BỘ GIÁO DỤC VÀ ĐÀO TẠO

TR- ỜNG ĐẠI HỌC DÂN LẬP HẢI PHÒNG

-------o0o-------

TÌM HIỂU, NGHIÊN CỨU MỘT SỐ TÌNH HUỐNG TRONG CHUYỂN GIAO HỒ SƠ Y TẾ ĐIỆN TỬ

ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC HỆ CHÍNH QUY

Ngành: Công nghệ thông tin

Sinh viên thực hiện: Nguyễn Thị Hồng Nhung

Giáo viên h- ớng dẫn:PGS.TS. Trịnh Nhật Tiến

Mã số sinh viên: 121556

Hải Phòng 7 - 2012

MỤC LỤC

LỜI CẢM ƠN

Em xin chân thành cảm ơn tất cả các thầy cô trong khoa Công nghệ thông tin Trường ĐHDL Hải Phòng, những người đã nhiệt tình giảng dạy và truyền đạt những kiến thức cần thiết trong suốt thời gian em học tập tại trường để em có thể hoàn thành tốt quá trình học tập của mình.

Đặc biệt, em xin gửi lời cảm ơn chân thành nhất đến PGS.TS.Trịnh Nhật Tiến người đã trực tiếp hướng dẫn tận tình chỉ bảo em trong suốt quá trình làm đồ án tốt nghiệp.

Với sự hiểu biết còn hạn chế cộng với vốn kiến thức còn phải học hỏi nhiều nên bài báo cáo của em không thể tránh khỏi những thiếu sót, em rất mong có được sự góp ý của các thầy cô giáo và các bạn để kết quả của em được hoàn thiện hơn.

Em xin chân thành cảm ơn!

Hải phòng, ngày… tháng… năm 2012

Sinh viên thực hiện

Nguyễn Thị Hồng Nhung

GIỚI THIỆU

Nhu cầu về bảo đảm an toàn thông tin trong lĩnh vực y sinh học ngày càng tăng, nhằm phục vụ công tác chăm sóc sức khỏe của cộng đồng và phục vụ các hoạt động nghiên cứu trong lĩnh vực này. Sự phát triển của dữ liệu đa phương tiện đã hỗ trợ tích cực các hoạt động y sinh học như chẩn đoán từ xa, chia sẻ thông tin y tế. Tuy nhiên, việc chia sẻ thông tin y sinh học của mỗi cá nhân (PHR – Patient Health Records) có thể xâm phạm tính riêng tư của người bệnh khi sử dụng các hệ thống E-Health. Do vậy vấn đề bảo đảm an toàn thông tin và chia sẻ thông tin trong hệ thống E-Health càng được đặt ra cấp thiết.

Chương 1. MỘT SỐ KHÁI NIỆM CƠ BẢN

1.1. TỔNG QUAN VỀ AN TOÀN THÔNG TIN

1.1.1. Định nghĩa An toàn thông tin

- An toàn nghĩa là thông tin được bảo vệ, các hệ thống và những dịch vụ có khả năng chống lại những tai hoạ, lỗi và sự tác động không mong đợi, các thay đổi tác động đến độ an toàn của hệ thống là nhỏ nhất.
- Hệ thống có một trong các đặc điểm sau là không an toàn: Các thông tin dữ liệu trong hệ thống bị người không được quyền truy nhập tìm cách lấy và sử dụng (thông tin bị rò rỉ). Các thông tin trong hệ thống bị thay thế hoặc sửa đổi làm sai lệch nội dung (thông tin bị xáo trộn)...
- Thông tin chỉ có giá trị cao khi đảm bảo tính chính xác và kịp thời, hệ thống chỉ có thể cung cấp các thông tin có giá trị thực sự khi các chức năng của hệ thống đảm bảo hoạt động đúng đắn. Mục tiêu của an toàn bảo mật trong công nghệ thông tin là đưa ra một số tiêu chuẩn an toàn. Ứng dụng các tiêu chuẩn an toàn này vào đâu để loại trừ hoặc giảm bớt các nguy hiểm.

1.1.2. Sự cần thiết của an toàn thông tin.

- Ngày nay, sự xuất hiện Internet và mạng máy tính đã giúp cho việc trao đổi thông tin trở nên nhanh gọn, dễ dàng, E-mail cho phép người ta gửi nhận thư ngay trên máy tính của mình, E-businees cho phép thực hiện các giao dịch trên mạng …
- Tuy nhiên lại phát sinh những vấn đề mới. Thông tin quan trọng nằm ở kho dữ liệu hay đang trên đường truyền có thể bị trộm cắp, có thể bị làm sai lệch, có thể bị giả mạo. Điều đó có thể ảnh hưởng tới các tổ chức, các công ty hay cả một Quốc gia. Những bí mật kinh doanh, tài chính là mục tiêu của các đối thủ cạnh tranh. Những tin tức về an ninh quốc gia là mục tiêu của các tổ chức tình báo trong và ngoài nước.
- Theo số liệu của CERT (Computer Emegency Response Team) số lượng các vụ tấn công trên Internet mỗi ngày một nhiều, quy mô của chúng ngày càng lớn và phương pháp tấn công ngày càng hoàn thiện.

- Khi trao đổi thông tin trên mạng, những tình huống mới nảy sinh:
- Người ta nhận được một bản tin trên mạng, thì lấy gì đảm bảo rằng nó là của đối tác đã gửi cho họ. Khi nhận được tờ Sec điện tử hay tiền điện tử trên mạng, thì có cách nào xác nhận rằng nó là của đối tác đã thanh toán cho ta. Tiền đó là thật hay tiền giả?
- Thông thường người gửi văn bản quan trọng phải ký phía dưới. Nhưng khi truyền tin trên mạng, văn bản hay giấy thanh toán có thể bị trộm cắp và phía dưới có thể dán một chữ ký khác. Tóm lại với hình thức ký như cũ, chữ ký rất dễ bị giả mạo.
- Để giải quyết vấn đề trên, vấn đề bảo đảm an toàn thông tin đã được đặt ra trong lý luận cũng như trong thực tiễn.

1.1.3. Mục tiêu của an toàn thông tin.

- Bảo đảm bí mật: thông tin không bị lộ đối với người không được phép.
- Bảo đảm toàn vẹn: ngăn chặn hay hạn chế việc bổ sung,loại bỏ và sửa dữ liệu không được phép.
- Bảo đảm xác thực: xác thực đúng thực thể cần kết nối giao dịch, xác thực đúng thực thể có trách nhiệm về nội dung thông tin.
- Bảo đảm sẵn sàng: thông tin săn sàng cho người dùng hợp pháp.

1.1.4. Các nội dung An toàn thông tin.

1.1.4.1. Nội dung chính:

- 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 là khoa học về đảm bảo an toàn thông tin trong máy tính.
- An toàn truyền tin (Communication Security): là sự bảo vệ thông tin trên đường truyền tin, là khoa học đảm bảo an toàn thông tin trên đường truyền tin.

1.1.4.2. Nội dung chuyên ngành

- Để bảo vệ thông tin bên trong máy tính hay đang trên đường truyền tin, phải nghiên cứu các nội dung chuyên ngành sau:

- An toàn dữ liệu
- An toàn cơ sở dữ liệu
- An toàn Hệ điều hành
- An toàn mạng máy tính

1.1.5. Các chiến lược bảo đảm an toàn thông tin

- Cấp quyền hạn tối thiểu: nguyên tắc cơ bản trong an toàn nói chung là "Hạn chế sự ưu tiên". Mỗi đối tượng sử dụng hệ thống chỉ được cấp phát một số quyền hạn nhất định đủ dùng cho công việc của mình.
- Phòng thủ theo chiều sâu: nguyên tắc tiếp theo trong an toàn nói chung là "Bảo vệ theo chiều sâu" cụ thể là lập nhiều lớp bảo vệ khác nhau cho hệ thống.

1.1.6. Các giải pháp bảo đảm an toàn thông tin

1.1.6.1. Phương pháp che giấu, bảo đảm toàn vẹn và xác thực thông tin

- "Che" dữ liệu (mã hóa): thay đổi hình dạng dữ liệu gốc, người khác khó nhận ra.
- "Giấu" dữ liệu: cất giấu dữ liệu này trong môi trường dữ liệu khác
- Bảo đảm toàn vẹn dữ liệu và xác thực thông tin

1.1.6.2. Phương pháp kiểm soát lối vào ra của thông tin

- Kiểm soát,ngăn chặn các thông tin vào ra hệ thống máy tính
- Kiểm soát, cấp quyền sử dụng các thông tin trong hệ thống máy tính
- Kiểm soát, tìm diệt "sâu bọ" vào ra hệ thống máy tính

1.1.6.3. Phát hiện và xử lý các lỗ hổng trong an toàn thông tin.

- Các "lỗ hổng" trong các thuật toán hay giao thức mật mã, giấu tin.
- Các "lỗ hổng" trong các giao thức mạng.
- Các "lỗ hổng" trong hệ điều hành.
- Các "lỗ hổng" trong các ứng dụng.

1.1.6.4. Phối hợp các phương pháp

- Hạ tầng mật mã khóa công khai
- Kiểm soát lối vào ra.
- Kiểm soát và xử lý các lỗ hổng

1.1.7. Các kỹ thuật bảo đảm An toàn thông tin

- Kỹ thuật diệt trừ: Virut máy tính, chương trình trái phép.
- Kỹ thuật tường lửa: Ngăn chặn truy cập trái phép, lọc thông tin không hợp pháp
- Kỹ thuật mạng ảo riêng: tạo ra hành lang riêng cho thông tin "đi lại"
- Kỹ thuật mật mã: mã hóa, ký số, các giao thức mật mã, chống chối cãi
- Kỹ thuật giấu tin: che giấu thông tin trong môi trường dữ liệu khác
- Kỹ thuật thủy ký: bảo vệ bản quyền tài liệu số hóa
- Kỹ thuật truy tìm "dấu vết" kẻ trộm tin.

1.1.8. Các công nghệ bảo đảm an toàn thông tin

- Công nghệ chung: tường lửa, mạng riêng ảo…
- Công nghệ cụ thể: SSL, TLS…

1.2. MỘT SỐ PHƯƠNG PHÁP BẢO VỆ THÔNG TIN

1.2.1. Mã hóa dữ liệu

1.2.1.1. Tổng quan về mã hóa dữ liệu

1/.Khái niệm Mã hóa điện tử

- Để đảm bảo an toàn thông tin lưu trữ trên 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.

a/.Hệ mã hóa

- Việc mã hóa phải theo 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 khóa có thể.
- E là tập các hàm lập mã.
- D là tập các hàm giải mã.
- Với khóa lập mã ke $\in$ K, có hàm lập mã $e_{ke} \in E$, e_{ke}: P$\rightarrow$ C,
- Với khóa giải mã kd $\in$ K, có hàm giải mã $d_{kd} \in D$, d_{kd}: C$\rightarrow$P,
  Sao cho $d_{kd}(e_{ke}(x)) = x$, $\forall x \in P$.
- Ở đây x được gọi là bản rõ, $e_{ke}(x)$ được gọi là bản mã.

b/.Mã hóa và giải mã

Người gửi G $\rightarrow\rightarrow$ $e_{ke}(T)\rightarrow\rightarrow$Người nhận N
(có khóa lập mã ke)(có khóa giải mã kd)
$\uparrow$
Tin tặc có thể trộm bản mã $e_{ke}(T)$

- Người gửi G muốn gửi tin T cho người nhận N. Để bảo đảm bí mật, G mã hóa bản tin bằng khóa lập mã ke, nhận được bản mã $e_{ke}(T)$, sau đó gửi cho N. Tin tặc có thể trộm bản mã $e_{ke}(T)$ nhưng mà cũng "khó" hiểu được bản tin gốc T nếu không có khóa giải mã kd.
- Người nhận N nhận được bản mã, họ dùng khóa giải mã kd để giải mã eke(T) sẽ nhận được bản tin gốc $T=d_{kd}(e_{ke}(T))$.

2/.Phân loại hệ mã hóa

- Có 2 loại mã hóa chính: mã hóa khóa đối xứng và mã hóa khóa công khai.

a/.Hệ mã hóa khóa đối xứng (khóa bí mật)

- Mã hóa khóa đối xứng là hệ mã hóa mà biết được khóa lập mã thì có thể "dễ" tính được khóa giải mã và ngược lại. Đặc biệt một số Hệ mã hóa có khóa lập mã và khóa giải mã trùng nhau (ke=kd), như Hệ mã hóa "dịch chuyển" hay DES.
- Hệ mã hóa khóa đối xứng còn gọi là hệ mã hóa khóa bí mật, hay khóa riêng, vì phải giữ bí mật cả 2 khóa. Trước khi dùng Hệ mã hóa khóa đối xứng, người gửi và người nhận phải thỏa thuận thuật toán mã hóa và khóa chung, khóa phải được giữ bí mật. Độ an toàn của Hệ mã hóa loại này phụ thuộc vào khóa.

b/.Hệ mã hóa khóa công khai

- Hệ mã hóa khóa phi đối xứng là Hệ mã hóa có khóa lập mã và khóa giải mã khác nhau ($ke \neq kd$), biết được khóa này cũng khó tính được khóa kia. Hệ mã hóa này còn được gọi là hệ mã hóa công khai vì:
  - Khóa lập mã cho công khai, gọi là khóa công khai (Public key)
  - Khóa giải mã giữ bí mật, còn gọi là khóa riêng (Private key) hay khóa bí mật.
- Một người bất kỳ có thể dùng khóa công khai để mã hóa bản tin, nhưng chỉ người nào có đúng khóa giải mã thì mới có khả năng đọc được bản rõ.

1.2.1.2. Hệ mã hóa đối xứng – Cổ điển

Khái niệm

- Hệ mã hóa 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 Lantin.
- 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

1/. 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.

2/.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 cố 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.

3/.Hệ mã hóa AFFINE

Sơ đồ

- Đặt P = C = Z_{26}. Bản mã y và bản rõ x $\in$ Z_{26}.
- Tập khóa K = {(a,b), với a,b$\in$ Z_{26}, UCLN(a,26)=1}
- Với khóa k=(a,b)$\in$K, ta định nghĩa:
- Phép mã hóay=$e_k(x)$= (ax + b) mod 26
- Phép giải mãx=$d_k(y)$= a^{-1}(y-b) mod 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} mod 26, tức là thuật toán giải mã d_k luôn thực hiện được.
- Số lượng a$\in$ Z_{26} nguyên tố với 26 là ϕ(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 $\in$ Z_{26} là 26
- Số khóa (a,b) có thể là 12*26 = 312. Rất ít
- Như vậy việc dò tìm khóa mật khá dễ dàng.

4/.Hệ mã hóa VIGENRE

Sơ đồ:

- Đặt P =C=K=$(Z_{26})^m$, m là số nguyên dương, các phép toán thực hiện trong $(Z_{26})^m$.
- Bản mã Y và bản rõ X $\in$ $(Z_{26})^m$. Khóa k = $(k_1, k_2, \ldots, k_m)$ gồm m phầm tử.

Mã hóa Y = $(y_1, y_2, \ldots, y_m) = e_k(x_1, x_2, \ldots, x_m) = (x_1 + k_1, x_2 + k_2, \ldots, x_m + k_m) \bmod 26$

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

*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 này được gọi là thay thế đa biểu. Như vậy số khóa có thể có trong mật 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.

5/. 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 $\in$ Z_{26}.
- Tập khóa K là tập tất cả các hoán vị của {1, 2, …, m}
- Với mỗi khóa k = $\pi \in$ K, k = $(k_1, k_2, \ldots, k_m)$ gồm m phần tử, ta định nghĩa:
  - Mã hóa Y = $(y_1, y_2, \ldots, y_m) = e_k(x_1, x_2, \ldots, x_m) = (x_{k(1)}, x_{k(2)}, \ldots, x_{k(m)})$
  - Giải mã X = $(x_1, x_2, \ldots, x_m) = d_k(y_1, y_2, \ldots, y_m) = (y_{k(1)}^{-1}, y_{k(2)}^{-1}, \ldots, y_{k(m)}^{-1})$
- Trong đó $k^{-1} = \pi^{-1}$ 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

  $1! + 2! + 3! + \ldots + m!$ trong đó $m \leq 26$.
- Hiện nay với hệ mã này, người ta có phương pháp thám mã khác nhanh hơn.

6/. 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: $Y = (y_1, y_2, \ldots, y_m) = e_k(x_1, x_2, \ldots, x_m) = (x_1, x_2, \ldots, x_m) * k$
    - Hàm giải mã: $X = (x_1, x_2, \ldots, x_m) = d_k(y_1, y_2, \ldots, y_m) = (y_1, y_2, \ldots, y_m) * k^{-1}$

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.

1.2.1.3. Hệ mã hóa đối xứng DES

1/. Hệ mã hóa DES

a/. Giới thiệu

- 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 hệmật 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.

b/.Quy trình mã hóa theo DES

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

Chia thành

Giai doạn 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

2/. Lập mã và giải mã

a/. Lập mã

- 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) = $L_0 R_0$, trong đó L_0 là 32 bit đầu (Left), R_0 là 32 bit cuối (Right).

(IP(x) tách thành $L_0 R_0$).

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 26)

$k_1, k_2, \ldots, k_{16}$ 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.

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

b/.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.

3/. 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 $e_K(x) = y$.

1.2.1.4. Hệ mã hóa khóa công khai

1/. Hệ mã hóa RSA

Sơ đồ

- 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 $\phi(n) = (p-1).(q-1)$. Chọn khóa công khai b <$\phi(n)$, nguyên tố với $\phi(n)$.

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

Tập cặp khóa (bí mật, công khai) $K = \{(a, b)/ a, b \in Z_n, a*b \equiv 1 \pmod{\phi(n)}\}$.

Với bản rõ $x \in P$ và bản mã $y \in C$, định nghĩa:

- Hàm mã hóa: $y = e_k(x) = x^b \bmod n$
- Hàm giải mã: $x = d_k(x) = y^a \bmod n$

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 khóa 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

- 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 $g \in Z_p^*$. Đặt $P = Z_p^*$, $C = Z_p^* \times Z_p^*$.

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

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

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

Với bản rõ $x \in P$ và bản mã $y \in C$, với khóa $k \in K$ 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: $x = d_k(y_1, y_2) = y_2(y_1^a)^{-1} \bmod p$

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 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 như sau: 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 phải bài toán logarit rời rạc.

1.2.2. Chữ ký số

1.2.2.1. Tổng quan về chữ ký số

1./ Khái niệm về chữ ký số

a/.Giới thiệu

- Để chứng thực nguồn gốc hay hiệu lực của một tài liệu 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 hay hiệu lực của tài liệu này. 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 bit tài liệu cũng không thể là một xâu bít nhỏ đặt 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 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 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
- 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, người ta thường dùng "hàm băm" để tạo đại diện cho tài liệu, sau đó mới ký lên đại diện này.

b/.Sơ đồ chữ ký số

- Sơ đồ chữ ký là bộ năm (P, A, K, S, V), trong đó:
  - P là tập hữu hạn các văn bản 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 kiểm thử.
- Với mỗi khóa $k \in K$, có thuật toán ký $Sig_k \in S$, $Sig_k: P \rightarrow A$, có thuật toán kiểm tra chữ ký $Ver_k \in V$, $Ver_k: P \times A \rightarrow$ {đúng, sai}, thỏa mãn điều kiện sau $\forall x \in P$, $y \in A$:
  - $Ver_k(x,y) =$ Đúng, nếu $y = Sig_k(x)$; Sai, nếu $y \neq Sig_k(x)$

2/. Phân loại chữ ký số

Cách 1: Phân loại chữ ký theo đặc trưng kiểm tra chữ ký.

- Chữ ký khôi phục thông điệp: Là loại chữ ký, trong đó người gửi chỉ cần gửi "chữ ký", người nhận có thể khôi phục lại được thông điệp, đã được "ký" bởi "chữ ký" này.
- Chữ ký đi kèm thông điệp: Là loại chữ ký, trong đó người gửi chỉ cần gửi "chữ ký", phải gửi kèm cả thông điệp đã được ký bởi "chữ ký" này. Ngược lại, người nhận sẽ không có được thông điệp gốc

Cách 2: Phân loại chữ ký theo mức an toàn

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

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)

1.2.2.2. Chữ ký RSA

1/. Sơ đồ chữ ký

Sơ đồ

- *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 $\phi(n) = (p-1).(q-1)$. Chọn khóa công khai b <$\phi(n)$, nguyên tố với $\phi(n)$.

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

Tập cặp khóa (bí mật, công khai) $K = \{(a, b)/\ a, b \in Z_n, a*b \equiv 1 \pmod{\phi(n)}\}$.

- *Ký số*: chữ ký trên $x \in P$ là $y = Sig_k(x) = x^a \pmod n$, $y \in A$.
- *Kiểm tra chữ ký*: $Ver_k(x, y)$ = đúng $\Leftrightarrow$ $x \equiv y^b \pmod n$.

2/. Độ an toàn của chữ ký RSA

a/.Người gửi G gửi tài liệu x cùng chữ ký y đến người nhận N, có 2 cách xử lý:

Cách 1: Ký trước, mã hóa sau:

- G ký trước vào x bằng chữ ký $y = Sig_G(x)$, sau đó mã hóa x và y nhận được $z = e_G(x, y)$. G gửi z cho N.
- Nhận được z, N giải mã z để được x và y.
- Tiếp theo kiểm tra chữ ký $Ver_N(x, y)$ = true ?

Cách 2: Mã hóa trước, ký sau:

- G mã hóa trước x bằng u = $e_G(x)$, sau đó ký vào u bằng chữ ký v = $Sig_G(u)$.
- G gửi (u, v) cho N.
- Nhận được (u, v), N giải mã u được x.
- Tiếp theo kiểm tra chữ ký $Ver_N(u, v)$ = true ?

b/.Giả sử H lấy trộm được thông tin trên đường truyền từ G đến N.

- Trong trường hợp a, H lấy được z. Trong trường hợp b, H lấy được (u, v)
- Để tấn công x, trong cả hai trường hợp, H đều phải giải mã thông tin lấy được
- Để tấn công vào chữ ký, thay bằng chữ ký (giả mạo), thì xảy ra điều gì ?

- Trường hợp 1, để tấn công chữ ký y, H phải giải mã z, mới nhận được y.
- Trường hợp 2,để tấn công chữ ký v, H đã có sẵn v, H chỉ việc thay v bằng v'.
  H thay chữ ký v trên u, bằng chữ ký của H là v' = $Sig_H(u)$, gửi (u, v') đến N.
  Khi nhận được v', N kiểm thử thấy sai, gửi phản hồi lại G
  G có thể chứng minh chữ ký đó là giả mạo
  G gửi chữ ký đúng v cho N, nhưng quá trình truyền tin sẽ bị chậm lại

- Như vậy trong trường hợp 2, H có thể giả mạo chữ ký mà không cần giải mã.
- Vì thế có lời khuyên: Hãy ký trước, sau đó mã hóa các dữ liệu.

1.2.2.3. Chữ ký Elgamal

1/. Sơ đồ chữ ký Elgamal

Sơ đồ

- *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 $g \in Z_p^*$. Đặt $P = Z_p^*$, $A = Z_p^* \times Z_p^*$.

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

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

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 $y= Sig_k(x, r) = (\gamma, \delta)$, $y \in A$

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

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

- *Kiểm tra chữ ký:*

$Ver_k(x, \gamma, \delta)$ = đúng $\Leftrightarrow h^\gamma * \gamma^\delta \equiv g^x \bmod p$.

2/. Độ an toàn của chữ ký Elgamal

a/. Vấn đề giả mạo chữ ký Elgamal

Trường hợp 1: Giả mạo chữ ký không cùng với tài liệu được ký.

❖ H cố gắng giải mạo chữ ký trên x, mà không biết khóa bí mật a.

Như vậy, H phải tính được γ và δ.

- Nếu chọn trước γ, H phải tính δ qua đẳng thức $h^\gamma * \gamma^\delta \equiv g^x \bmod p$.

  Tức là $\gamma^\delta \equiv g^x h^{-\gamma} \bmod p$ hay $\delta \equiv \log_\gamma g^x h^{-\gamma} \bmod p$.

- Nếu chọn trước δ, H phải tính γ qua phương trình: $h^\gamma * \gamma^\delta \equiv g^x \bmod p$.

- Hiện nay chưa có cánh hữu hiệu 2 trường hợp trên, nhưng phỏng đoán là khó hơn bài toán logarit rời rạc.
- Có thể có cách tính γ, δ đồng thời với (γ, δ) là chữ ký ? chưa có trả lời rõ.

- Nếu chọn trước γ, δ, sau đó tính x, H phải đối đầu với bài toán logarit rời rạc.

  Ta có $h^\gamma * \gamma^\delta \equiv g^x \bmod p$.

  Như vậy $x \equiv \log_g g^x \equiv \log_g h^\gamma * \gamma^\delta$

Trường hợp 2: Giả mạo chữ ký cùng với tài liệu được ký.

❖ H có thể ký trên tài liệu ngẫu nhiên bàng cách chọn trước đồng thời x, γ, δ.

Cách 1:

- Chọn x, γ, δ thỏa mãn điều kiện thử như sau:
- Chọn các số nguyên i, j sao cho $0 \leq i, j \leq (p-2)$, $(j, p-1) = 1$ và tính:

$\gamma = g^i h^j \bmod p$, $\delta = -\gamma j^{-1} \bmod (p-1)$, $x = -\gamma i j^{-1} \bmod (p-1)$.

- Trong đó j^{-1} được tính theo mod (p-1) (nghĩa là j nguyên tố với p-1).
- Chứng minh (γ, δ) là chữ ký trên x, bằng cách kiểm tra điều kiện kiểm thử:

$h^\gamma * \gamma^\delta \equiv h^\gamma (g^i h^j)^{-\gamma j^{-1}} \bmod p \equiv h^\gamma g^{-\gamma i j^{-1}} h^{-\gamma} \bmod p \equiv g^x \bmod p$

Cách 2:

- Nếu (γ, δ) là chữ ký trên tài liệu x có từ trước, thì có thể giả mạo chữ ký trên tài liệu x' khác.
- Chọn số nguyên k, i, j thỏa mãn $0 \leq k, i, j \leq (p-2)$, $(k\gamma - j\delta, p-1)=1$ và tính:

$\lambda = \gamma^k g^i h^j \bmod p, \mu = \delta\lambda (k\gamma - j\delta)^{-1} \bmod (p-1)$,

$x' = \lambda (kx + i\delta) (k\gamma - j\delta)^{-1} \bmod (p-1)$,

- (λ, μ) là chữ ký trên x', vì thỏa mãn điều kiện kiểm thử:

$h^\lambda \lambda^m \equiv g^{x'} \bmod p$.

b/.Vấn đề phá khóa theo sơ đồ

❖ Khóa bí mật a có thể bị phát hiện, nếu việc ký không thận trọng. Ví dụ trong các trường hợp: khóa ngẫu nhiên r bị lộ, hoặc dùng r cho hai lần ký khác nhau.

Trường hợp 1: số ngẫu nhiên r bị lộ

- Nếu r bị lộ, thám mã sẽ được tính khóa mật a = $(x - r\,\delta)\,\gamma^{-1} \bmod (p-1)$

Trường hợp 2: Dùng r cho hai lần ký khác nhau:

- Giả sử dùng r cho 2 lần ký trên x1 và x2

(γ, δ_1) là chữ ký trên x_1, (γ, δ_2) là chữ ký trên x_2,

- Khi đó thám mã có thể tính a như sau:

$h^{\gamma} * \gamma^{\delta_1} \equiv g^{x_1} \bmod p.$ $\quad h^{\gamma} * \gamma^{\delta_2} \equiv g^{x_2} \bmod p.$

- Do đó ta có : $g^{x_1-x_2} \equiv \gamma^{\delta_1-\delta_2} \bmod p$

  Đặt $\gamma = g^r$ ta có : $g^{x_1-x_2} \equiv \gamma^{r*(\delta_1-\delta_2)} \bmod p$

  Tương đương với $x_1-x_2 \equiv r * (\delta_1 - \delta_2) \bmod (p-1)$ (1)

  Đặt $d = (\delta_1 - \delta_2, p-1)$. Khi đó $d \mid (p-1)$, $d \mid (\delta_1 - \delta_2) \Rightarrow d \mid (x_1-x_2)$

$$x' = \frac{x_1-x_2}{d}$$

$$\delta' = \frac{\delta_1-\delta_2}{d}$$

$$x' = \frac{p-1}{d}$$

- Khi đó đồng dư thức (1) trở thành : $x' \equiv r * \delta' \bmod p'$
- Vì $(\delta', p') = 1$ nên tính $\varepsilon = (\delta')^{-1} \bmod p'$ và tính $r = x' * \varepsilon \bmod p'$

$\Rightarrow r = x' * \varepsilon + i * p' \bmod (p-1)$, Với i là giá trị nào đó $0 \le i \le d-1$.

- Thử với giá trị đó, ta tìm được r (điều kiện thử để xác định r là $\gamma = \alpha^r \bmod p$).
- Tiếp theo sẽ tính được a như trường hợp 1

1.2.2.4. Chữ ký DSS

1/. Sơ đồ chữ ký DSS

a/. Giới thiệu chuẩn chữ ký số DSS

- Chuẩn chữ ký số (DSS: Digital Signature Standard) được đề xuất năm 1991, là cải biên của sơ đồ chữ ký Elgamal, và được chấp nhận là chuẩn năm 1994 để dùng trong một số lĩnh vực giao dịch ở USA.
- Thông thường tài liệu số được mã hóa và giải mã 1 lần. Nhưng chữ ký lại liên quan tới pháp luật, chữ ký có thể phải kiểm thử sau nhiều năm đã ký. Do đó chữ ký phải được bảo vệ cẩn thận. Như vậy số nguyên tố p phải đủ lớn (chẳng hạn dài cỡ 512 bit) để đảm bảo an toàn, nhiều người đề nghị nó phải dài 1024 bit. Tuy nhiên, độ dài chữ ký theo sơ đồ Elgamal là gấp đôi số bit của p, do đó nếu p dài 512 bit thì độ dài chữ ký là 1024 bit.
- Trong ứng dụng dùng thẻ thông minh (Smart card) lại mong muốn có chữ ký ngắn, nên giải pháp sửa đổi là một mặt dùng p với độ dài từ 512 bít đến 1024 bit mặt khác trong chữ ký (γ, δ), các số γ, δ có độ dài biểu diễn ngắn
- Điều này được thực hiện bằng cách dùng nhóm con cyclic Z_q^* của Z_p^* thay cho Z_p^*, do đó mọi tính toán được thực hiện trong Z_p^*, nhưng thành phần chữ ký lại thuộc Z_q^*.
- Thay đổi công thức tính δ trong sơ đồ ký Elgamal thành $\delta = (x + a * \gamma)\, r^{-1} \bmod q$. Điều kiện kiểm thử là: $h^{\gamma} * \gamma^{\delta} \equiv g^{x} \bmod p$ được sửa thành

  $\alpha^{x*\delta^{-1}} * h^{\gamma*\delta^{-1}} \equiv y \bmod p$

  Nếu $(x + g * \gamma, p-1) = 1$ thì $\delta^{-1} \bmod p$ tồn tại.

b/. Sơ đồ chuẩn chữ ký số DSS

Sơ đồ

- *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 q là ước nguyên tố của p-1. Tức là p-1 =t * q hay p = t * q + 1

- Chọn g $\in Z_p^*$ là căn bậc q của 1 mod p (g là phần tử sinh của Z_p^*)

Tính $\alpha = g^t$, chọn khóa bí mật a$\in Z_p^*$, tính khóa công khai $h \equiv \alpha^a \bmod p$.

- Đặt $P = Z_q^*$, $A = Z_q^* \times Z_q^*$, $K = \{(p, q, \alpha, a, h)/ a \in Z_p^*, h \equiv \alpha^a \bmod p\}$.
- Với mỗi khóa (p, q, α, a, h), k' = a bí mật, k''= (p, q, α, h) công khai.

- *Ký số*: Dùng 2 khóa ký: khóa a và khóa ngẫu nhiên bí mật r $\in Z_q^*$

  Chữ ký trên x$\in Z_p^*$ là $Sig_{k'}(x, r) = (\gamma, \delta)$.

  Trong đó $\gamma = (\alpha^r \bmod p) \bmod q$, $\delta = (x + a * \gamma) * r^{-1} \bmod q$

- *Kiểm tra chữ ký:*

  Với $e_1 = x * \delta^{-1} \bmod q$, $e_2 = \gamma * \delta^{-1} \bmod q$.

  $Ver_{k''}(x, \gamma, \delta)$ = đúng $\Leftrightarrow (\alpha^{e_1} * h^{e_2} \bmod p) \bmod q = \gamma$.

1.2.2.5. Chữ ký không thể phủ định

1/. Sơ đồ chữ ký

a/. Giới thiệu chữ ký không thể phủ định

- Trong phần trước ta đã trình bày một số sơ đồ chữ ký điện tử. Trong các sơ đồ đó, việc kiểm thử tính đúng đắn của chữ ký là do người nhận thực hiện. Nhằm tránh việc nhân bản chữ ký để sử dụng nhiều lần, tốt nhất là để 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.
- Giả sử tài liệu cùng chữ ký từ G gửi đến N. Khi N yêu cầu G cùng kiểm thử chữ ký, thì một vấn đề nảy sinh là làm sao để ngăn cản G chối bỏ một chữ ký mà anh ta đã ký, G có thể tuyên bố rằng chữ ký đó là giả mạo?
- Để giải quyết tình huống trên, cần có thêm giao thức chối bỏ, bằng giao thức này, G có thể chứng minh một chữ ký là giả mạo. Nếu G từ chối tham gia vào giao thức đó, thì có thể xem rằng G không chứng minh được chữ ký đó là giả mạo
- Như vậy sơ đồ chữ ký không phủ định được gồm 3 phần: một thuật toán ký, một giao thức kiểm thử, và một giao thức chối bỏ.

b/. Sơ đồ chữ ký không thể phủ định

❖ **Chuẩn bị các tham số**

- Chọn số nguyên tố p sao cho bài toán rời rạc trong Z_p là khó

  p = 2*q+1, q cũng là số nguyên tố.

- Gọi P là nhóm nhân con của Zp* theo q (P gồm các thặng dư bậc 2 theo mod p).
- Chọn phần tử sinh g của nhóm P cấp q.

Đặt P = A, K = {(p, q, a, h)/ a$\in$ Z_q^*, h $\equiv$ g^a mod p}.

❖ **Thuật toán ký**

- Dùng khóa bí mật k' = a để ký lên x:

Chữ ký là y = $Sig_{k'}$ (x) = x^a mod p.

❖ **Giao thức kiểm thử**

- Dùng khóa công khai k'' = (p, g, h)
- Với x, y $\in$ P người nhận N cùng người gửi G thực hiện giao thức kiểm thử:

B1: N chọn ngẫu nhiên e_1 , $e_2\in$ Z_q^*

B2: N tính c = $y^{e_1}h^{e_2}$mod p, và gửi cho G.

B3: G tính d = $c^{a^{-1}\bmod q}$ mod p và gửi cho N.

B4: N chấp nhận y là chữ ký đúng nếu d $\equiv y^{e_1}g^{e_2}$mod p

❖ **Giao thức chối bỏ**

B1: N chọn ngẫu nhiên e_1 , $e_2\in$ Z_q^*

B2: N tính c = $y^{e_1}h^{e_2}$mod p, và gửi cho G.

B3: G tính d = $c^{a^{-1}\bmod q}$ mod p và gửi cho N.

B4: N thử điều kiện d $\neq$ $x^{e_1}g^{e_2}$mod p.

B5: N chọn ngẫu nhiên f_1 , $f_2\in Z_q^*$

B6: N tính C = $\gamma^{f_1}\beta^{f_2}$mod p, và gửi cho G.

B7: G tính D = $C^{\alpha^{-1}\bmod q}$mod p và gửi cho N.

B8: N thử điều kiện D $\neq$ $x^{f_1}g^{f_2}$mod p.

B9: N kết luận y là chữ ký giả mạo nếu:

$(d * \alpha^{-e_2})^{f_1} \equiv (D * \alpha^{-f_2})^{e_1}$ mod p (thay α bằng g)

1.2.2.6. Đại diện tài liệu và hàm băm

1/. Vấn đề đại diện tài liệu và hàm băm

a/. Một số vấn đề với chữ ký số

Vấn đề 1:

- "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. Một số chữ ký trên bản tin có kích thước gấp đôi bản tin gốc. Ví dụ khi dùng sơ đồ chữ ký DSS để ký vào bản tin có kích thước 160bit, thì chữ ký số này sẽ có kích thước 320bit.
- Trong khi đó trên thực tế, ta cần phải ký vào các bản tin có kích thước rất lớn, ví dụ dài vài chục MegaByte (tương ứng với hàng ngàn trang in trên giấy). Như vậy phải tốn nhiều bộ nhớ để lưu trữ "chữ ký", mặt khác tốn nhiều thời gian để truyền "chữ ký" trên mạng.

Vấn đề 2:

- Với một số sơ đồ chữ ký an toàn, thì tốc độ ký lại chậm vì chúng dùng nhiều phép tính số học phức tạp như số mũ modulo.

Vấn đề 3:

- Thực tế có thể xảy ra trường hợp: Với nhiều bản tin đầu vào khác nhau, sử dụng hệ mã hóa hay sơ đồ ký số giống nhau (có thể khác nhau), nhưng lại cho ra bản mã hay chữ ký giống nhau (đó là ánh xạ nhiều – một). Điều này sẽ dẫn đến phức tạp cho việc xác thực thông tin.

b/. Cách giải quyết vấn đề trên

Cách 1:

- Một cách đơn giản để giải quyết các vấn đề trên với thông điệp có kích thước lớn là "chặt" bản tin thành nhiều bản nhỏ, sau đó ký lên các đoạn có độc lập với nhau. Nhưng biện pháp này gặp các vấn đề trên.
- Hơn thế nữa còn gặp vấn đề ngiêm trọng hơn. Đó là kết quả sau khi ký, nội dung của thông điệp có thể bị xáo trộn các đoạn với nhau, hoặc một số đoạn trong chúng có thể mất mát. Ta cần bảo vệ tính toàn vẹn của bản tin gốc.

Cách 2:

- Thay vì phải 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.
- Các tài liệu có thể dưới dạng văn bản, hình ảnh, âm thanh, …và kích thước của chúng tùy ý, qua các thuật toán băm như: MD4, MD5, SHA, các đại diện tương ứng của chúng có kích thước cố định như 128 bit với dòng MD, 160 bít với dòng SHA.
- "Đại diện" của tài liệu chính là giá trị của "hàm băm" trên tài liệu, nó còn được gọi là "tóm lược" hay "bản thu gọn" của tài liệu.
- Với mỗi tài liệu (đầu vào), qua hàm băm chỉ có thể tính ra được một "đại diện"-giá trị băm tương ứng – duy nhất. "Đại diện" của tài liệu được xem là đặc thù của tài liệu (thông điệp), giống như dấu vân tay của mỗi người.
- Trên thực tế, hai tài liệu khác nhau có hai đại diện khác nhau. Như vậy khi đã có đại diện duy nhất cho một tài liệu, thì việc ký vào tài liệu, được thay bằng ký vào đại diện của nó là hòa toàn hợp lý. Đó là chưa kể việc tiết kiệm bao nhiêu thời gian cho việc "ký số", bộ nhớ lưu giữ chữ ký, thời gian truyền chữ ký trên mạng, …
- Cơ chế gửi tài liệu cùng chữ ký trên nó sử dụng hàm băm.

2/. Tổng quan về hàm băm

a/. Hàm băm

❖ *Khái niệm hàm băm*

- Hàm băm là thuật toán không dùng khóa để mã hóa nó có nhiệm vụ lọc tài liệu và cho kết quả là một giá trị băm có kích thước cố định, còn gọi là đại diện tài liệu hay đại diện bản tin, đại diện thông điệp.
- Hàm băm là hàm một chiều, theo nghĩa giá trị của hàm băm là duy nhất, và từ giá trị băm này, khó thể suy ngược lại được nội dung hay độ dài ban đầu của tài liệu gốc.

❖ *Đặc tính của hàm băm*

✓ Hàm băm h là hàm một chiều (one way Hash) với các đặc tính sau;

- Với tài liệu đầu vào (bản tin gốc) x, chỉ thu được giá trị băm duy nhất z = h (x).
- Nếu dữ liệu trong bản tin x bị thay đổi hay bị xóa để thành bản tin x', thì giá trị băm $h(x') \neq h(x)$.

  Cho dù chỉ là một sự thay đổi nhỏ, ví dụ chỉ thay đổi 1 bit dữ liệu của bản tin gốc x, thì giá trị băm h(x) của nó cũng vẫn thay đổi. Điều này có nghĩa là hai thông điệp khác nhau thì giá trị băm của chúng cũng khác nhau.
- Nội dung của bản tin gốc khó có thể suy ra từ giá trị hàm băm của nó. Nghĩa là với thông điệp x thì dễ tính được z= h(x), nhưng lại khó tính ngược lại được x nếu chỉ biết giá trị băm h(x).

❖ *Ứng dụng của hàm băm*

- Với bản tin dài x, thì chữ ký trên x cũng sẽ dài, như vậy tốn thời gian ký tốn bộ nhớ lưu giữ chữ ký, tốn thời gian truyền chữ ký trên mạng.

  Người ta dùng hàm băm h để tạo đại diện bản tin z = h(x), nó có độ dài ngắn. Sau đó ký trên z, như vậy chữ ký trên z sẽ nhỏ hơn rất nhiều so với chữ ký trên bản tin gốc
- Hàm băm dùng để xác định tính toàn vẹn dữ liệu.
- Hàm băm dùng để bảo mật một số dữ liệu đặc biệt, ví dụ bảo vệ mật khẩu, bảo vệ khóa mật mã, …

b/. Các tính chất của hàm băm

Tính chất 1: Hàm băm h là không va chạm yếu

- Hàm băm h được gọi là không va chạm yếu, nếu cho trước bức điện x, khó thể tính toán tìm ra bức điện x' ≠ x mà h(x') = h(x).

Tính chất 2: Hàm băm h là không va chạm mạnh

- Hàm băm h được gọi là không va chạm mạnh nếu khó thể tính toán để tìm ra hai bức thông điệp khác nhau x' và x (x' ≠ x) mà h(x') = h(x).

Tính chất 3: Hàm băm h là hàm một chiều

- Hàm băm h được gọi là hàm một chiều nếu khi cho trước một bản tóm lược thông báo z thì khó thể tính toán để tìm ra thông điệp ban đầu x sao cho h(x) = z

c/. Các hàm băm

- Các hàm băm dòng MD (MD2, MD4, MD5) do Rivest đề xuất. Gí trị băm theo các thuật toán này có độ dài cố định là 128 bit. Hàm băm MD4 được đưa ra vào năm 1990. Một năm sau phiên bản mạnh hơn là MD5 cũng được đề xuất.
- Hàm băm an toàn SHA, phức tạp hơn nhiều, cũng dựa trên các phương pháp tương tự, được công bố trong hồ sơ liên bang năm 1992 và được chấp nhận làm tiêu chuẩn vào năm 1993 do Viện Tiêu Chuẩn và Công Nghệ Quốc Gia (NIST). Giá trị băm theo thuật toán này có độ dài cố định là 160bit.

1.2.3. Ẩn giấu tin

1.2.3.1. Tổng quan về ẩn giấu tin

1/.Khái niệm

- "Ẩn giấu tin" được hiểu là nhúng mẩu tin mật vào một vật mang tin khác, sao cho mắt thường khó pháp hiện ra mẩu tin mật đó, mặt khác khó nhận biết được vật mang tin đã được giấu một tin mật.

2/. Các thành phần của hệ ẩn giấu tin

Các thành phần chính của một hệ "Ẩn giấu tin" trong ảnh gồm có:

- Mẩu tin mật: có thể là văn bản, hình ảnh hay tệp tin tùy ý(audio, video …), vì trong quá trình giấu tin chúng đều được chuyển thành chuỗi các bit.
- Môi trường sẽ chứa tin mật: Thường là ảnh, nên gọi là ảnh phủ hay ảnh gốc
- Khóa K: khóa viết mật, tham gia vào quá trình giấu tin để tăng tính bảo mật.
- Môi trường đã chứa tin mật: Thường là ảnh, nên gọi là ảnh mang, là ảnh sau khi đã nhúng tin mật vào.

3/. Ẩn giấu tin và mật mã

- Có thể xem Ẩn giấu tin là một nhánh của ngành mật mã với mục tiêu là nghiên cứu các phương pháp che giấu thông tin mật.
- Ẩn giấu tin và mã hóa tuy cùng có mục đích là để đối phương "khó" phát hiện ra tin cần giấu, tuy nhiên nó khác với mã hóa ở chỗ:

+ Mã hóa là giấu đi ý nghĩa của thông tin.
+ Ẩn giấu tin là giấu đi sự hiện diện của thông tin.

4/. Phân loại Ẩn giấu tin

a/. Giấu tin(Steganography) là kỹ thuật nhúng mẩu tin mật vào môi trường giấu tin.

- Giấu tin có xử lý là một dạng giấu tin, trong đó để tăng bảo mật, có thể phải dùng khóa viết mật. Để giải mã, người ta cũng phải có khóa viết mật đó.

+ Khóa viết mật không phải dùng để mã hóa mẩu tin, nó có thể là khóa dùng để sinh ra "hàm băm", phục vụ rải tin mật vào môi trường giấu tin.

- Giấu tin đơn thuần: là một dạng giấu tin trong đó không dùng khóa viết mật để giấu tin, tức là chỉ giấu tin đơn thuần vào môi trường giấu tin.

b/. Thủy vân số (watermarking) là kỹ thuật nhúng dấu ấn số vào một tài liệu số nhằm chứng thực nguồn gốc hay chủ sở hữu của tài liệu số này.

- Tạm gọi thủy vân số là ẩn tin để phân biệt với giấu tin

+ Dấu vân tay là một dạng thủy ấn số trong đó dấu ấn là một định danh duy nhất.

c/. So sánh "ẩn tin" và "giấu tin"

- Về mặt hình thức, ẩn tin giống giấu tin ở chỗ đều tìm cách nhúng thông tin vào một môi trường.
- Về mặt nội dung, ẩn tin có điểm khác so với giấu tin.

• Về mục tiêu:

+ Mục tiêu của ẩn tin là nhúng mẩu tin thường là biểu tượng, chữ ký, dấu nhỏ đặc trưng vào môi trường phủ, nhằm phục vụ việc chứng thực bản quyền tài liệu. Như vậy mẩu tin cần nhúng không nhất thiết phải là bí mật, nhiều khi cần lộ ra cho mọi người biết để mà dè chừng.

+ Ẩn tin có thể vô hình hoặc hữu hình trên vật mang tin. Ẩn tin tìm cách biến tin giấu thành một thuộc tính của vật mang tin. Mục đích của ẩn tin là bảo vệ môi trường giấu tin.

+ Mục tiêu của giấu tin: là nhúng mẩu tin thường là bí mật, vào môi trường phủ, sau đó có thể lấy ra tin mật từ môi trường phủ.

+ Giấu tin không cho phép nhìn thấy tin giấu trên vật mang tin. Mục đính của giấu tin là bảo vệ tin được giấu.

• Về đánh giá hiệu quả:

+ Chỉ tiêu quan trọng nhất của ẩn tin là tính bền vững của tin được giấu.

+ Chỉ tiêu quan trọng nhất của giấu tin là dung lượng của tin được giấu.

5/. Các tính chất của Ẩn giấu tin

a/. Bảo đảm tính "vô hình"

- Ẩn giấu tin trong ảnh sẽ làm biến đổi ảnh mang tin. Tính vô hình thể hiện mức độ biến đổi ảnh mang. Phương pháp ẩn giấu tin tốt sẽ làm cho thông tin mật trở lên vô hình trên ảnh mang, người dùng khó thể nhận ra trong ảnh có ẩn chứa thông tin mật.
- Với ẩn tin thì trong thực tế không phải khi nào cũng cố gắng để đạt được tính vô hình cao nhất, ví dụ trong truyền hình, người ta gắn hình ảnh mờ gọi là thủy ấn để bảo vệ bản quyền bản tin.

b/. Khả năng chống giả mạo

- Mục đích của giấu tin là để truyền đi thông tin mật. Nếu không thể do thám tin mật, thì kẻ địch cũng cố tìm cách làm sai lạc tin mật, làm giả mạo tin mật để gây bất lợi cho đối phương. Phương pháp "Giấu tin" tốt phải đảm bảo tin mật không bị tấn công một cách chủ động trên cơ sở những hiểu biết về thuật toán nhúng tin và có ảnh mang
- Đối với ẩn tin thì khả năng chống giả mạo là yêu cầu vô cùng quan trọng, vì có như vậy mới bảo vệ được bản quyền, minh chứng tính pháp lý của sản phẩm.

c/. Dung lượng giấu

- Dung lượng giấu được tính bằng tỷ lệ của lượng tin cần giấu so với kích thước ảnh mang tin. Các phương pháp đều cố gắng giấu được nhiều tin trong ảnh nhưng vẫn giữ được bí mật. Tuy nhiên trong thực tế người ta luôn phải cân nhắc giữa dung lượng và các chỉ tiêu khác như tính vô hình, tính bền vững.

d/. Tính bền vững

- Sau khi ẩn giấu tin vào ảnh mang, bản thân ảnh mang có thể phải qua các biến đổi khác nhau như lọc ảnh, thêm nhiễu, làm sắc nét, mờ nhạt, quay, nén mất dữ liệu,… Tính bền vững là thước đo sự nguyên vẹn của tin mật sau những biến đổi như vậy.

e/. Độ phức tạp tính toán

- Độ phức tạp của của thuật toán ẩn giấu tin và giải tin cũng là một chỉ tiêu quan trọng để đánh giá một phương pháp ẩn giấu tin trong ảnh. Chỉ tiêu này cho chúng ta biết tài nguyên (thời gian và bộ nhớ) tốn bao nhiêu dùng cho một phương pháp ẩn giấu tin.
- Với chủ nhân ẩn giấu tin thì thời gian thực hiện phải nhanh, nhưng kẻ thám tin thì tách tin phải là bài toán khó.

6/. Các ứng dụng của ẩn giấu tin

a/. Liên lạc bí mật

- Bản mã của tin mật có thể gây ra sự chú ý của tin tặc, nhưng tin mật được giấu vào trong môi trường nào đó, rồi gửi đi trên mạng máy tính, thì ít gây ra sự chú ý của tin tặc. Đó là một ứng dụng của giấu tin.
- Hiện nay người ta phối hợp đồng thời nhiều giải pháp để truyền tin mật trên mạng công khai: Đầu tiên tin mật được nén tin, sau đó mã hóa bản tin nén, cuối cùng giấu bản mã vào môi trường nào đó.

b/. Bảo vệ bản quyền

- ***Thủy vân (Watermark):***

- Một biểu tượng bí mật gọi là thủy ấn được nhúng vào trong một tài liệu để xác nhận quyền sở hữu về tài liệu.
- "Thủy vân" được đính lên tranh ảnh khi bán hoặc phân phối, thêm vào đó có thể gán một nhãn thời gian để chống giả mạo.
- "Thủy vân" cũng được dùng để phát hiện xem các ảnh có bị sửa đổi hay không. Việc phát hiện "Thủy vân" được thực hiện bằng thống kê, so sánh độ tương quan hoặc bằng cách đo đạc xác định chất lượng của "Thủy vân" trong ảnh mang.

- ***Điểm chỉ số:*** Điểm chỉ số tương tự như số Seri của phần mềm

- "Điểm chỉ số" dùng để chuyển thông tin về người nhận "sản phẩm số" nhằm chứng thực bản sao duy nhất của sản phẩm.

- ***Gán nhãn***

- Tiêu đề, chú giải, nhãn thời gian … có thể được nhúng vào sản phẩm số. Gắn tên người lên ảnh của họ, gắn tên địa phương lên bản đồ. Khi đó nếu sao chép ảnh thì cũng sao chép cả thông tin đã nhúng vào nó. Chủ sở hữu của sản phẩm, người có "khóa biết mật" có thể tách ra và xem các chú giải.
- Trong một cơ sở dữ liệu ảnh, người ta có thể nhúng các từ khóa, để các động cơ tìm kiếm có thể tìm nhanh một bức ảnh nào đó. Nếu là một khung ảnh cho cả một đoạn phim, người ta có thể gán cả thời điểm diễn ra sự kiện để đồng bộ hình ảnh với âm thanh. Người ta cũng có thể gán số lần mà hình ảnh được xem, để tính tiền thanh toán.

7/. Một số chương trình ẩn giấu tin

- Chương trình Hide and Seek v4.1: Chương trình chạy dưới hệ điều hành DOS để giấu tin vào các ảnh GIF. Nó thực hiện giấu tin một cách ngẫu nhiên, do đó nếu lượng tin cần giấu nhỏ thì tin sẽ được rải đều khắp ảnh mang. Nếu lượng tin nhiều, thì các vùng thay đổi dầy hơn, vì vậy dễ bị phát hiện.
- Chương trình StegoDos: Chương trình chạy dưới hệ điều hành DOS, sử dụng ảnh mang 320×200 điểm ảnh và 256 mầu.
- Chương trình While Noise Storm: Chương trình này dễ dùng hơn và nhúng được nhiều tin hơn các chương trình trước. Ảnh mang không cần có kích thước cố định, tính vô hình cao.
- Chương trình S-Tools for Windows: là một chương trình giấu ảnh tốt. Có thể giấu tin trong ảnh BMP,GIF, tệp âm thanh WAV, các vùng chưa dùng đến của đĩa mềm. Giao diện đồ họa kéo thả. Để giấu tin chỉ cần kéo biểu tượng tệp tin cần giấu và thả lên ảnh

1.2.3.2. Phương pháp giấu tin trong ảnh

1/. Giấu tin trong ảnh đen trắng

- Ảnh đen trắng số được thể hiện là một ma trận điểm ảnh gồm số 0 hay 1.Giấu tin trong ảnh đen trắng là việc khó khăn, vì dễ bị nhận biết bằng mất thường. Số lượng tin giấu là hạn chế. Tuy nhiên ảnh đen trắng ngày càng ít được dùng, do đó việc nghiên cứu giấu tin trong loại ảnh này là ít thực tế

a/. Thuật toán giấu tin sử dụng tính chẵn lẻ của tổng số bit 1

- **Ý tưởng**

- Chia ảnh mang thành các khối nhỏ. Mỗi khối nhỏ sẽ được gài 1 bit của tin cần giấu. Dựa vào tính chẵn lẻ của tổng số các bit 1 trong khối để quy định giấu bit 1 hay bit 0. Cụ thể là sau khi giấu, thì tổng số các bit 1 trong khối và bit cần giấu sẽ có cùng tính chẵn lẻ.

- **Thuật toán giấu tin**

- Input: FF là file ảnh bitmap đen trắng (sẽ mang tin giấu), Fb là file tin cần giấu, K là khóa bí mật, đó là kích thước của khối nhỏ sẽ được tách từ FF.
- Output: FF^* là file ảnh đã được giấu file tin mật Fb.

Bước 1: Tiền xử lý

- Chuyển file cần giấu Fb sang xâu bit nhị phân b.
- Đọc Header của ảnh, đọc bảng màu, để lấy thông tin về ảnh.
  Đọc phần dữ liệu ảnh vào mảng 2 chiều (ma trận) F.

Bước 2: Giấu tin

- Input: F là ma trận mang ảnh, b là dãy bit bí mật cần giấu,
  K là khóa bí mật, đó là kích thước của khối nhỏ (được xác định trước)
- Output: F^* là ma trận ảnh đã được giấu dãy bit bí mật b.

B1: Chia ảnh mang F thành các khối nhỏ với kích thước K

B2: Theo một thứ tự xác định trước, xét từng khối nhỏ:

+ Nếu muốn giấu bit 1 vào một khối thì phải thỏa mãn điều kiện:
  (L): Tổng số các bit 1 trong khối đó là số lẻ.
+ Nếu muốn giấu bit 1 vào một khối, nhưng không thỏa mãn điều kiện (L), thì trong khối đó chọn ngẫu nhiên một bit và thay đổi giá trị của nó (từ 0 đổi sang 1 hay từ 1 đổi sang 0). Bằng cách đó, khối mang tin sẽ thỏa mãn điều kiện (L).
+ Nếu muốn giấu bít 0 vào một khối thì phải thỏa mãn điều kiện:
  (C): Tổng số các bit 1 trong khối đó là số chẵn.
+ Nếu muốn giấu bit 1 vào một khối, nhưng không thỏa mãn điều kiện (C), thì trong khối đó chọn ngẫu nhiên một bit và thay đổi giá trị của nó (từ 0 đổi sang 1 hay từ 1 đổi sang 0). Bằng cách đó, khối mang tin sẽ thỏa mãn điều kiện (C).

- **Thuật toán tách tin giấu**

- Input: F^* là ảnh đã được giấu dãy bit bí mật b.
  K là khóa bí mật, đó là kích thước của khối nhỏ (được xác định trước).
- Output: F là ảnh mang(ảnh trước khi giấu tin mật),b là dãy bit bí mật cần giấu.

B0: Đọc Header của ảnh, đọc bảng màu để lấy thông tin về ảnh.

Đọc phần dữ liệu ảnh vào mảng 2 chiều (ma trận) F.

B1: Chia ảnh F mang thành các khối nhỏ với kích thước K

B2: Theo một thứ tự xác định trước, xét từng khối nhỏ:

+ Nếu tổng số bit 1 là lẻ thì ta thu được bit giấu là 1.
+ Nếu tổng số bit 1 là chẵn thì ta thu được bit giấu là 0.

2/. Giấu tin trong ảnh màu

a/. Các yêu cầu kỹ thuật

- Chất lượng ảnh mang vẫn đảm bảo, tin giấu không nhìn được bằng mắt thường.
- Tin giấu phải được mã hóa trực tiếp vào ảnh mang, chứ không phải vào phần khác, như vậy mới giữ được cho nhiều dạng tệp ảnh khác nhau.
- Tin giấu phải bền vững với các sửa đổi và tấn công từ bên ngoài
- Đảm bảo toàn vẹn dữ liệu, vì điều khó tránh khỏi là tin giấu cũng sẽ bị thay đổi, nếu biến đổi ảnh mang.
- Chú ý các phương pháp giấu tin cho phép phục hồi tin giấu không cần ảnh gốc.

b/. Phương pháp giấu tin trong ảnh màu

- **Phân nhóm phương pháp giấu tin theo kỹ thuật**

- Giấu tin mật vào các "bit có trọng số thấp" của ảnh: hay được áp dụng trên các ảnh Bitmap không nén và cá ảnh dùng bảng màu (như GIF, TIF). Ý tưởng chính của phương pháp này là lấy từng bit của mẩu tin mật, rải nó lên ảnh mang, gài vào các bít có trọng số thấp.
- Giấu tin dựa vào kỹ thuật biến đổi ảnh: lợi dụng việc biến đổi ảnh từ miền biểu diễn này sang miền biểu diễn khác để giấu các bit tin mật.
- Giấu tin sử dụng mặt nạ giác quan: dựa trên nguyên lý đánh lừa hệ thống giác quan con người.

- **Phân nhóm phương pháp giấu tin theo định dạng ảnh**

- Nhóm phương pháp phụ thuộc định dạng ảnh: Thông tin giấu dễ bị tổn thương bởi các phép biến đổi.
- Nhóm phương pháp độc lập với định dạng ảnh: lợi dụng vào việc biến đổi ảnh để giấu tin vào trong đó.
    - Một số phép biến đổi ảnh

+ Phương pháp biến đổi theo miền không gian.
+ Phương pháp biến đổi theo miền tần số.
+ Phương pháp biến đổi hình học.

- **Phân nhóm phương pháp giấu tin theo định dạng ảnh**

- Phương pháp thay thế.

+ Thay thế các bit dữ liệu trong bản đồ bit.

+ Thay thế bảng mầu.

- Phương pháp xử lý tín hiệu.

+ Các phương pháp biến đổi ảnh.

+ Các kỹ thuật điều chế dải phổ.

- Phương pháp mã hóa.

+ Lượng hóa, dithering.

+ Mã hóa sửa lỗi.

- Phương pháp thống kê – kiểm thử giả thuyết.

- Phương pháp sinh mặt nạ.

3/. Giấu tin sử dụng tính chẵn lẻ của tổng số bit 1

- Đối với ảnh màu hay ảnh đa cấp xám, cũng có thể áp dụng thuật toán "Giấu tin sử dụng tính chẵn lẽ của tổng số bit 1" cho ảnh đen trắng.
- Với các loại ảnh này, mỗi điểm ảnh được biểu diễn bằng nhiều bit, trong đó có những bit ít quan trọng (LSB: Least Significant bit). Từ mỗi điểm ảnh, ta chọn ra một bit LSB, lưu nó vào ma trận 2 chiều F gồm các bit 0, 1.

4/. Giấu tin vào các bit có trọng số thấp (LSB)

a/. Cơ sở kỹ thuật

- Ý tưởng chính của phương pháp nhúng tin giấu vào các bit có trọng số thấp (LSB).
- Khi chuyển ảnh tương tự sang ảnh số, người ta chọn 3 cách thể hiện màu.

- 24-bit mầu:Mỗi điểm ảnh có thể nhận một trong 2^{24} mầu, mỗi mầu được tạo từ 3 mầu cơ bản: red (R), green (G), blue (B), mỗi mầu nhận một giá trị từ 0 đến 255 (8 bit).
- 8-bit mầu:Mỗi điểm ảnh có thể nhận một trong 256 mầu.
- 8-bit dải xám:Mỗi điểm ảnh có thể nhận một trong 256 sắc thái xám.

b/. Dung lượng tin giấu

- Phương pháp LSB giấu được nhiều thông tin.
- Với ảnh 24bit / điểm ảnh, dùng 1 bit có trọng số thấp có thể giấu được:
  3bit ẩn / 1 điểm ảnh (24 bit dữ liệu) = 1/8 bit ẩn / bit dữ liệu.
- Nếu dùng 2 bit có trọng số thấp
  6bit ẩn / 1 điểm ảnh (24 bit dữ liệu) = 1/4 bit ẩn / bit dữ liệu.
- Trong các ảnh sặc sỡ chúng ta có thể dùng thậm chí 3 bit LSB, khi đó thu được tỷ lệ bit ẩn / bit dữ liệu là 3/8.
- Đôi khi người ta hỏi ngược lại là cần bao nhiêu byte ảnh để có thể giấu 1 byte tin mật. Nếu chỉ dùng 1 bít thấp ta cần 8 byte , nếu dùng đến 2 bit thấp ta cần 4 byte dữ liệu là đã giấu được 1 byte tin mật.

c/. Tính bền vững

- Phương pháp LSB có tính ổn định kém nhất vì:

+ Phương pháp LSB rất dễ bị tổn thương bởi một loạt các phép biến đổi ảnh, ngay cả phép biến đổi ảnh đơn giản và thông dụng nhất.
+ Nén ảnh mất dữ liệu như JPEG rất dễ dàng phá hủy tin mật.
+ Các phép biến đổi hình học như dịch chuyển hay xoay cũng dễ làm mất dữ liệu mật vì khi đó vị trí của các bit giấu sẽ bị thay đổi. Chỉ có một phép dịch chuyển đơn giản thì mới có thể phục hồi lại dữ liệu mật.
+ Các phép xử lý ảnh khác như làm mờ ảnh cũng sẽ làm mất dữ liệu hoàn toàn.

1.3. TỔNG QUAN VỀ Y TẾ ĐIỆN TỬ

1.3.1. Khái niệm Y tế điện tử

1/. Khái niệm

- Y tế điện tử là một hình thức khám chữa bệnh nhờ sự hỗ trợ của công nghệ thông tin.Sử dụng Internet vào lĩnh vực chăm sóc sức khỏe và tất cả những gì liên quan đến tin học, máy tính để ứng dụng vào ngành y tế.
- Các loại hồ sơ Y tế điện tử

+ Hồ sơ khám sức khoẻ

Thông tin về các bộ phận trong cơ thể: Tim, Phổi, Gan, Thận

Thông tin về máu

Thông tin về đường hô hấp

Thông tin về đường tiêu hoá

Siêu âm, X-quang, ...

+ Bệnh án

+ Đơn thuốc

+ Hợp đồng chữa bệnh

2/.Ví dụ

- Có 2 loại hình khám và chữa bệnh cho bệnh nhân
  - ➢ Thứ 1: Bệnh nhân cảm thấy không khỏe.
  - + Bệnh nhân phải đến bệnh viện hoặc các cơ sở Y tế để khám bệnh. Các hồ sơ Y tế của bệnh nhân đều lưu dưới dạng trên giấy tờ.
    - o Hồ sơ khám sức khỏe: như các xét nghiệm về máu, siêu âm và phim chụp X-quang về tim, phổi, gan, thận … đều được lưu dưới dạng giấy tờ.
    - o Bệnh án, đơn thuốc và hợp đồng chữa bệnh cũng đều được lưu giữ trên giấy.
  - + Bệnh nhân sau khi khám bệnh xong nếu bệnh nhẹ có thể được kê đơn thuốc về nhà chữa trị. Nếu bệnh của bệnh nhân mà nặng sẽ trực tiếp nhập viện để nằm viện điều trị.
  - + Bác sĩ sẽ trực tiếp khám chuẩn đoán bệnh và kê đơn thuốc chữa trị cho bệnh nhân. Sau khi bệnh nhân có tiến triển tốt mới được xuất viện.

- Thứ 2: Bệnh nhân cảm thấy không khỏe có thể khám bệnh ở nhiều bệnh viện khác nhau.

+ Hồ sơ Y tế của bệnh nhân: phiếu xét nghiệm, siêu âm, phim chụp X-quang, hồ sơ bệnh án đềuđược lưu dữ trong bộ nhớ của máy tính dưới dạng văn bản điện tử.
+ Bệnh nhân không cần nhập viện có thể gửi hồ sơ Y tế điện tử cho bác sĩ qua mạng.
+ Bác sĩ nhận được hồ sơ Y tế điện tử của bệnh nhân sẽ đưa ra kết luận bệnh tình của bệnh nhân. Tình trạng bệnh của bệnh nhân có cần nhập viện ngay không hoặc có thể chữa trị tại nhà.
+ Bệnh nhân nếu đồng ý với kết quả chuẩn đoán của bác sĩ và muốn chữa trị thì bệnh nhân và bác sĩ sẽ có hợp đồng chữa trị bằng điện tử.
+ Nếu chữa trị tại nhà bác sĩ sẽ kê đơn thuốc(dưới dạng điện tử) cho bệnh nhân qua mạng. Bệnh nhân sẽ trả tiền cho mỗi kết luận và đơn thuốc chữa trị của bác sĩ.

a/.Khi y tế điện tử chưa ra đời

- Mọi người có bệnh sẽ đến khám và chữa bệnh theo hình thức thứ 1.

b/.Khi y tế điện tử ra đời

- Mọi người có thể khám và chữa bệnh theo cả 2 loại hình trên.

1.3.2. Các loại hình Y tế điện tử

- Dữ liệu y tế điện tử (Electronic health record): là những hồ sơ y tế được tin học hóa, phục vụ cho việc trao đổi dữ liệu về bệnh nhân giữa các bác sĩ điều trị một cách dễ dàng bằng Internet.
- Điều trị từ xa (telemedicine): là việc điều trị bệnh, tâm lý được thực hiện từ xa của các bác sĩ đối với bệnh nhân thông qua Internet.
- Thông tin điện tử về sức khỏe (health informatics): là những thông tin về sức khỏe được mang đến cho cộng đồng hay bệnh nhân bằng phương tiện Internet.
- Đội ngũ chăm sóc "ảo"(Virtual healthcare team): bao gồm những nhân viên y tế luôn theo sát và chia sẻ thông tin với bệnh nhân thông qua các dụng cụ số hóa.
- Điện thoại di động y tế: bao gồm việc sử dụng các thiết bị di động (gồm cả những thiết bị theo dõi chỉ số sinh học như máy đo huyết áp, đường huyết... kết hợp với điện thoại di động) trong việc thu thập dữ liệu tổng hợp và mức độ sức khỏe bệnh nhân, cung cấp thông tin chăm sóc sức khỏe cho các bác sĩ, các nhà nghiên cứu, và bệnh nhân, theo dõi thời gian thực các thông số sinh tồn của bệnh nhân, và cung cấp trực tiếp các dịch vụ chăm sóc (y học từ xa thông qua điện thoại di động)
- Cập nhận kiến thức y tế bằng Internet : để giúp các nhân viên trong ngành (bác sĩ, điều dưỡng, dược sĩ…) cập nhật các kiến thức chuyên môn về y học và thuốc (như Medscape, MDLinx…)
- Nghiên cứu y học thông qua hệ thống trao đổi dữ liệu toàn cầu : đó là các nghiên cứu lâm sàng có những hệ thống thông tin rất mạnh, có thể quản lý và trao đổi số lượng lớn các dữ liệu bệnh nhân trên quy mô toàn cầu.
- Hệ thống thông tin y tế (Healthcare Information System): bao gồm việc xây dựng cơ sở hạ tầng về tin học cho các bệnh viện, trung tâm chăm sóc y tế, các phần mềm quản lý y tế, giúp bệnh nhân sắp xếp thời gian biểu khám chữa bệnh, điều trị cũng như quản lý các thông tin về sức khỏe của mình.

1.3.3. Các tính chất đặc trưng cho Y tế điện tử

- Hiệu quả: một trong những hứa hẹn mà y tế điện tử mang lại là tăng hiệu quả của việc chăm sóc sức khỏe, từ đó sẽ giúp giảm được chi phí. Thật vậy, với những hồ sơ y tế điện tử, khả năng trao đổi thông tin giữa các bác sĩ và sự tham gia của bệnh nhân được tăng cường đáng kể, giúp tránh được các xét nghiệm chẩn đoán trùng lặp hoặc không cần thiết, và rút ngắn thời gian chẩn đoán cũng như điều trị bệnh nhân.
- Nâng cao chất lượng chăm sóc: việc tăng hiệu quả không chỉ đồng nghĩa với việc giảm chi phí, nó còn giúp nâng cao chất lượng điều trị.

  Ví dụ, nó giúp việc theo sát tình trạng sức khỏe của bệnh nhân, giúp bệnh nhân tự nâng cao hiểu biết về sức khỏe để chăm sóc bản thân mình.
- Dựa vào chứng cứ: hiệu quả của e-health không chỉ dựa trên cảm giác mà còn được chứng minh bởi nhiều công trình khoa học nghiêm túc.
- Trao quyền: Tăng sức mạnh cho người tiêu dùng và bệnh nhân, bằng cách mang đến cho họ một cơ sở kiến thức về y tế vào chăm sóc sức khỏe, khả năng tiếp cận đến hồ sơ bệnh án của họ thông qua Internet, e-health sẽ mở ra 1 xu hướng mới về 1 ngành y tế lấy bệnh nhân làm trung tâm, tăng khả năng chọn lựa dựa trên bằng chứng các dịch vụ y tế cho bệnh nhân.
- Khuyến khích: khuyến khích một mối quan hệ mới giữa bệnh nhân và chuyên gia y tế, hướng tới 1 quan hệ đối tác thật sự, nơi mà mọi quyết định đều được thực hiện bằng cách chia sẻ thông tin cho nhau.
- Giáo dục: giáo dục nhân viên y tế về kiến thức chuyên môn, cũng như giáo dục bệnh nhân về kiến thức tự chăm sóc sức khỏe cho mình. Điều này là rất quan trọng trong việc điều trị các bệnh mãn tính.
- Mở rộng: Mở rộng phạm vi chăm sóc sức khỏe ngoài ranh giới thông thường của nó. Điều này vừa có nghĩa mở rộng về địa lý vừa có nghĩa mở rộng về khái niệm. Y tế điện tử cho phép người dùng dễ dàng có được dịch vụ y tế từ các nhà cung cấp trực tuyến trên toàn cầu. Những dịch vụ này có thể từ những lời khuyên đơn giản đến những việc phức tạp như khám chữa bệnh hay tiếp cận các sản phẩm như dược phẩm.

- Cho phép: Cho phép trao đổi thông tin và truyền thông một cách tiêu chuẩn hóa giữa các cơ sở chăm sóc y tế.
- Đạo đức: y tế điện tử liên quan đến một mối quan hệ mới giữa bệnh nhân, bác sĩ và đặt ra những thách thức mới và các mối đe dọa đến vấn đề đạo đức như thực hành chuyên môn trực tuyến, thông báo chấp thuận của bệnh nhân, bảo mật và các vấn đề công bằng.
- Công bằng: làm cho việc chăm sóc sức khỏe trở nên công bằng hơn là một trong những hứa hẹn của y tế điện tử, nhưng nó cũng có thể đào sâu thêm khoảng cách giữa những người giàu và người nghèo. Những người không có tiền, tri thức, và khả năng tiếp cận công nghệ cao sẽ trở thành nhóm bệnh nhân ít hưởng lợi nhất từ các tiến bộ mà y tế điện tử mang lại (trong khi thực tế nhóm bệnh nhân này lại cần được tiếp cận thông tin về sức khỏe nhiều nhất) nếu các biện pháp và đường lối quản lý không đảm bảo được sự công bằng. Chính công nghệ thông tin hiện nay vẫn đang chia rẽ 2 thành phần chính của 1 quốc gia: nông thôn và thành thị, giới trẻ và người già, người giàu và người nghèo, cũng như những bệnh lạ, hiếm với những bệnh phổ biến trong xã hội.
- Ngoài những tính chất kể trên, chúng ta còn có thể kể thêm 1 số ưu điểm nổi bật khác của y tế điện tử: như dễ sử dụng có tính giải trí và hào hứng.

1.3.4. Tình hình Y tế điện tử ở nước ta hiện nay

- Chiều ngày 11/03/2009 tại Hà Nội, Bộ Y tế, Tập đoàn Bưu chính Viễn thông Việt Nam và Tập đoàn Intel phối hợp tổ chức lễ ký thoả thuận triển khai chương trình Y tế điện tử.

+ Những năm qua, việc ứng dụng công nghệ thông tin vào hoạt động của ngành Y tế đạt được một số kết quả khả quan. Tất cả các tuyến Trung ương, cơ sở khám chữa bệnh trực thuộc Bộ Y tế, các trường đại học, cơ sở y tế tại 63 tỉnh, thành được nối mạng máy tính trong hoạt động; ngành Y tế có cổng thông tin điện tử riêng…
+ Tuy nhiên việc sử dụng và khai thác, ứng dụng tối đa hiệu quả công nghệ thông tin trong toàn ngành vẫn còn hạn chế.

- Ngày 20/12/2010 ICTnews – Tại triển lãm Vietnam Telecomp vừa diễn ra ở TP.HCM, Ericsson lần đầu tiên giới thiệu hệ thống kết nối thông tin trong y tế (HNIS) của hãng này tại Việt Nam.

+ HNIS là giải pháp tích hợp các chu trình trong chăm sóc y tế và sức khỏe, tối ưu hóa phương thức truy cập trực tuyến để đảm bảo tính cơ động, quản lý thông tin và các chu trình vận hành của các tổ chức y tế, doanh nghiệp và hệ thống cung cấp dịch vụ. Nó được xây dựng theo hướng dạng mô-đul, nền mở nhằm tích hợp dịch vụ doanh nghiệp với các thành tố ứng dụng cụ thể trong lĩnh vực y tế. Hệ thống này giúp cho các tổ chức cung cấp dịch vụ y tế và sức khỏe tối ưu hiệu quả quản lý tài chính, lập kế hoạch và chất lượng dịch vụ cung cấp.
+ Hệ thống này gồm các thành phần có thể hoạt động độc lập và phối hợp lại thành từng gói giải pháp tùy theo các cấp độ đầu tư và quy mô: cơ sở dữ liệu về bệnh án y tế; cơ sở dữ liệu về bệnh nhân; cơ sở dữ liệu các cơ sở y tế; các dịch vụ tích hợp cơ bản; cung cấp đơn thuốc điện tử; chỉ định tư vấn bác sỹ điện tử, đặt chỗ khám điện tử, và hệ thống báo cáo và phân tích.
+ Ông Charles Raby, chuyên gia kỹ thuật, Quản lý tri thức WHO khu vực Tây Thái Bình Dương nói : Theo tôi được biết, ở Việt Nam, chưa có mạng lưới thư viện y học toàn quốc. Chúng ta hoàn toàn có thể thông qua bao phủ di động và internet để chia sẻ kiến thức trong mạng lưới thư viện y học và điều hành y tế. Việt Nam cần xây dựng văn hóa Y tế điện tử. Không chỉ là công nghệ mà còn là thói quen và cách thức trao đổi và chia sẻ thông tin. Ở Việt Nam rất nhiều người chưa biết đến các ứng dụng sẵn có của ĐTDĐ để tiếp cận với dịch vụ tư vấn và điều trị y tế. Qua diễn đàn lần này, Việt Nam có thể học hỏi từ thành công và thất bại của các nước để lựa chọn hướng đi của mình. Tôi nghĩ, khu vực tư nhân có thể tham gia vào phát triển Y tế điện tử. Điều quan trọng đối với Việt Nam là phải điều phối tốt ở cấp độ quốc gia, phải có cơ quan đi đầu trong Y tế điện tử.

Chương 2. MỘT SỐ TÌNH HUỐNG VÀ CÁCH GIẢIQUYẾT TRONG CHUYỂN GIAO HỒ SƠ Y TẾ ĐIỆN TỬ

2.1. VẤN ĐỀ XEM TRỘM NỘI DUNG HỒ SƠ Y TẾ ĐIỆN TỬ

2.1.1. Xem trộm nội dung hồ sơ Y tế điện tử

- Khi bệnh nhân gửi hồ sơ y tế điện tử (bệnh án) cho bác sĩ gửi qua mạng thường hay bị những kẻ xâm nhậpxem trộm trái phép thông tin về nội dung hồ sơ bệnh án của bệnh nhân.
- Sau khi bác sĩ nhận được bệnh án sẽ đưa ra kết luận tình trạng sức khỏe của bệnh nhân và gửi trả lại kết quả tình trạng bệnh và cách chữa trị qua đường truyền mạng thường hay bị những kẻ xâm nhập xem trộm trái phép kết quả tình trạng sức khỏe của bệnh nhân và đơn thuốc chữa trị bệnh của bệnh nhân.
- Những thông tin của hồ sơ Y tế điện tử gửi qua mạng thường hay bị kẻ xâm nhập đánh cắp bất hợp pháp.

- ***Đánh cắp thông tin***

+ Kẻ xâm nhập lắng nghe thông tin trên đường truyền, biết được thông tin về người gửi và nhận nhờ vào thông tin được chứa trong các gói tin truyền trên hệ thống mạng. Hình thức này, kẻ xâm nhập có thể kiểm tra được tần số trao đổi, số lượng gói tin truyền đi và độ dài của gói tin này. Tuy nhiên, với hành động trên, thông thường với mục đích là xem thông tin, sao chép, đánh cắp nội dung thông tin chứ không làm ảnh hưởng nguy hại về mặt vật lý đối với dữ liệu hay làm sai lệch nội dung dữ liệu.

+ Kẻ xâm nhập sử dụng các biện pháp kỹ thuật can thiệp vật lý như trích cáp, thu bức xạ hồng ngoại, điện từ…để đánh cắp thông tin nội dung hồ sơ Y tế điện tử của người sử dụng máy vi tính. Sau đó, dữ liệu bị đánh cắp này sẽ được truyền tải bất hợp pháp trên mạng. Đối với những mạng cục bộ, internet không áp dụng các biện pháp bảo mật dữ liệu, nơi lưu giữ dữ liệu do đó hệ thống rất dễ bị can thiệp sao chép nội dung…

+ Bằng cách sử dụng các đoạn mã ẩn bí mật gắn vào một thông điệp thư điện tử, cho phép người xem lén có thể giám sát toàn bộ các thông điệp chuyển tiếp được gửi cùng với thông điệp ban đầu.

- Khi hồ sơ Y tế điện tử ở dạng tĩnh nằm cố định trong máy tính của bệnh viện có thể bị kẻ xâm nhập xem trộm nội dung hồ sơ Y tế điện tử.
- Khi hồ sơ Y tế điện tử ở dạng tĩnh nằm cố định trong máy tính của bệnh nhân có thể bị kẻ xâm nhập xem trộm nội dung hồ sơ Y tế điện tử.
- Thông tin tình trạng sức khỏe của bệnh nhân bị xem trộm một cách bất hợp pháp và kẻ xâm phạm có khả năng phát tán nội dung hồ sơ Y tế của bệnh nhân trên mạng xã hội gây ảnh hưởng nghiêm trọng tới bệnh nhân.
- Kẻ xâm nhập sau khi biết được nội dung hồ sơ y tế điện tử có thể có ý đồ xấu gây bất lợi đối với bệnh nhân. Đặc biệt ảnh hưởng nghiêm trọng với bệnh nhân.

2.1.2. Phương pháp giải quyết

- Phương pháp mã hóa dữ liệu

+ Hồ sơ khám sức khỏe và bệnh án của bệnh nhân được mã hóa gửi cho bác sĩ điều trị trên đường truyền mạng. Kẻ gian khó mà nhận ra đó là nội dung hồ sơ Y tế. Vì hồ sơ Y tế đã được mã hóa thành các ký tự khó hiểu chỉ có những người có khóa bí mật mới được biết nội dung hồ sơ y tế, còn những kẻ xâm nhập bất hợp pháp thì chỉ có thể xem bản mã mà không hiểu được nội dung hồ sơ Y tế.
+ Hợp đồng chữa trị và đơn thuốc cũng được mã hóa trước khi gửi cho bệnh nhân trên đường truyền mạng. Kẻ gian khó mà biết được nội dung đơn thuốc và hợp đồng.

- Phương pháp ẩn giấu tin.

+ Các hồ sơ Y tế được nhúng vào một vật mang tin(ảnh, video, audio,…) mắt thường khó mà phát hiện được vật mang tin chứa các hồ sơ Y tế. Sau đó gửi các vật mang tin trên đường truyền mạng kẻ gian khó mà phát hiện được hồ sơ Y tế.

2.2. VẤN ĐỀ SỬA ĐỔI TRÁI PHÉP NỘI DUNG HỒ SƠ Y TẾ ĐIỆN TỬ

2.2.1. Sửa đổi trái phép nội dung hồ sơ Y tế điện tử

- Khi hồ sơ Y tế điện tử gửi qua mạng thường hay bị những kẻ xâm nhậpphá hoại thông tin nội dung hồ sơ Y tế điện tử : Hồ sơ Y tế bị thay đổi nội dung, chèn thêm thông tin dữ liệu, phá hủy làm hỏng các gói tin, làm trễ thời gian truyền tin, sao chép lặp đi lặp lại dữ liệu… với mục đích phá hỏng hay làm sai lệch nội dung thông tin. Nội dung hồ sơ Y tế bị thay đổi nhưng rất khó bị phát hiện.
- Khi bệnh nhân A có yêu cầu muốn được khám và chuẩn đoán bệnh bởi một bác sĩ B nào đó. Bệnh nhân A gửi hồ sơ bệnh án của mình cho bác sĩ B để chuẩn đoán và trị bệnh qua đường truyền mạng. Hồ sơ bệnh án của bệnh nhân A trên đường truyền có thể bị một số kẻ xâm nhập sửa đổi trái phép nội dung bệnh án trước khi bác sĩ B nhận được bệnh án của bệnh nhân A. Bác sĩ B nhận được bệnh án giả sẽ dẫn đến chuẩn đoán nhầm và đưa ra cách chữa trị sai cho bệnh nhân A.
- Sau khi bác sĩ B chuẩn đoán và đưa ra cách chữa trị. Bác sĩ B sẽ gửi cho bệnh nhân A kết quả chuẩn đoán và cách điều trị trên đường truyền mạng. Hồ sơ chữa bệnh của bệnh nhân A có thể bị một số kẻ xâm nhập sửa đổi trái phép tình trạng sức khỏe và cách chữa trị mà bác sĩ B đưa ra đối với bệnh nhân A trước khi bệnh nhân A nhận được. Bệnh nhân A nhận được kết quả và cách chữa trị sai sẽ dẫn đến tình trạng sức khỏe bị ảnh hưởng nghiêm trọng, tình trạng bệnh không cải thiện trong trường hợp xấu có thể gây ra tử vong cho bệnh nhân.
- Hồ sơ Y tế của bệnh nhân (bệnh án,đơn thuốc…) nằm trong máy tính của bệnh nhân. Kẻ gian tấn công vào máy tính của bệnh nhân sửa đổi trái phép nội dung trong hồ sơ Y tế của bệnh nhân. Bệnh nhân rất dễ gửi bệnh án đã bị phá hoại cho bác sĩ chuẩn và chữa trị hoặc bệnh nhân sử dụng đơn thuốc đã bị kẻ gian sửa đổi mà không hay biết.
- Hồ sơ Y tế của bệnh nhân được lưu giữ trong máy tính của bệnh viện hay máy tính của bác sĩ. Kẻ gian có thể tấn công vào máy tính của bệnh viện hay máy tính của bác sĩ để thay đổi hồ sơ bệnh án của bệnh nhân hay kết quả chuẩn đoán của bác sĩ cho bệnh nhân.

- Khi hồ sơ Y tế điện tử gửi qua mạng bị tấn công bởi virut dễ bị biến dạng ảnh, nội dung bệnh án của bệnh nhân hoặc máy tính của bệnh nhân hay bác sĩ bị nhiễm virut mà không hay biết rằng virut đã làm thay đổi nội dung hồ sơ Y tế điện tử.
- Kẻ gian sửa đổi trái phép nội dung hồ sơ Y tế điện tử như:

+ Hồ sơ khám sức khỏe

Sửa đổi ảnh chụp X-Quang của bệnh nhân (ảnh chụp tim, phổi, gan, thận..)

Sửa đổi ảnhchụp cắt lớp CT của bệnh nhân.

Sửa đổi thông tin xét nghiệm về máu.

Sửa đổi thông tin xét nghiệm về đường hô hấp, đường tiêu hóa, đường tiết liệu…

+ Hồ sơ bệnh án.

Sửa đổi các triệu chứng xuất hiện khi phát hiện bệnh.

Sửa đổi thời gian xuất hiện bệnh.

Sửa đổi các phương pháp mà người bệnh đã từng chữa trị trước đó (nếu trước đó đã chữa trị)…

+ Đơn thuốc

Sửa đổi tên thuốc cần để điều trị bệnh.

Sửa đổi số lượng thuốc trong đơn thuốc.

Sửa đổi số lượng thuốc trong từng loại thuốc.

Sửa đổi đơn giá thuốc.

Sửa đổi số lượng thuốc của từng loại thuốc cần dùng trong 1 ngày.

+ Hợp đồng chữa bệnh.

Sửa đổi tên bệnh nhân và bác sĩ

Sửa đổi cam kết của bệnh nhân và bác sĩ trong quá trình chữa bệnh.

Sửa đổi tiền bệnh nhân sẽ phải trả cho bác sĩ sau khi chữa xong bệnh.

- Hồ sơ bị sửa đổi sẽ dẫn đến chuẩn đoán bệnh không chính xác gây ảnh hưởng nghiêm trọng đến tình trạng sức khỏe cũng như tính mạng của bệnh nhân.

2.2.2. Phương pháp giải quyết

- Phương pháp mã hóa dữ liệu.

  Ví dụ: phiếu siêu âm của bệnh nhân gửi cho bác sĩ được mã hóa. Kẻ gian khó mà nhận ra đó là phiếu siêu âm của bệnh nhân để mà sửa chữa.

- Phương pháp ẩn giấu tin.

  Ví dụ: phiếu xét nghiệm máu được giấu trong bức ảnh. Kẻ gian khó mà phát hiện trong bức ảnh có giấu tin để mà sửa đổi.

- Sử dụng phương pháp chữ ký số.

  Ví dụ: Hợp đồng chữa bệnh của bệnh nhân và bác sĩ được ký bằng chữ ký số. Kẻ gian sửa đổi nội dung trong hợp đồng chữa bệnh. Bệnh nhân và bác sĩ lấy chìa khóa công khai nhồi vào thuật toán kiểm tra chữ ký để kiểm tra. Chữ ký sai bác sĩ và bệnh nhân nghi vấn sẽ hỏi lại nhau.

- Sử dụng phương pháp mã xác thực.

  Ví dụ: hồ sơ bệnh án của bệnh nhân trước khi gửi cho bác sĩ có gắn mã xác thực. Kẻ gian sửa đổi nội dung hồ sơ bệnh án. Bác sĩ nhận được hồ sơ bệnh án kiểm tra lại mã xác thực. Mã xác thực bác sĩ kiểm tra không giống với mã xác thực của bệnh nhân gửi. Bác sĩ hỏi lại bệnh nhân.

- Sử dụng phương pháp thủy vân số.

  Ví dụ: Ảnh chụp Phổi bệnh nhân: Rất tốt, được gắn Thuỷ vân.

  Kẻ gian sửa đổi lại Ảnh chụp Phổi bệnh nhân thành méo mó rất xấu.

  Khi đó thuỷ vân bị sai lệch, không giống như cũ.

  Bác sỹ sẽ nghi vấn, hỏi lại bệnh nhân.

- Sử dụng phương pháp đại diện tài liệu.

  Ví dụ: Đơn thuốc bác sĩ gửi cho bệnh nhân có gắn đại diện tài liệu là A. Bệnh nhân nhận được đơn thuốc có đại diện tài liệu là B thì sẽ hỏi lại bác sĩ.

2.3. VẤN ĐỀ THAY ĐỔI HỒ SƠ GỐC

2.3.1. Thay đổi hồ sơ gốc

- Khi hồ sơ y tế điện tử gửi qua mạng thường hay bị những kẻ xâm nhập thay một hồ sơ khác thay cho hồ sơ gốc.

+ Hồ sơ Y tế bị giả mạo: Các thông tin của hồ sơ Y tế trong khi truyền đi bị thay đổi hoặc thay thế khi đến tay người nhận.

+ Hồ sơ Y tế bị xuyên tạc: Kẻ xâm nhập có thể thêm hoặc giảm hồ sơ bệnh án đưa những thông tin không đúng về tình trạng bệnh của bệnh nhân cho bác sĩ.

+ Thay đổi hồ sơ Y tế gốc.

  Thay ảnh chụp tim bình thường thành ảnh chụp tim ở cuống tim bị phình to.

  Thay phiếu siêu âm dạ dày bị viêm thành phieus siêu âm gan bị nhiễm mỡ.

  Thay bệnh án của bệnh nhân A thành bệnh nhân B.

  Thay đơn thuốc chữa bệnh tim thành chữa bệnh gan.

  Thay hợp đồng chữa bệnh của bệnh nhân A với bác sĩ B…

- Hồ sơ bị thay đổi sẽ dẫn đến chuẩn đoán bệnh không chính xác gây ảnh hưởng nghiêm trọng đến tình trạng sức khỏe hoặc tính mạng của bệnh nhân.

2.3.2. Phương pháp giải quyết.

- Sử dụng phương pháp chữ ký số.

  Ví dụ: Bản hợp đồng chữa bệnh của bệnh nhân A và bác sĩ B bị thay đổi thành bác sĩ B và bệnh nhân C. Bác sĩ nhận bản hợp đồng và sử dụng khóa công khai nhồi vào thuật toán kiểm tra chữ ký. Chữ ký sai bác sĩ hỏi lại bệnh nhân.

- Sử dụng phương pháp mã xác thực.

  Ví dụ: hồ sơ bệnh án của bệnh nhân trước khi gửi cho bác sĩ có gắn mã xác thực. Kẻ gian thay đổi nội dung hồ sơ bệnh án của bệnh nhân A thành bệnh nhân B. Bác sĩ nhận được hồ sơ bệnh án kiểm tra lại mã xác thực. Mã xác thực bác sĩ kiểm tra không giống với mã xác thực của bệnh nhân A gửi. Bác sĩ hỏi lại bệnh nhân A.

- Sử dụng phương pháp thủy vân số.

  Ví dụ: Ảnh chụp Phổi bệnh nhân: Rất tốt, được gắn Thuỷ vân.

  Kẻ gian thay đổi lại Ảnh chụp Phổi bệnh nhân thành méo mó rất xấu.Khi đó thuỷ vân bị sai lệch, không giống như cũ.Bác sỹ sẽ nghi vấn, hỏi lại bệnh nhân.

2.4. VẤN ĐỀ THỜI GIAN TRUYỀN HỒ SƠ Y TẾ CHẬM

2.4.1. Thời gian truyền hồ sơ Y tế chậm.

- .Hồ sơ bệnh nhân đã gửi đi cho Bác sĩ. Nhưng kẻ nghịch ngợm giữ lại vài ngày mới gửi tiếp. Bác sĩnhận được hồ sơ chậm. Không kịp thời chữa cho bệnh nhân, nên bệnh tình trở nên nguy cấp, khó cứu chữa.
- Hồ sơ khám chữa bệnh của Bác sĩ đã gửi đi cho bệnh nhân. Nhưng kẻ nghịch ngợm giữ lại vài ngày mới gửi tiếp. Bệnh nhân nhận được hồ sơ chậm, không kịp thời chữa trị bệnh, nên bệnh tình trở nên nguy cấp, khó cứu chữa.

2.4.2. Phương pháp giải quyết.

- Phương pháp mã hóa dữ liệu.

  Ví dụ: Hồ sơ khám chữa bệnh được mã hóa. Kẻ gian nghịch ngợm sẽ không hiểu gì mà bắt giữ hồ sơ gây chậm trễ.
- Phương pháp ẩn giấu tin.

  Ví dụ: Hồ sơ Y tế của bệnh nhân gửi cho bác sĩ được giấu trong bức ảnh. Kẻ gian khó mà biết được trong ảnh có giấu hồ sơ Y tế để mà bắt giữ lại gây chậm trễ.

2.5. VẤN ĐỀ GÂY ÁCH TẮC TRONG TRAO ĐỔI HỒ SƠ Y TẾ

2.5.1. Ách tắc trong trao đổi hồ sơ Y tế.

- Bệnh nhân gửi hồ sơ Y tế của mình cho bác sĩ trên đường truyền mạng. Đường truyền mạng bị tắc nghẽn bác sĩ không nhận được hồ sơ Y tế của bệnh nhân. Nên không chuẩn đoán và chữa cho bệnh nhân dẫn đến tìn trạng bệnh kéo dài trở nên nguy cấp, khó cứu chữa.
- Bác sĩ gửi hồ sơ chuẩn đoán kết quả và chữa trị bệnh cho bệnh nhân trên đường truyền mạng. Đường truyền bị tắc nghẽn bệnh nhân không nhận được hồ sơ chữa bệnh bệnh tình kéo dài trở nên nguy cấp, khó cứu chữa.
- Bệnh nhân gửi hồ sơ Y tế của mình cho bác sĩ trên đường truyền mạng. Kẻ gian bắt giữ hồ sơ Y tế không gửi cho bác sĩ. Bác sĩ không nhận được hồ sơ Y tế của bệnh nhân nên không chuẩn đoán và chữa cho bệnh nhân. Tình trạng bệnh để lâu trở nên nguy kịch, khó cứu chữa.

- Bác sĩ gửi hồ sơ khám chữa bệnh cho bệnh nhân trên đường truyền mạng. Kẻ gian bắt giữ hồ sơ khám chữa bệnh của bác sĩ gửi cho bệnh nhân. Bệnh nhân không nhận được hồ sơ khám chữa bệnh, bệnh tình trở nên nguy cấp, khó cứu chữa.

2.5.2. Phương pháp giải quyết

- Phòng tránh tắc nghẽn mạng máy tính: Dự đoán trước khả năng tắc nghẽn và đưa ra một số hoạt động điều khiển để chống lại hoặc giảm thiểu khả năng tắc nghẽn. Có 3 kỹ thuật cơ bản là kỹ thuật loại bỏ gói tin sớm ngẫu nhiên RED (Random Early Discarding). Kỹ thuật loại bỏ gới tin sớm ngẫu nhiên theo trọng số WRED (Weighted Random Early Discarding). Thông báo tắc nghẽn hiện ECN (Explicit Congestion Notification).

  Ví dụ: Hồ sơ bệnh án của bệnh nhân gửi cho bác sĩ trên đường truyền mạng bị tắc nghẽn. Bệnh nhân lên gửi Hồ sơ bệnh án nhiều lần.
- Phòng tránh kẻ nghịch ngợm bắt giữ Hồ sơ Y tế, để lưu giữ lại.

+ Sử dụng phương pháp mã hóa dữ liệu.

  Ví dụ: Hồ sơ khám chữa bệnh được mã hóa. Kẻ gian nghịch ngợm sẽ không hiểu gì mà bắt giữ hồ sơ lưu trữ lại không gửi đi.

+ Sử dụng phương pháp ẩn giấu tin.

  Ví dụ: Hồ sơ Y tế của bệnh nhân gửi cho bác sĩ được giấu trong bức ảnh. Kẻ gian khó mà biết được trong ảnh có giấu hồ sơ Y tế để mà bắt giữ lại.

*Chương 3.*CHƯƠNG TRÌNH THỬ NGHIỆM

3.1. BÀI TOÁN CHỮ KÝ SỐ RSA

- *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 $\phi(n) = (p-1).(q-1)$. Chọn khóa công khai $b < \phi(n)$, nguyên tố với $\phi(n)$.

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

Tập cặp khóa (bí mật, công khai) $K = \{(a, b)/\ a, b \in Z_n, a*b \equiv 1 \pmod{\phi(n)}\}$.

- *Ký số*: chữ ký trên $x \in P$ là $y = Sig_k(x) = x^a \pmod n$, $y \in A$.
- *Kiểm tra chữ ký*: $Ver_k(x, y) =$ đúng $\Leftrightarrow x \equiv y^b \pmod n$.

3.2. CẤU HÌNH HỆ THỐNG

3.2.1. Cấu hình phần cứng

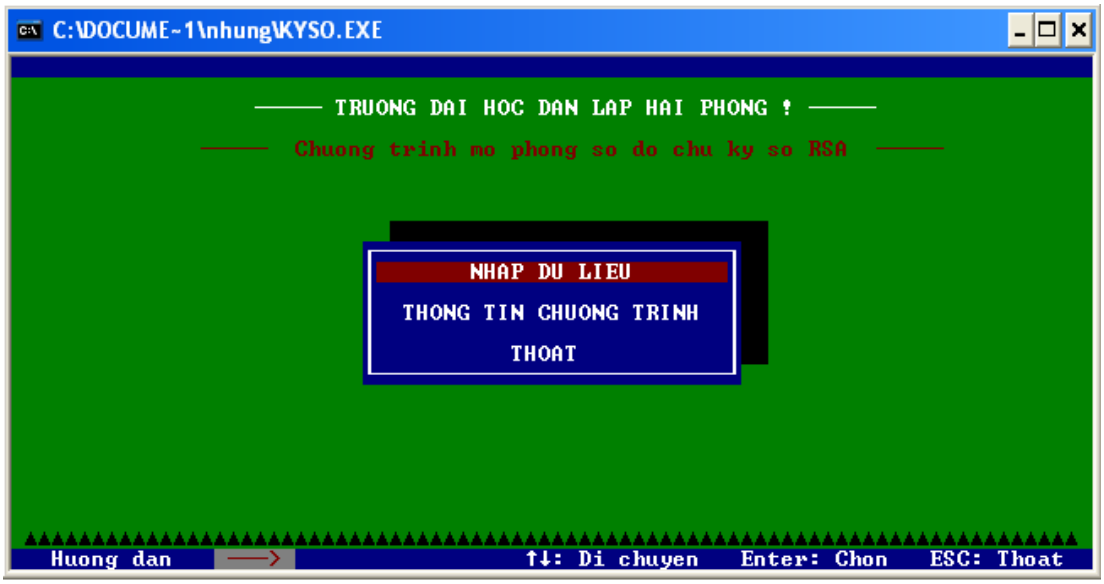
- Bộ nhớ trong 1GB
- Cấu hình Chip CPU 2,2GHz

3.2.2. Cấu hình phần mềm

- Hệ điều hành MicroSoft
- Ngôn ngữ lập trình C.

3.3. HƯỚNG DẪN SỬ DỤNG CHƯƠNG TRÌNH

3.3.1. Giao diện của chương trình



Hình 3.4.1. Giao diện chính của chương trình

3.3.2. Chữ ký RSA

- Khởi tạo chữ ký

+ Nhập số nguyên tố p và q.
+ Chương trình tính được n và ϕn, tự động sinh khóa công khai b, tính được khóa bí mật a.
+ Nhập bản rõ.
+ Chương trình sẽ thực hiện ký và sinh ra bản ký số

- Kiểm tra chữ ký

+ Nhập vào số công khai n.
+ Nhập vào khóa công khai b.
+ Nhập bản rõ.
+ Nhập bản ký số.
+ Chương trình kiểm tra chữ ký đúng hoặc sai.

KẾT LUẬN

Đồ án tốt nghiệp đã thực hiện được các nội dung sau:

1/. Tìm hiểu tổng quan về An toàn thông tin và Y tế điện tử

2/. Tìm hiểu một số tình huống và cách giải quyết trong chuyển giao hồ sơ Y tế điện tử.

3/. Thử nghiệm chương trình: Demo Chương trình chữ ký RSA