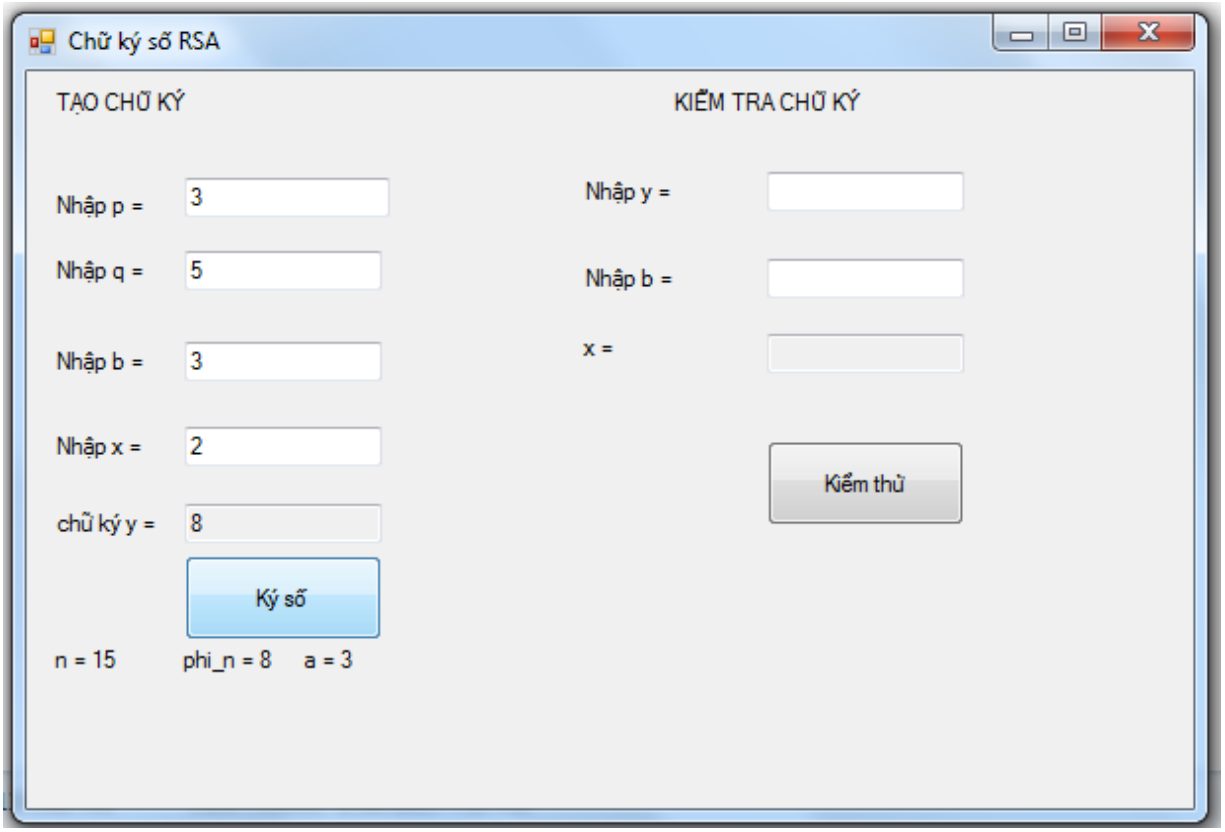
Các bước thực hiện:

- Bước 1: Nhập xâu ký tự cần giải mã.
- Bước 2: Nhập khóa k để giải mã (k>=1; k<=26)
- Bước 3: Click nút “Giải mã” để thực hiện quá trình giải mã.

Quá trình giải mã thành công sẽ hiện thị thông tin đã được giải mã trong ô “Bản rõ”.

3.4.2. Chương trình ký số RSA

1/. **Thực hiện ký số**

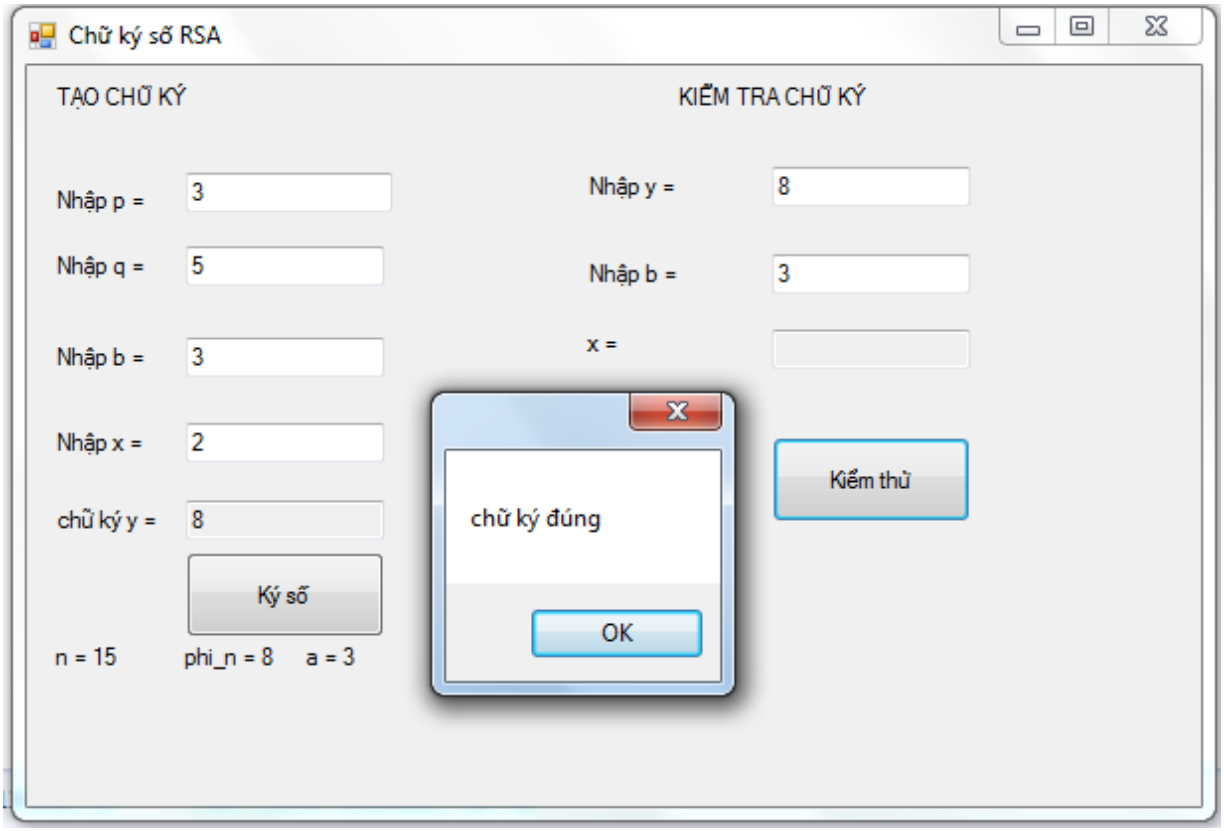


Các bước thực hiện:

- Bước 1: Nhập số nguyên tố p, q.
- Bước 2: Nhập khóa công khai b.
- Bước 3: Nhập chữ số x cần tạo chữ ký trên x.
- Bước 4: Click nút "Ký số" để thực hiện tạo chữ ký trên x.

Thực hiện ký số xong sẽ hiện thị thông tin chữ ký y, và khóa bí mật công khai (a,b).

2/. **Thực hiện kiểm thử chữ ký**



Các bước thực hiện:

- Bước 1: Nhập chữ ký y.
- Bước 2: Nhập khóa công khai b.
- Bước 3: Click nút "Kiểm thử" để thực hiện kiểm tra chữ ký y.

Thực hiện kiểm thử xong, chương trình sẽ thông báo "chữ ký đúng" hoặc "chữ ký sai".

KẾT LUẬN

Đồ án tốt nghiệp có hai kết quả chính:

1/. **Về mặt lý thuyết**

Đồ án tốt nghiệp trình bày các vấn đề sau:

- Tổng quan về An toàn thông tin.
- Tổng quan về Mạng riêng ảo.
- Một số Bài toán An toàn thông tin trong Mạng riêng ảo.

2/. **Về mặt thực hành**

Đồ án tốt nghiệp đã thử nghiệm chương trình:

- Chương trình mã hóa dịch chuyển.
- Chương trình ký số RSA.

PHỤ LỤC

1/. Code chương trình mã hóa dịch chuyển

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Windows.Forms;

namespace Ma_hoa_dich_chuyen
{
    public partial class Form1 : Form
    {
        public Form1()
        {
            InitializeComponent();
        }
        //============================================================
        public static int kytu_so(char c)//tu ky tu chuyen sang so
        {
            if (c == 'a') return 0;
            if (c == 'b') return 1;
            if (c == 'c') return 2;
            if (c == 'd') return 3;
            if (c == 'e') return 4;
            if (c == 'f') return 5;
            if (c == 'g') return 6;
            if (c == 'h') return 7;
            if (c == 'i') return 8;
            if (c == 'j') return 9;
            if (c == 'k') return 10;
            if (c == 'l') return 11;
            if (c == 'm') return 12;
            if (c == 'n') return 13;
            if (c == 'o') return 14;
            if (c == 'p') return 15;
            if (c == 'q') return 16;
            if (c == 'r') return 17;
            if (c == 's') return 18;
            if (c == 't') return 19;
            if (c == 'u') return 20;
            if (c == 'v') return 21;
            if (c == 'w') return 22;
            if (c == 'x') return 23;
            if (c == 'y') return 24;
            if (c == 'z') return 25;
```

```
        return 1;
    }
    public static String so_kytu(int c)//tu so chuyen sang ky tu
    {
        if (c == 0) return "a";
        if (c == 1) return "b";
        if (c == 2) return "c";
        if (c == 3) return "d";
        if (c == 4) return "e";
        if (c == 5) return "f";
        if (c == 6) return "g";
        if (c == 7) return "h";
        if (c == 8) return "i";
        if (c == 9) return "j";
        if (c == 10) return "k";
        if (c == 11) return "l";
        if (c == 12) return "m";
        if (c == 13) return "n";
        if (c == 14) return "o";
        if (c == 15) return "p";
        if (c == 16) return "q";
        if (c == 17) return "r";
        if (c == 18) return "s";
        if (c == 19) return "t";
        if (c == 20) return "u";
        if (c == 21) return "v";
        if (c == 22) return "w";
        if (c == 23) return "x";
        if (c == 24) return "y";
        if (c == 25) return "z";

        return "";
    }
    private void btmahoa_Click(object sender, EventArgs e)
    {
        String banro;
        int k;
        int idx;
        banro = txtbanro.Text;
        k = Convert.ToInt16(txtk.Text);
        txtbanma.Text = "";
        txtmaso.Text = "";
        txtroso.Text = "";
        if (k >= 1 && k < 26)
        {
            for (int i = 0; i < banro.Length; i++)
            {
                if (banro[i].ToString() != " ")
                {
                    idx = kytu_so(banro[i]);
                    txtroso.Text +=" " + idx;
                    idx = (idx + k) % 26;
```

```
                    txtmaso.Text +=" " + idx;
                    txtbanma.Text +=so_kytu(idx);

                }
                else
                    txtbanma.Text += " ";

            }
        }

        else
            MessageBox.Show("Yêu cầu nhập k >= 1 và k < 26");
    }

    private void txtgiaima_Click(object sender, EventArgs e)
    {
        String banma;
        int k;
        int idy;
        banma = txtbma.Text;
        k = Convert.ToInt16(txtgmk.Text);
        txtbro.Text = "";
        txtrso.Text = "";
        txtmso.Text = "";
        if (k >= 1 && k < 26)
        {
            for (int i = 0; i < banma.Length; i++)
            {
                if (banma[i].ToString() != " ")
                {
                    idy = kytu_so(banma[i]);
                    txtmso.Text +=" " + idy;
                    if(idy>=k)
                        idy = (idy - k) % 26;
                    else
                        idy = (idy - k + 26) % 26;
                    txtrso.Text +=" " + idy;
                    txtbro.Text += so_kytu(idy);

                }
                else
                    txtbro.Text += " ";

            }
        }

        else
            MessageBox.Show("Yêu cầu nhập k >= 1 và k < 26");
    }

}
}
```

2/. **Code chương trình ký số RSA**

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Windows.Forms;

namespace chu_ky_RSA
{
    public partial class Form1 : Form
    {
        public Form1()
        {
            InitializeComponent();
        }
        //=====================================================

        //tinh nghich dao
        public int nghichdao(int A, int B)
        {

            for (int i = 1; i < B; i++)
            {

                if ((i * A) % B == 1)
                {
                    A = i;
                    break;
                }
            }
            return (A);
        }
        //=====================================================
        int p, q, pi_n, n, a, b;
        Int64 x, y,xkt;
        private void btkyso_Click(object sender, EventArgs e)
        {

            p =Convert.ToInt16( txtp.Text);
            q = Convert.ToInt16(txtq.Text);
            x = Convert.ToInt16(txtx.Text);
            b = Convert.ToInt16(txtb.Text);
            n = p * q;
            pi_n = (p - 1) * (q - 1);
            //-----------------------
            //tao khoa a
            a = nghichdao(b, pi_n);
```

```
            //ký số trên x
            y = Convert.ToInt64(Math.Pow(x, a)) % n;
            txty.Text = y.ToString();
            lbn.Text = "n = " + n.ToString();
            lbb.Text = "phi_n = " + pi_n.ToString();
            lba.Text = "a = " + a.ToString();
        }

        private void btkiemthu_Click(object sender, EventArgs e)
        {
            y = Convert.ToInt16(txtkty.Text);
            b = Convert.ToInt16(txtktb.Text);
            xkt = Convert.ToInt64(Math.Pow(y,b)) % n;
            if (x == xkt)
                MessageBox.Show("chữ ký đúng");
            else
                MessageBox.Show("chữ ký sai");
            txtktx.Text = xkt.ToString();
        }



    }
}
```