|  |
| --- |
| Trang |

Mục Lục

Lời nói đầu

Giới thiệu nhóm thực hiện

Nội dung

Phần I- tổng quan về an toàn bảo mật thông tin

1.1 Tin và vai trò của thông tin

1.1.1 Thông tin là gì?

1.1.2 Vai trò của thông tin

1.2 An toàn bảo mật thông tin của hệ thống

1.3 Bảo mật thông tin

* 1. Các hệ thống mã hóa cổ điền

Phần II: sử dụng bảo mật cho 1 web tự lập

2.1 Chuẩn bị

2.2 Tiến hành bảo mật

2.3 Bài học, nhận xét nhóm sau quá trình làm đồ án

LỜI NÓI ĐẦU.

Trước hết các thành viên nhóm xin trân thành cảm ơn sự tận tình và nhiệt huyết trong giảng dạy và cố vấn của thầy Mai Hà AN đối với môn học an toàn và bảo mật thoogn tin trong kì học lần này. Đồi với môn học này có phần thử thách cũng cũng khó khan đối với nhóm khá nhiều do chưa được tiêp xúc quá nhiều với tạo lập web và khó khan nhất là đối với phần bảo mật thông tin web. Nhóm chúng em không phủ nhận việc thông tin tìm kiếm dễ dàng nhưng cũng k thể bác bỏ việc chọn lọc ra thông tin đúng và chuẩn xác là việc dễ dàng. Báo cáo này là công sức, cố gắng của nhóm, chũng em đã nỗ lực hết mìnhvà mong rằng thầy cũng thấu hiểu. chúng em hy vọng sẽ nhận được những lời góp ý từ thầy. chúng em xin cảm ơn!

Giới thiệu nhóm thực hiện

Thành viên nhóm:

1. Nguyễn Thị Mai:

Lớp k66AHTTT

SĐT: 0984682146

MSV: 2174801040994

Email: [nmai67700@gmail.com](mailto:nmai67700@gmail.com)

1. Nguyễn Thị Lộc:

Lớp: K66AHTTT

SĐT: …

MSV:2174801040…

Email: …

Nội dung thực hiện:

Bảo mật thông tin cho 1 shop online.

Phần I: Tổng quan về an toàn bảo mật thông tin.

* 1. Thông tin và vai trò của thông tin
     1. Thông tin là gì?

Thông tin là cái được truyền từ đối tượng này sang đối tượng khác để báo một “điều” gì đó. Thông tin chỉ có ý nghĩa khi “điều” đó bên nhận chưa biết. như vậy, nói cách khác thông tin là tất cả những gì nhằm đem lại sự hiểu biết cho con người.

Thông tin xuất hiện dưới nhiều dạng âm thanh, hình ảnh…

những dạng này chỉ là “vỏ bọc” vật chất chứa thông tin. “vỏ bọc” là phần “xác”, thông tin là phần “hồn”. ngữ nghĩa của thông tin chỉ có thể hiểu được khi bên nhận hiểu được cách biểu diễn ngữ nghĩa của bên phát.

Có hai trạng thái của thông tin: truyền và lưu trữ. Môi trường truyền / lưu trữ được gọi chung là môi trường chứa tin hay kênh tin.

Thông tin là một khái niệm trừu tượng, phi vật chất và rất khó đưuọc định nghĩa chính xác. Hai định nghĩa về thông tin:

* Thông tin là sự cảm hiểu của con người về thế giới xung quanh thông qua sự tiếp xúc trực tiếp với nó.
* Thông tin là một hệ thống những tin báo và mệnh lệnh giúp loại trừ sự chắc chắn trong trạng thái của nơi nhận tin. Nói tóm lại, thông tin là cái mà loại trừ sự chắc chắn.

Định nghĩa đầ chưa nói lên được bản chất của thông tin. định nghĩa thứ hai nói lên rõ hơn về bản chất của thông tin và được dung để định lượng thông tin trong kĩ thuật.

Thông tin lad một đại lượng vật lí, nó thường tồn taị và được truyền dưới một dạng vật chất nào đó. Những dạng vật chất mang thông tin được gọi là tín hiệu.

1.2 Vai trò của thông tin:

Thông tin có một vai trò vô cùng to lớn đới với sự tồn tại và phát triển. các đối tượng sống luôn có nhu cầu muốn timfhieeur cề thế giới xung quanh đẻ thích nghi và tồn tại

Khi khoa học kỹ thuật và xã hội ngày càng phát triển, thông tin cnagf thể hiện đưuọc vai trò của nó đối với chũng ta. Nó có thể chi phối mọi hành động của con người, vì hành động của con người thì xuất phát từ suy nghi , mà suy nghĩ thì lại là hệ quả của quá trình tiếp nhận thông tin.

* + 1. An toàn thông tin của hệ thống.

\*An toàn thoogn tin (dữ liệu) là giữu cho thoogn tin dữ liệu được toàn vẹn (không bị đánh tráo, mất mát, sửa đổi…) dù là vô tình hay cố ý.

\*Các yêu cầu về an toàn thông tin:

- Tính bí mật: tính kín đáo riêng tư của thông tin.

- Tín h xác thực: Bao gồm xác thực người đối tá (danh tính và xác thực thông tin được trao đổi.

- Tính toàn vẹn: Bảo đảm thông tin không bị cắt xén hay xuyên tạc qua kênh trao đổi.

- Tính trách nhiệm: Bảo đảm người gửi thông tin không thể thoái thác trách nhiệm về thông tin mà mình gửi.

- Tính kịp thời: Thông tin đến nơi nhqanj đúng thời gian.

\* ý nghĩa của an toàn thông tin:

- Bảo vệ an toàn thông tin dữ liệu là một đề tài rộng, có liên quan đến nhiều lĩnh vực và trong thực tế có nhiều phương pháp được thực hiện để bảo đảm an toàn thông tin dữ liệu. Các phương pháp bảo vệ an toàn thông tin dữ liệu có thể quy về ba nhóm chính sau:

- Bảo vệ an toàn thông tin bằng các biện pháp hành chính.

- Bảo vệ an toàn thông tin dữ liệu bằng các biện pháp kỹ thuật (phàn cứng).

Bảo vệ an toàn thông tin dữ liệu bằng các biện pháp thuật toán (phần mềm)

* Ba nhóm biện pháp trên có thể ứng dụng riêng hoặc phối hợp. Môi trường khó bảo vệ an toàn thông tin dữ liệu nhất là môi trường đối phương dễ xâm nhập nhất như môi trường mạng và truyền thông. Biện pháp bảo vệ an toàn thông tin hiệu quả nhất trên môi trường mạng truyền tin là các biện pháp thuật toán.

- Để bảo vệ an toàn thông tin trên đường truyền tin và trên mạng cố hiệu quả nhất thì việc trước tên phải dự đoán được hoặc lường trước được các khả năng xâm phạm, các sự cố rủi ro có thể xảy ra với thông tin lưu trữ hay truyền trên mạng. xác định càng chính xác các nguy cơ nói trên thì càng dễ tìm ra các giải pháp tốt để giảm thiều thiệt hại.

\*Phân loại các hành vi vi phạm

Về bản chất có thể phân loại các hành vi vi phạm trên đường truyền thành hai loại: vi phạm chủ động và vi phạm thụ động.

* Vi phạm chủ động: là dạng vi phạm có thể làm thay đổi nội dung, xóa bỏ, làm trễ, sắp xếp lại thứ tự, làm lặp lại các gói tin đó thười điểm hiện tại sau đó.
* Vi phạm thụ động: la loại vi phạm nhằm mục đính nắm bắt được thông tin (đánh cắp thông tin).
* Vi phạm thụ động khó phát hiện nhưng có thể có những biện pháp ngăn chặn hiệu quả trong khi đó vi phamj chủ ddoognj dễ pahst hiện nhưng biện pháp ngăn chặn lại khó hơn nhiều.

\*Các vị trí có thể xâm phạm

Trong thực tế, kẻ xâm phạm có thể xâm nhập vào hệ thống thông tin bất cứ thời điểm naò mà thông tin đi qua hoặc được lưu trữ. Điểm đó có thể trên đường truyền, nút mạng, máy tính chủ có nhiều người sử dụng hoặc tại giao diện kết nối mạng (bridge, gateway, router…). Trogn quan hệ tương tác người-máy thì các thiết bị ngoại vi, đặc biệt các thiết bị đầu cuối (terminal) là cửa ngõ thuận tiện nhất cho việc xâm nhập.

Ngoài ra có thể tính tđến các thiết bị điện tử có các phát xạ điện tử và các thiết bị máy tính. Bằng các thiết bị chuyên dụng có khả năng đón bắt các phát xạ này và xử lý chúng. Cũng có trường hợp sử dụng các bức xạ điều khiển từ bên ngoài để tác động gây nhiễu, gây lỗi nội dung truyền tin.

\*Các mức bảo vệ của một hệ thống thông tin

1- Quyền truy nhập: đây là lớp bảo vệ trong nhất, nhằm kiểm soát truy cập tài nguyên mạng và quyền hạn sử dụng tài nguyên đó. Cụ theervieecj quản lý được tiến hành ở mức truy nhập File (đọc, ghi ,xóa, sửa…) do người quản lí mạng thiết lập.

2- Đăng ký và mật khẩu: phương pháp này không mấy hiệu quả đối với những người hiểu biết về hệ thống của ta nhưng ưu điểm của nó là đơn giản.

3- Mã hóa dữ liệu: biên sđổi dữ liệu từ dạng nhận thức được sang dạng không nhận thức được theo một quy luật nào đó.

4- Bảo vệ vật lý: nhằm ngăn chặn các truy cạp vật lý bát hợp pháp vào hệ thốn

 5- Tường lửa: bảo đảm an toàn và ngăn chặn từu xa cho các mạng nội bộ, đây là phương thức bảo vệ cho mạng cục bộ (internet), ngăn chặn các xâm phạm trái phép, lọc bỏ các gói tin không muốn nhận (gửi) vì một lý do nào đó

* + 1. Đảm bảo ann toàn

Các quan điểm bảo vệ an toàn quyền hạn ít nhất (least privilege): mỗi một đối tượng chỉ có quyền hạn nào đó, khi đó nếu kẻ xâm nhập có vào được hệ thống cũng chỉ phá hoại được một phần nào đó của hệ thống.

Phòng thủ theo chiều sâu: đặt nhieefiu cô chế bảo vệ khác nhau trên một hệ thống, nếu một cơ chế bị phá vỡ thì còn cơ chế khác.

Tạo điểm thắt: chỉ có xâm nhập vào hệ thống qua một kênh hẹp, sau đó tập trung giám sát điều khiển hệ thống qua kênh này.

Tìm ra điểm yếu nhất: cần phải biết điểm yếu nhất của mình nếu không loại bỏ được thì cũng cần có cơ chế giám sát chặt chẽ. An toàn về mặt vậy lý được gọi là điểm yếu nhất trong hệ thống.

Cơ chế tự động ngắt khi có sự cố: hẹ thống có thể tự ngắt tức là khi hệ thống có nguy cơ bị đe doa thì có khả năng tự bảo vệ.

Hợp nhất các thành phần tham gia: tất cả các thành phần trong hệ thống từ các quy chế an toàn, người sử dụng, thiết bị bảo vệ, phần mềm… phải được kết hợp thành một hệ thống bảo vệ có hiệu quả và hỗ trợ bảo vệ lẫn nhau.

Tính đa dạng của hệ thống phòng thủ: sự bảo vệ của hê thống sẽ tang khi ta sử dụng nhiều modul phòng thủ khác nhau thì kẻ tấn công sẽ dễ dàng vào được mọi nơi trong hệ thống.

Tính đơn giản: làm cho hệ thống trở nên dễ hiểu, nên ta không hiểu một vẫn đề, một phần nào đó trong hệ thống thf cũng không biết hệ thống có bí mật không. Bảo vệ cả phần nhỏ sẽ dễ dàng hơn bảo vệ cả một hệ thống lớn.

\*Quan điểm để đặt ra quy tắc an toàn:

Quan điểm mặc nhiên từ chối (Default deny stance) chiri cho phép một số dịch cụ phục vụ, các dịch vụ khác không đề cập đến coi như từ chối. Quan điểm mặc nhiên cho phép (default permit stance) tức là những gì không cấm thì được phép làm. Tùy từng trường hợp, tuy từng đặc thù riêng của hệ thống ta sẽ đi đến quyết định chọn quan điểm nào.

* + 1. Chính sách an toàn thông tin

Trước khi một hệ thống thống tin có thể được bảo đảm an toàn nhất thiết phảo xác lập một chính sách an toàn, nó là nền tảng tiêu chuẩn đúng đắn để xem xét. Nếu không có chính sách an toàn đúng đắn thì hiệu quả của mọi biện pháp khác sẽ bị giảm sút.

Các bước để phát triển một chính sách của mình

* Xác định mục đích
* Xác định phạm vi
* Tham khảo các chính sách để cảm nhận chính sách của mình.
* Đánh giá rủi ro
* Quyết định các thành phần và viết chính sách. Việc lwuja chọn thành phần nào là phụ thuộc vào cấ trúc của hệ thống thông tin, vị trí, quy mô của tổ chức.
* Đánh giá : sau khi chính sách được phát triển, việc đánh giá lại chính sách là thực sự cần thiết để xem mục đích của chính sách đa đạt được chưa? Ngoài ra các mối đe dọa, các lỗ hổng bảo mật, yêu cầu nghiệp vụ luôn biến đổi, do đố phảo địn kỳ và luôn xem xét lại hệ thống để có chính sách an toàn cho phù hợp.
  1. Bảo mật thông tin

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

Ở trạm nhận phải thực hiện quá trình ngược lai, tức là biến đổi thông tin từ dạng không nhận thức được quay trở lại ddnagj nhận thức được (dạng gốc), qua strinhf này được gọi là quá trình giải mã. Đây là một lớp bảo vệ thông tin rất quan trọng và được sử dựng rộng rãi trong quá trình truyền tin.

Như vậy lý do mã hóa thông tin chính là để đảm bảo an toàn thông tin trong quá trình truyền-nhận.

Để bảo vệ an toàn thông tin bằng mật mã, người ta tiếp cân theo hai hướng:

* Theo đường truyền (link oriented sercurity)
* Từ nút đến nút (end to end)

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

Ngược lại theo cách thứ hai, thoogn tin trên mạng được bảo vệ trên toàn đường truyền từ nguồn đến đích. Thông tin sẽ được mã hóa ngay sau khi mới tạo ra và chỉ được giải mã sau khi đã về đến đích. Cách này mắc phải nhược điểm là chỉ có dữ liệu của người sử dugnj thì mới có thể mã hóa được còn dữ liệu điều khiển thì giữ nguyên để có thể sử lý các nút.

* 1. Các hệ thống mã hóa cổ điển.
     1. Mã hóa dịch vòng.

Phần này sẽ mô tả mã dịch (MD) dựa trên số học theo modulo. Trước tiên sẽ điểm qua một số định nghĩa cơ bản của số học này.

Mã hóa dịch vòng là một bộ năm (P, C, K, E, D) thỏa mãn:

* P=C=K=Zn
* E={ek,k {"mathml":"<math style=\"font-family:stix;font-size:16px;\" xmlns=\"http://www.w3.org/1998/Math/MathML\"><mstyle mathsize=\"16px\"><mo>&#x2208;</mo></mstyle></math>"} K} trong đó: ek(x)=(x+k) mod n với x {"mathml":"<math xmlns=\"http://www.w3.org/1998/Math/MathML\" style=\"font-family:stix;font-size:16px;\"/>"}{"mathml":"<math style=\"font-family:stix;font-size:16px;\" xmlns=\"http://www.w3.org/1998/Math/MathML\"><mstyle mathsize=\"16px\"><mo>&#x2208;</mo></mstyle></math>"}Zn
* D={dk,k {"mathml":"<math style=\"font-family:stix;font-size:16px;\" xmlns=\"http://www.w3.org/1998/Math/MathML\"><mstyle mathsize=\"16px\"><mo>&#x2208;</mo></mstyle></math>"} K} trong đó:dk(y)=(y-k)mod n với y {"mathml":"<math style=\"font-family:stix;font-size:16px;\" xmlns=\"http://www.w3.org/1998/Math/MathML\"><mstyle mathsize=\"16px\"><mo>&#x2208;</mo></mstyle></math>"} Zn

Ví dụ : giải mã và mã hóa đoạn text: p = " abcde" với k = 5 ( p ở đây là các kí tự thường trong bảng chữ cái tiếng anh )

Quy ước: Số thứ tự của các chữ cái trong bảng chữ cái tiếng anh như sau: a = 0, b = 1, …, z= 25 nên t có :

* n = 26
* p = "abcde"
* k = 5 Xách định bản mã c = ?
* Bước 1 : Đổi các ký tự trong p sang thứ tự của chúng trong bảng chữ cái.  
  a = 0 , b=1, c= 2, d= 3, e = 4
* Bước 2 : Tiến hành mã hóa bản rõ p với khóa k = 5

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| p | 0 | 1 | 2 | 3 | 4 |
| (p+k)mod 26 | 5 | 6 | 7 | 8 | 9 |

* Bước 3: xác định bản mã c

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| (p+k)mod 26 | 5 | 6 | 7 | 8 | 9 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| c | f | g | h | i | j |

=>

c = "fghij"

Bài toán đảo ngược

* cho bản mã c = "fghij"
* k =5
* n =26
* xác đinh bản rõ p

Quy ước: Số thứ tự của các chữ cái trong bảng chữ cái tiếng anh như sau: a = 0, b = 1, …, z= 25

Bước 1: đổi các ký tự trong c sang thứ tự của chúng trong bảng chữu cái.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| f | g | h | i | j |
| 5 | 6 | 7 | 8 | 9 |

Bước 2: tiến hành giải mã bản c với khóa k=5

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| c | 5 | 6 | 7 | 8 | 9 |
| (c- 5) mode 26 | 0 | 1 | 2 | 3 | 4 |

Bước 3: xác định rõ p

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| (c- 5) mode 26 | 0 | 1 | 2 | 3 | 4 |

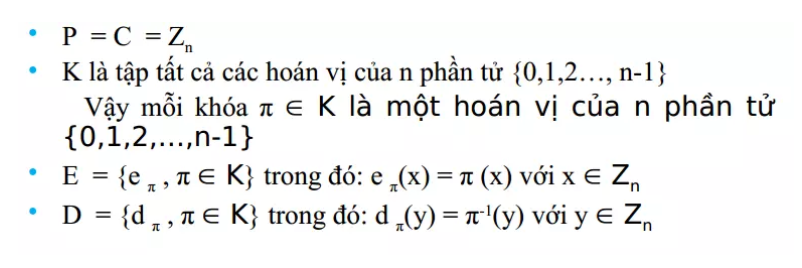
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| p | a | b | c | d | e |

=> p = "abcde"

1.4.2 Mã hóa thay thế

Như vậy khoá trong một cipher loại này là một bảng hoán vị (A →F, b→G, ..., z→L) như trên, hoặc biểu diễn ngắn gọn hơn là bằngdòng thứ hai của phép biến đổi này, tức là FGNT...PL. Dòng thứ nhất của bảng biến đổi này là bảng chữ cái gốc, vì nó là cố định nên không được tính tới trong khoá. Dòng thứ hai, được gọi là bảng thay thế (substitution alphabet). Chú ý rằng không nhất thiết phải dùng một bảng chữ cái mà ta có thể dùng bất cứ một thứ bảng ký hiệu nào đó. Ví dụ 1.2. Ở đây bảng chữ bản

Mã hóa thay thế là một bộ năm thành phần (P, C, K, E, D) thỏa mãn:

****

ví dụ : giải mã với

* c = "yudhk"
* pi được mô tả ở bảng dưới

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| a | b | c | d | e | f | g | h | i | j | k | l | m |
| y | u | d | h | k | e | m | i | l | j | f | p | n |
| n | o | p | q | r | s | t | u | v | w | x | y | Z |
| w | z | t | q | v | x | c | o | r | b | s | g | a |

xác định c=?

ta có c:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| P | a | b | c | d | e |
| c | y | u | d | h | k |

=> c = “yudhk”

Tương tự như trên đối với bài toán ngược cho:

* c = “yudhk”
* π -1 được mô tả như ở bảng bên dưới

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| y | u | d | h | k | e | m | i | l | j | f | p | n |
| a | b | c | d | e | f | g | h | i | j | k | l | m |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| w | z | t | q | v | x | c | o | r | b | s | g | a |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| n | o | p | q | r | s | t | u | v | w | x | y | Z |

ta xác định được p=”abcde”

# 1.4.3 Mã hóa Affine

MDV là một trường hợp đặc biệt của MTT chỉ gồm 26 trong số 26! các hoán vị có thể của 26 phần tử. Một trường hợp đặc biệt khác của MTT là mã Affine được mô tả dưới đây. trong mã Affine, ta giới hạn chỉ xét các hàm mã có dạng: e(x) = ax + b mod 26,

Mã hóa Affine là một bộ năm (P, C, K, E, D) thỏa mãn:

Ví dụ : mã hóa

* p = "abcde"
* k = (a, b) = (5, 3); n =26
* Tính c = ?

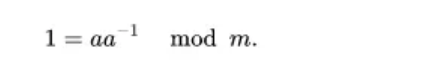
Ta có c :

| **p** | **a** | **b** | **c** | | **d** | **e** |
| --- | --- | --- | --- | --- | --- | --- |
| x | 0 | 1 | | 2 | 3 | 4 |
| (5x +3 ) mod 26 | 3 | 8 | | 13 | 18 | 23 |
| c | d | i | | n | s | x |

> c= "dinsx"

Tương tự với bài toán ngược, cho

* "dinsx"
* k = (a, b) = (5, 3); n= 26; tính được a mũ -1 = 21 từ công thức :

****

* tính p = ?

ta có p :

| **c** | **d** | **i** | **n** | **s** | **x** |
| --- | --- | --- | --- | --- | --- |
| y | 3 | 8 | 13 | 18 | 23 |
| (21(y-3))mod 26 | 0 | 1 | 2 | 3 | 4 |
| p | a | b | c | d | e |

=> p = "abcde"

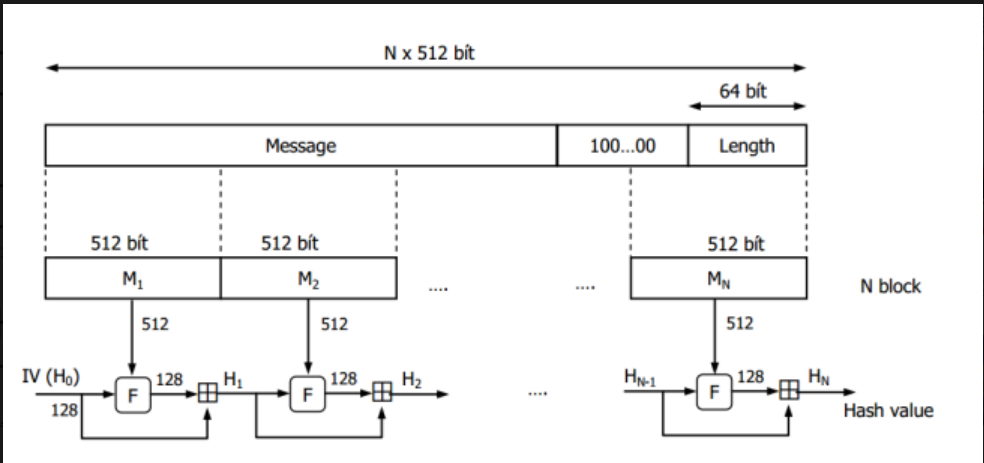
Để giải mã một bản rõ nhận được từ thuật toán mật mã trên, người có bản mã ciphertext cần biết khóa, do đó yêu cầu một giao thức về trao khoá. Đơn giản nhất có thể thực hiện là người gửi tin ghi khoá ra đĩa và chuyển đĩa cho người nhận. Rõ ràng cách làm này đơn giản nhưng thực tế không an toàn. Trong thực tế người ta sử dụng nhiều giao thức phức tạp và tinh vi hơn.

1.4.4 MD5

MD5 được phát minh bởi Ron Rivest ,người đã tham gia xây dựng RSA.MD5 viết tắt của chữ Message Digest,được phát triển lên từ MD4 và trước đó là MD2,do MD2 và MD4 không còn an toàn.Kích thước của MD5 là 128 bit được tính giá trị của thông điệp có kích thước tối đa 2^4 bit

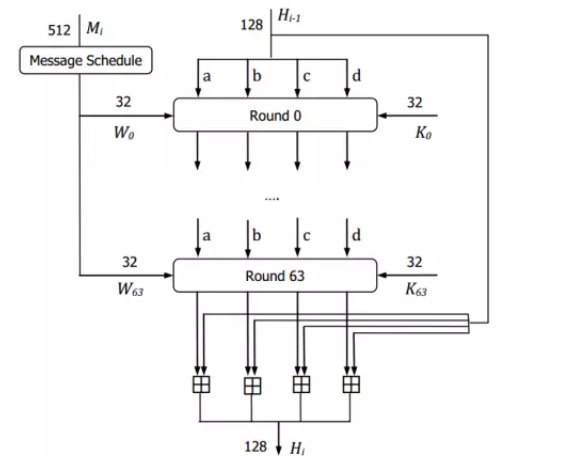
Thuật toán :

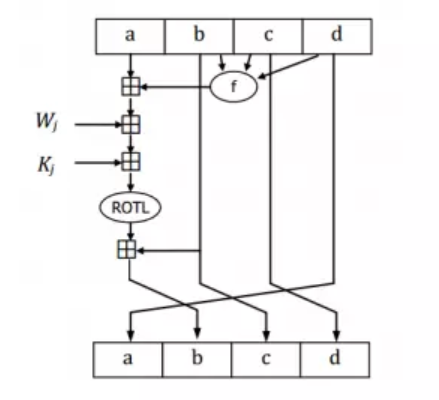
-Input: xâu đầu vào x có độ dài tối đa 2^64 -Output: chuỗi băm 128 bit -Sơ đồ thuật

****

Trước tiên thông điệp được đệm vào dãy padding 100...00. Chiều dài của dãy padding được chọn sao cho thông điệp cuối cùng có thể chia làm N block 512 bit M1,M2,...,MN.Quá trình tính giá trị băm của thông điệp là quá trình lũy tiến. Trước tiên block M1 kết hợp với giá trị khởi tạo H0 thông qua hàm F để tính giá trị hash H1. Sau đó block M2 được kết hợp với H1 để cho ra giá trị hash là H2. Block M3 kết hợp với H2 cho ra giá trị H3. Cứ như vậy cho đến block MN thì có giá trị băm của toàn bộ thông điệp là HN.

* H0 là một dãy 128 bit được chia thành 4 từ 32 bit, ký hiệu 4 từ 32 bit trên là abcd. Với a, b, c, d là các hằng số như sau (viết dưới dạng thập lục phân):  
  a = 01234567  
  b = 89abcdef  
  c = fedbca98  
  d = 76543210  
    
  -Cấu trúc của hàm F như sau:

****

Tại mỗi bước lũy tiến, các giá trị abcd của giá trị hash Hi-1 được biến đổi qua 64 vòng từ 0 đến 63. Tại vòng thứ j sẽ có 2 tham số là Kj và Wj đều có kích thước 32 bit. Các tham số Kj được tính từ công thức: Kj là phần nguyên của số 2^32 abs(sin(i)) với i biểu diễn theo rad.  
Giá trị block Mi 512bit được biến đổi qua một hàm message schedule cho ra 64 giá trị W0, W1…, W63 mỗi giá trị 32 bit. Block Mi 512bit được chia thành 16 block 32bit ứng với các giá trị W0, W1, …, W15 (16×32=512). Tiếp theo, 16 giá trị này được lặp lại 3 lần tạo thành dãy 64 giá trị.  
Sau vòng cuối cùng, các giá trị abcde được cộng với các giá trị abcd của Hi-1 để cho ra các giá trị abcd của Hi. Phép cộng ở đây là phép cộng modulo 232.  
Tiếp theo tìm hiểu cấu trúc của một vòng. Việc biến đổi các giá trị abcd trong vòng thứ i được thể hiện trong hình bên dưới.  


Note:Phép + trong sơ đồ trên là phép cộng modul 2^32  
Ở đây c lấy giá trị của b, d lấy giá trị của c, a lấy giá trị của d.  
Giá trị b được tính qua hàm:  
t = a + f(b,c,d) + Wi + Ki  
b = b + ROTL(t,s)  
Trong đó : Hàm f(x,y,z):  
f (x,y,z) = (x ^ y) v (\_x ^ z) nếu vòng từ 0 đến 15  
f (x,y,z) = (z ^ x) v (\_z ^ y) nếu vòng từ 16 đến 32  
f (x,y,z) = x xor y xor z nếu vòng từ 32 đến 48  
f (x,y,z) = y xor (x v \_z) nếu vòng từ 49 đến 63  
Hàm ROTL(t, s): t được dịch vòng trái s bit, với s là các hằng số cho vòng thứ i như sau:

Khi sử dụng cùng một thuật toán băm sẽ trả về các kết quả tương tự. Tức là bạn có thể sử dụng cùng một MD5 calculator để lấy mã MD5 của một số văn bản cụ thể, sau đó sử dụng MD5 calculator khác cũng sẽ nhận được kết quả tương tự. Điều này có thể lặp lại trên các công cụ tạo mã tổng kiểm dựa trên hàm băm MD5.

* + 1. Mã Vigenère

Trong cả hai hệ MDV và MTT (một khi khoá đã được chọn) mỗi ký tự sẽ được ánh xạ vào một ký tự duy nhất. Vì lý do đó, các hệ mật còn được gọi hệ thay thế đơn biểu. Bây giờ ta sẽ trình bày ( trong hùnh 1.5) một hệ mật không phải là bộ chữ đơn, đó là hệ mã Vigenère nổi tiếng. Mật mã này lấy tên của Blaise de Vigenère sống vào thế kỷ XVI.

Sử dụng phép tương ứng A ⇔ 0, B ⇔ 1, . . . , Z ⇔ 25 mô tả ở trên, ta có thể gắn cho mỗi khoa K với một chuỗi kí tự có độ dài m được gọi là từ khoá. Mật mã Vigenère sẽ mã hoá đồng thời m kí tự: Mỗi phần tử của bản rõ tương đương với m ký tự.

Giả sử m =6 và từ khoá là CIPHER. Từ khoá này tương ứng với dãy số K = (2,8,15,4,17). Giả sử bản rõ là xâu:

Cho m là một số nguyên dương cố định nào đó. Định nghĩa *P = C = K* = (Z26)m . Với khoá K = (k1, k2, . . . ,km) ta xác định :

eK(x1, x2, . . . ,xm) = (x1+k1, x2+k2, . . . , xm+km)

và

dK(y1, y2, . . . ,ym) = (y1-k1, y2-k2, . . . , ym-km)

trong đó tất cả các phép toán được thực hiện trong Z26

Ta sẽ biến đổi các phần tử của bản rõ thành các thặng dư theo modulo 26, viết chúng thành các nhóm 6 rồi cộng với từ khoá theo modulo 26 như sau:

19 7 8 18 2 17 24 15 19 14 18 24

2 8 15 7 4 17 2 8 15 7 4 17

21 15 23 25 6 8 0 23 8 21 22 15

18 19 4 12 8 18 13 14 19 18 4 2

2 8 15 7 4 17 2 8 15 7 4 17

20 1 19 19 12 9 15 22 8 15 8 19

20 17 4

2 8 15

22 25 19

Bởi vậy, dãy ký tự tương ứng của xâu bản mã sẽ là:

V P X Z G I A X I V W P U B T T M J P W I Z I T W Z T

Để giải mã ta có thể dùng cùng từ khoá nhưng thay cho cộng, ta trừ cho nó theo modulo 26.

Ta thấy rằng các từ khoá có thể với số độ dài m trong mật mã Vigenère là 26m, bởi vậy, thậm chí với các giá trị m khá nhỏ, phương pháp tìm kiếm vét cạn cũng yêu cầu thời gian khá lớn. Ví dụ, nếu m = 5 thì không gian khoá cũng có kích thước lớn hơn 1,1 × 107 . Lượng khoá này đã đủ lớn để ngaen ngừa việc tìm khoá bằng tay( chứ không phải dùng máy tính).

Trong hệ mật Vigenère có từ khoá độ dài m,mỗi ký tự có thể được ánh xạ vào trong m ký tự có thể có (giả sử rằng từ khoá chứa m ký tự phân biệt). Một hệ mật như vậy được gọi là hệ mật thay thế đa biểu (polyalphabetic). Nói chung, việc thám mã hệ thay thế đa biểu sẽ khó khăn hơn so việc thám mã hệ đơn biểu.

1.4.5 Mật mã Hill

Trong phần này sẽ mô tả một hệ mật thay thế đa biểu khác được gọi là mật mã Hill. Mật mã này do Lester S.Hill đưa ra năm 1929. Giả sử m là một số nguyên dương, đặt *P = C =*  (Z26)m . Ý tưởng ở đây là lấy m tổ hợp tuyến tính của m ký tự trong một phần tử của bản rõ để tạo ra m ký tự ở một phần tử của bản mã.

Ví dụ nếu m = 2 ta có thể viết một phần tử của bản rõ là x = (x1,x2) và một phần tử của bản mã là y = (y1,y2). Ở đây, y1cũng như y2 đều là một tổ hợp tuyến tính của x1và x2. Chẳng hạn, có thể lấy

y1 = 11x1+ 3x2

y2 = 8x1+ 7x2

Tất nhiên có thể viết gọn hơn theo ký hiệu ma trận như sau

11 8

3 7

(y1 y2) = (x1 x2)

Nói chung, có thể lấy một ma trận K kích thước m × m làm khoá. Nếu một phần tử ở hàng i và cột j của K là ki,,j thì có thể viết K = (ki,,j), với x = (x1, x2, . . . ,xm) ∈ *P* và K ∈*K* , ta tính y = eK(x) = (y1, y2, . . . ,ym) như sau:

(y1,. . .,ym) (x1, . . . ,xm)

k1,1 k1,2 ... k1,m

k2,1 k2,2 ... k2,m

... ... ... . .

km,1 km,2 ... km,m

Nói một cách khác y = xK.

Chúng ta nói rằng bản mã nhận được từ bản rõ nhờ phép biến đổi tuyến tính. Ta sẽ xét xem phải thực hiện giải mã như thế nào, tức là làm thế nào để tính x từ y. Bạn đọc đã làm quen với đại số tuyến tính sẽ thấy rằng phải dùng ma trận nghịch đảo K-1 để giả mã. Bản mã được giải mã bằng công thức y K-1 .

Sau đây là một số định nghĩa về những khái niệm cần thiết lấy từ đại số tuyến tính. Nếu A = (xi,j) là một ma trận cấp l × m và B = (b1,k ) là một ma trận cấp m × n thì tích ma trận AB = (c1,k ) được định nghĩa theo công thức:

m

c1,k  = Σ ai,j bj,k

j=1

Với 1 ≤ i ≤ l và 1 ≤ k ≤ l. Tức là các phần tử ở hàng i và cột thứ k của AB được tạo ra bằng cách lấy hàng thứ i của A và cột thứ k của B, sau đó nhân tương ứng các phần tử với nhau và cộng lại. Cần để ý rằng AB là một ma trận cấp l × n.

Theo định nghĩa này, phép nhân ma trận là kết hợp (tức (AB)C = A(BC)) nhưng noiâ chung là không giao hoán ( không phải lúc nào AB = BA, thậm chí đố với ma trận vuông A và B).

Ma trận đơn vị m × m (ký hiệu là Im ) là ma trận cấp m × m có các số 1 nằm ở đường chéo chính và các số 0 ở vị trí còn lại. Như vậy ma trận đơn vị 2 × 2 là:

1. 0

0 1

Im được gọi là ma trận đơn vị vì AIm = A với mọi ma trận cấp l × m và ImB =B với mọi ma trận cấp m × n. Ma trận nghịch đảo của ma trận A cấp m × m ( nếu tồn tại) là ma trận A-1 sao cho AA-1 = A-1A = Im . Không phải mọi ma trận đều có nghịch đảo, nhưng nếu tồn tại thì nó duy nhất.

I2 =

Với các định nghĩa trên, có thể dễ dàng xây dựng công thức giải mã đã nêu: Vì y = xK, ta có thể nhân cả hai vế của đẳng thức với K-1 và nhận được:

yK-1 = (xK)K-1 = x(KK-1) = xIm = x

( Chú ý sử dụng tính chất kết hợp)

Có thể thấy rằng, ma trận mã hoá ở trên có nghịch đảo trong Z26:

1. 8

3 7

-1

=

1. 18

23 11

vì

1. 8

3 7

1. 18

23 11

=

11×7+8×23 11×18+8×11

3×7+7×23 3×18+7×11

Hãy nhớ rằng mọi phép toán số học đều được thực hiện theo modulo 26).

=

261 286

182 131

=

1. 0

0 1

Sau đây là một ví dụ minh hoạ cho việc mã hoá và iải mã trong hệ mật mã Hill.

Via dụ

1. 8

3 7

=

Từ các tính toán trên ta có:

1. 18

23 11

K-1 =

Giả sử khoá K

Giả sử cần mã hoá bản rõ "July". Ta có hai phần tử của bản rõ để mã hoá: (9,20) (ứng với Ju) và (11,24) (ứng với ly). Ta tính như sau:

va Bởi vậy bản mã của July là DELW. Để giải mã Bob sẽ tính

(9,20)

1. 8

3 7

= (99+60, 72+140) = (3,4)

(11,24)

1. 8

3 7

= (121+72, 88+168) = (11,22)

(11,22)

1. 18

23 11

= (11,24)

(3,4)

1. 18

23 11

= (9,20)

và

Như vậy Bob đã nhận được bản đúng. Cho tới lúc này ta đã chỉ ra rằng có thể thực hiện phép giải mã nếu K có một nghịch đảo. Trên thực tế, để phép giải mã là có thể thực hiện được, điều kiện cần là K phải có nghịch đảo. ( Điều này dễ dàng rút ra từ đại số tuyến tính sơ cấp, tuy nhiên sẽ không chứng minh ở đây). Bởi vậy, chúng ta chỉ quan tâm tới các ma trận K khả nghich.

Tính khả nghịch của một ma trận vuông phụ thuộc vào giá trị định thức của nó. Để tránh sự tổng quát hoá không cần thiết, ta chỉ giới hạn trong trường hợp 2×2.

Định nghĩa

*Định thức của ma trận A = (a,i j ) cấp 2× 2 là giá trị*

*det A = a1,1 a2,2 - a1,2 a2,1*

*Nhận xét:* Định thức của một ma trận vuông cấp mm có thể được tính theo các phép toán hằng sơ cấp: hãy xem một giáo trình bất kỳ về đại số tuyến tính.

Hai tính chất quan trọng của định thức là det Im = 1 và quy tắc nhân det(AB) = det A × det B.

Một ma trận thức K là có nghịch đảo khi và chỉ khi định thức của nó khác 0. Tuy nhiên, điều quan trọng cần nhớ là ta đang làm việc trên Z26 . Kết quả tương ứng là ma trận K có nghịch đảo theo modulo 26 khi và chỉ khi UCLN(det K,26) = 1.

Sau đây sẽ chứng minh ngắn gọn kết quả này.

Trước tiên, giả sử rằng UCLN(det K,26) = 1. Khi đó det K có nghịch đảo trong Z26 . Với 1 ≤ i ≤ m, 1 ≤ j ≤ m, định nghĩa Ki j ma trận thu được từ K bằng cách loại bỏ hàng thứ i và cột thứ j. Và định nghĩa ma trận K\* có phần tử (i,j) của nó nhận giá trị(-1) det Kj i (K\* được gọi là ma trận bù đại số của K). Khi đó có thể chứng tỏ rằng:

K-1 = (det K)-1K\* .

Bởi vậy K là khả nghịch.

Ngược lại K có nghịch đảo K-1 . Theo quy tắc nhân của định thức

1 = det I = det (KK-1) = det K det K-1

Bởi vậy det K có nghịch đảo trong Z26 .

Nhận xét: Công thức đối với ở trên không phải là một công thức tính toán có hiệu quả trừ các trường hợp m nhỏ ( chẳng hạn m = 2, 3). Vớim lớn, phương pháp thích hợp để tính các ma trận nghịch đảo phải dựa vào các phép toán hằng sơ cấp.

Trong trường hợp 2×2, ta có công thức sau: *Giả sử A = (ai j) là một ma trận cấp 2 × 2 trên Z26 sao cho det A = a1,1a2,2 - a1,2 a2,1 có nghịch đảo. Khi đó*

A-1 = (det A)-1

a2,2 -a1,2

-a2,1 a1,1

Trở lại ví dụ đã xét ở trên . Trước hết ta có:

det

1. 8

3 7

= 11 × 7 - 8 ×3 mod 2

= 77 - 24 mod 26 = 53 mod 26

= 1

Vì 1-1 mod 26 = 1 nên ma trận nghịch đảo là

1. 8

3 7

-1

=

1. 18

23 11

Đây chính là ma trận đã có ở trên.

Bây giờ ta sẽ mô tả chính xác mật mã Hill trên Z26 (hình 1.6)

Cho m là một số nguyên dương có định. Cho *P = C =* (Z26 )m và cho

*K*  = { các ma trận khả nghịch cấp m × m trên Z26}

Với một khoá K ∈*K* ta xác định

eK(x) = xK

và dK(y) = yK -1

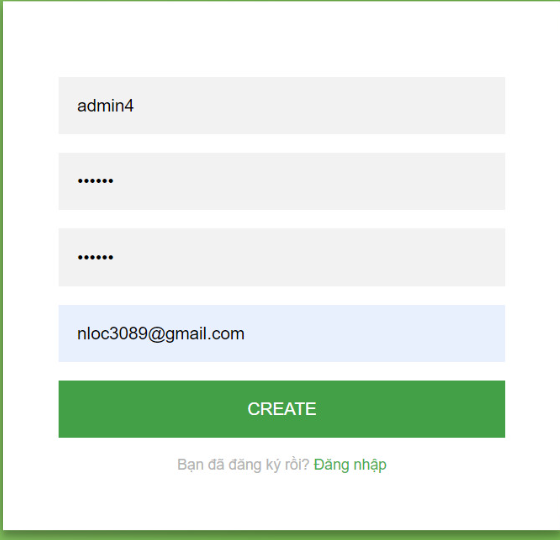
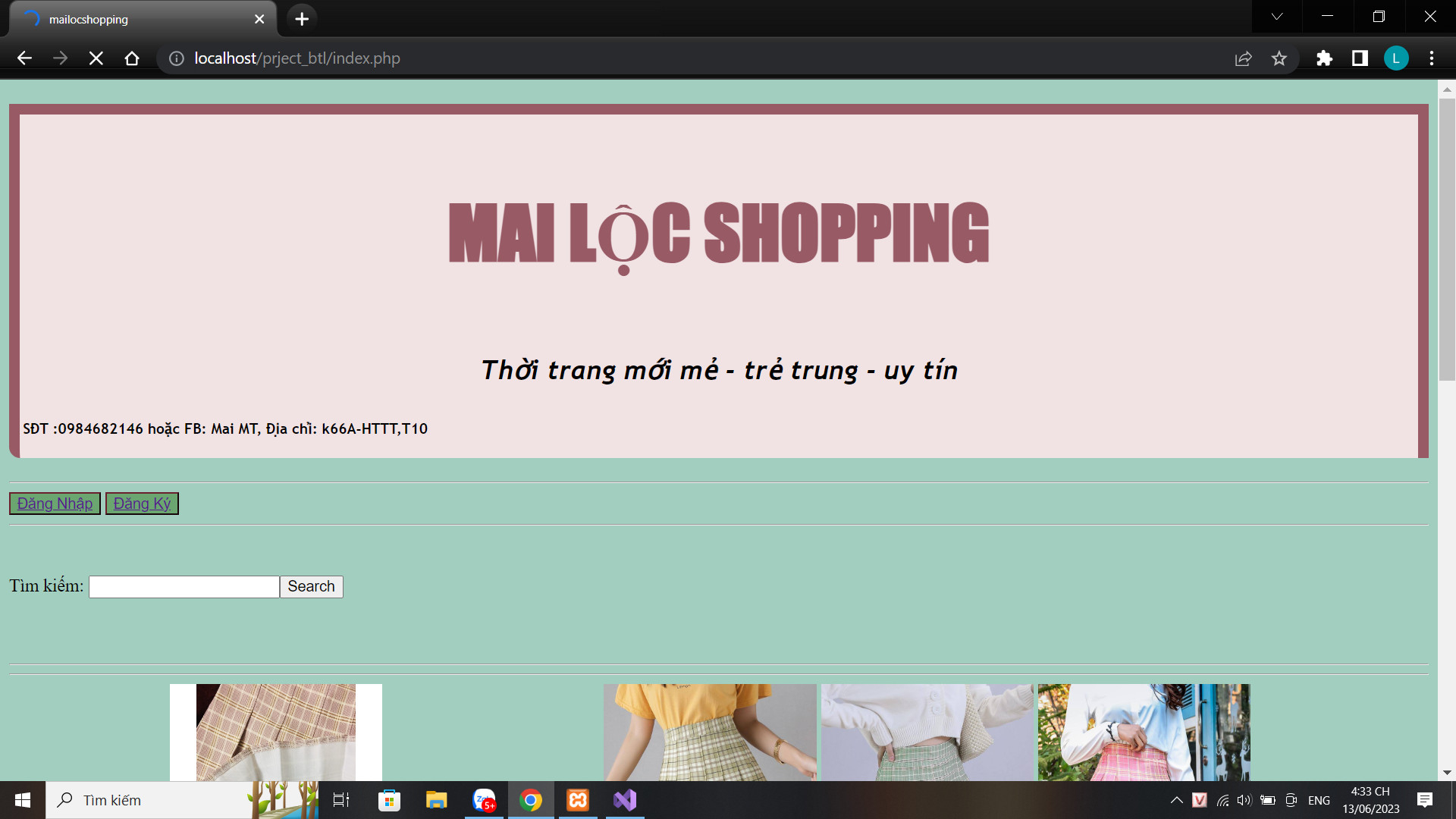
Tất cả các phép toán được thực hiện trong Z26

Phần II: THIẾT LẬP BẢO MẬT CHO WEB TỰ LẬP

2.1 Chuẩn bị

Tạo lập phần web sử dụng html để tạo lập. Giao diện đơn giản, tối giản nhất có thể. Có đầy đủ các thành phần cần thiết trong một trang web ( đăng nhập/ đăng xuất/ tìm kiếm…)

Các form cũng được tạo lập đơn giản bằng php chứa các thông tin thuộc tính được thiết lập trong database. Bao gồm các thông tin cần khai thác và lưu trữ từ khách hàng.



2.2 Thiết lập bảo mật:

Để tiến hành bảo mật không thể không kể đến thành phần dữ liệu. thông tin đăng nhập sau khi được nhập vào form nhập sẽ được sử lý chuyển đổi trước khi được lưu tự động vào bảng chứa dữ liệu. vậy thì chngs sẽ được xủa lí như thế nào? Dung thuật toán nào để mã hóa và giải mã.

Sau quá trình học tập và tìm hiểu chúng em cũng biết đến cả các thuật toán mã hóa hiện đại và cổ điển, tuy vậy do tính chất phức tạp của các thuật toán hiện đại nên nhóm quyết định sử dụng một thuật toán cổ điển. phía trên, nhóm đã đưa ra một vài thuật toán mã hóa cổ điển trong đó có thuật toán MD5 và nhóm đã lựa chọn để dung trong đồ an bảo mật của nhóm.

Hơn hết MD5 là một thuật toán đac được giảng viên hướng dẫn trực tiếp và cụ thể trong quá trình giảng dạy và cũng vì MD5 có phần dễ hiểu hơn các thuật toán còn lại.

Thêm một phần thuận lợi nữa MD5 được thiết lập sẵn trên một số phần mềm lập trình nên cũng đem lại sự thuận tiện nhất định trong quá trình sử dụng.

Quá trình sử dụng nhóm đã cho ra được kết quả như sau:

Khi người dung điền mật khẩu vào form đăng ký, hệ thống sẽ kiểm tra bằng lệnh check. Điều kiện thảo mãn đăng nhập thành công là không được để trống/ NULL, mật khẩu nhắc lại phải trùng khớp với mật khẩu được nhập trước đó, hoặc thông tin dăng ký trùng khớp với thông tin đã có trong bẳng chứa thông tin hệ thống. nếu vi phạm 1 trong các điều kiện hệ thống lập tức sẽ xuất ra các dòng thông báo, đồng thời yêu cầu người dung điền lại thông tin. Ngược lại khi mội điều kiện được thảo mãn hệ thống sẽ xuất thông báo thành công đăng ký. các thông tin vừa rồi được thêm tự động vào bẳng chứa dữ liệu trong database với phần mật khẩu được mã hóa thành một dãy ký tự hoàn toàn khác chuôi ký tự ban đầu theo dạng random. Đồng thời chuyển giao diện ra form đăng nhập web.

Khi người dung điền thông tin đăng nhập, hệ thống so sánh cột mật khẩu ứng với tên đăng nhập trong bảng chứa. quy chế ở đây là mật khẩu nhập vào sẽ được mã hóa trước khi so sánh với bảng chứa trước đó. Nếu mật khẩu không trùng khớp sẽ có thông báo không thể đăng nhaapjra màn hình. Nếu đúng giao diện được chuyển qua trang chính của trang web được lập trước đó. Trong trường hợp thông tin điền ngay từ mục tên đăng nhập đương nhiên thông tin k tồn tại trong bẳng dữ kiệu sẽ có thông báo hiển thị tài khoản không tồn tại. người dung buộc phải nhập lại hoặc quay lại đăng ký trước.

Mật khẩu do người dung thiết lập rất nahnh chóng được chuyển đổi phức tạp hơn, dài hơn đảm bảo bảo mật một phần cho thông tin của khách hàng-người sử dụng

2.3 Bài học, nhận xét nhóm sau quá trình thực hiện đồ án:

Cả hai thành viên nhóm tự nhận thấy rằng mình còn nhiều hạn chế trong phạm vi này. Rõ rang nhất là kể từ khi nhóm chọn đề tài làm đồ án. Cả hai thành viên còn chưa tiếp xúc với taọ lập web nhưng đã chọn web đó là một điều thwucj sự khó khắn trong quá trình làm việc nhóm. Chính vì thế mà nhóm cũng đã mất khá nhiều thời gian để nguyên cứu và tìm hiểu về web và các tạo lập web. May mắn sau khi hiểu được phần nào vấn đề, từng phần của trang web đã dần được hoàn thành.

Tuy vậy do còn nhiều thiếu sót chính vì thế mà phần giao diện cũng như chức năng của trang web còn khá sơ sài, thiếu thẩm mỹ. Một phần cũng do thời gian không đủ sau tổng kết nhóm thấy phần mã hóa mật khẩu còn chưa đủ mạnh mẽ. có thể trong qúa trình học tập trải nghiệm sắp tới từng phần còn tồn tại sẽ được bù đắp và trau dồi hơn nữa.

Bài học rút ra của nhóm: tập trung tìm hiểu nội dung chủ chốt, tránh chủ quan, tìm thông tin từ những nguồn uy tín và chuẩn xác.