LỜI CẢM ƠN

Trước tiên, em xin gửi lời cảm ơn chân thành sâu sắc tới các thày cô giáo trong trường Đại học dân lập Hải Phòng nói chung và các thày cô giáo trong khoa Công nghệ Thông tin nói riêng đã tận tình giảng dạy, truyền đạt cho em những kiến thức, kinh nghiệm quý báu trong suốt thời gian qua.

Đặc biệt em xin gửi lời cảm ơn đến thày Trần Ngọc Thái, thày đã tận tình giúp đỡ, trực tiếp chỉ bảo, hướng dẫn em trong suốt quá trình làm đồ án tốt nghiệp. Trong thời gian làm việc với thày, em không ngừng tiếp thu thêm nhiều kiến thức bổ ích mà còn học tập được tinh thần làm việc, thái độ nghiên cứu khoa học nghiêm túc, hiệu quả, đây là những điều rất cần thiết cho em trong quá trình học tập và công tác sau này.

Sau cùng, xin gửi lời cảm ơn chân thành tới gia đình, bạn bè đã động viên, đóng góp ý kiến và giúp đỡ trong quá trình học tập, nghiên cứu và hoàn thành đồ án tốt nghiệp.

MỤC LỤC

MỞ ĐẦU

Khi ứng dụng trên mạng máy tính càng trở lên phổ biến, thuận lợi và quan trọng thì yêu cầu về an toàn mạng, an ninh dữ liệu mạng ngày càng trở lên cấp bách và cần thiết. Nguồn tài nguyên mạng rất dễ bị đánh cắp hoặc phá hỏng nếu không có một cơ chế bảo mật cho chúng hoặc sử dụng những cơ chế bảo mật quá lỏng lẻo. Thông tin trên mạng, dù đang truyền hay được lưu trữ đều cần được bảo vệ. Các thông tin ấy phải được giữ bí mật. Cho phép người ta kiểm tra để tin tưởng rằng chúng không bị sửa đổi so với dạng nguyên thủy của mình và chúng đúng là của người nhận gửi nó cho ta.Mạng máy tính có đặc điểm là nhiều người sử dụng, nhiều người cùng khai thác kho tài nguyên, đặc biệt là tài nguyên thông tin và người sử dụng thường phân tán về mặt địa lí. Các điểm này thể hiện lợi ích to lớn của mạng thông tin máy tính đồng thời cũng là điều kiện thuận lợi cho những kẻ muốn phá hoại an toàn thông tin trên mạng máy tính.

Do đó cách tốt nhất để bảo vệ thông tin là mã hóa thông tin trước khi gửi đi. Mục tiêu cơ bản của mật mã là cho phép hai người, giả sử là A và B, liên lạc qua kênh không an toàn theo cách mà đối thủ O (được nói đến như người thám mã) khó có thể hiểu cái gì đang được nói. Kênh này có thể là đường điện thoại hoặc mạng máy tính. Thông tin A muốn gửi đến B sẽ được gọi là "bản rõ" (plaintext), có thể là bất kì tài liệu nào có cấu trúc tùy ý. A sẽ mã bản rõ bằng khóa xác định trước và gửi bản mã thu được qua kênh không an toàn. O dù thu trộm được bản mã trên kênh nhưng khó có thể hiểu bản mã đó là gì nhưng B là người biết khóa mã nên có thể giải mã và thiết lập lại bản rõ. Có hai loại hệ mật gồm hệ mật mã khóa bí mật và hệ mật mã khóa công khai. Trong hệ mật mã khóa công khai, hai người muốn trao đổi thông tin với nhau phải thỏa thuận với nhau một cách bí mật khóa k. Trong hệ mật này có hai hàm lập mã e_k và hàm giải mã d_k. Nếu tiết lộ khóa k sẽ làm cho hệ thống không an toàn. Trong thực tế, Độ an toàn hệ thống chính là độ an toàn tính toán. Một hệ mật là "an toàn tính toán" nếu phương pháp tốt nhất đã biết để phá nó yêu cầu một số lớn không hợp lý thời gian tính toán, nghĩa là quá trình thực hiện tính toán cực kỳ phức tạp, phức tạp đến mức ta coi"không thể được". Hệ mã khóa công khai đã đáp ứng được yêu cầu đó. Ý tưởng của hệ mã khóa công khai là ở chỗ nó có thể tìm ra một hệ mã khó có thể tính toán xác định d_k khi biết e_k, quy tắc mã e_k có thể công khai. Hàm mã hóa công khai e_k phải dễ dàng tính toán nhưng việc giải mã phải khó đối với bất kì người nào ngoài người lập mã. Tính chất dễ tính toán và khó đảo ngược này thường được gọi là tính chất một chiều. Điều này bảo đảm tính bí mật cao. Như chúng ta đã biết,

trong cách thức giao dịch truyền thống, thông báo được truyền đi trong giao dịch thường dưới dạng viết tay hoặc đánh máy kèm theo chữ ký(viết tay) của người gửi ở bên dưới văn bản. Chữ ký đó là bằng chứng xác nhận thông báo đúng là của người ký, tức là chủ thể giao dịch. Chữ ký viết tay có nhiều ưu điểm đó là dễ kiểm thử, không sao chép được chữ ký của một người là giống nhau trên nhiều văn bản…

Ngày nay, cùng với sự phát triển của khoa học và công nghệ thông tin đặc biệt là sự bùng nổ của mạng máy tính thì nhu cầu trao đổi thông tin trên mạng ngày càng phổ biến. Khi chúng ta chuyển sang cách thức truyền tin bằng các phương tiện hiện đại, các thông báo được truyền đi trên các mạng truyền tin số hóa, song song với nó, tính an toàn và bảo mật thông tin cũng phát triển mạnh mẽ không ngừng đáp ứng như cầu bảo vệ riêng tư của người sử dụng.

Đồ án trình bày một khía cạnh nhỏ về bảo mật thông tin trong thương mại điện tử. Xây dựng lên một trang web về đấu giá trực tuyến và xác thực các thông tin an toàn và bảo mật trong việc mua bán, thanh toán hang hóa mà người bán cũng như người mua chỉ cần ngồi tại nhà với một cú click chuột.

Đồ án gồm 4 chương: Chương 1 Mật mã, Chương 2 Ký điện tử và vấn đề xác thực, Chương 3 Đấu giá điện tử, Chương 4 Ứng dụng đấu giá điện tử.

DANH MỤC HÌNH VẼ

MẬT MÃ

1.1. Sơ lược về lịch sử mật mã

Từ khi còn người có nhu cầu trao đổi thông tin, thư từ cho nhau thì nhu cầu giữ bí mật và bảo vệ tính riêng tư của những thông tin, thừ từ được trao đổi cũng nảy sinh. Hình thức thông tin được trao đổi phổ biến và sớm nhất là dưới dạng văn bản, để giữ bí mật của thông tin họ đã sớm nghĩ đến việc che giấu nội dung các văn bản bằng cách biến dạng các văn bản đó để người đọc không hiểu được, đồng thời có cách khôi phục lại nguyên dạng ban đầu để người trong cuộc vẫn đọc hiểu được; theo cách gọi ngày nay thì dạng biến đổi của văn bản được gọi là mật mã của văn bản, cách lập mật mã cho một văn bản được gọi là phép lập mật mã, còn cách khôi phục lại nguyên dạng ban đầu của văn bản từ bản mật mã gọi là phép giải mã. Phép lập mật mã và phép giải mã được thực hiện nhờ một chìa khóa riêng nào đó mà chỉ những người trong cuộc biết được ta gọi là khóa mật mã. Người ngoài cuộc không biết được khóa mật mã, nên dù có được bản mật mã trên dường truyền tin, về nguyên tắc thì cũng không thể giải mã để hiểu được nội dung của văn bản truyền đi.

Đến các thập niên gần đây, khi con người bước vào kỷ nguyên máy tính, hay trong nhiều các lĩnh vực khác, lĩnh vực mật mã cũng có những chuyển biến to lớn từ giai đoạn mật mã truyền thống sang giai đoạn mật mã máy tính; máy tính điện tử được sử dụng ngày càng phổ biến trong việc lập mật mã, giải mật mã, và những chuyển biến đó đã kích thích việc nghiên cứu các giải pháp mật mã,biến việc nghiên cứu mật mã thành một khoa học có đôi tượng ngày càng rộng lớn và được sử dụng có hiệu quả trong nhiều phạm vi hoạt động của cuộc sống.

Việc chuyển sang giai đoạn mật mã máy tính đã có tác dụng phát triển và hiện đại hóa nhiều hệ thống mật mã theo kiểu truyền thống, làm cho các hệ thống đó có các cấu trúc tinh tế hơn, đòi hỏi lập mật mã và giải mã phức tạp hơn, do đó hiệu quả giữ bí mật của các giải pháp mật mã được nâng cao hơn trước rất nhiều.

1.2. Sơ đồ hệ thống mật mã

1.2.1. Hướng tiếp cận

Mật mã được sử dụng để bảo vệ tính bí mật của thông tin khi thông tin được truyền trên các kênh truyền thông công cộng như các kênh bưu chính, điện thoại, mạng truyền thông máy tính, internet…

Giả sử một người gửi A muốn gửi đến một người nhận B một văn bản(ví như như một bức thư)p, để bảo mật, A lập cho p một bản mã c, và thay cho việc gửi p, A gửi cho B bản mật mã c, B nhận được c và giải mã c để lại được văn bản p như A định gửi. Để A biến p thành c và B biến ngược lại c thành p, A và B phải thỏa thuận trước với nhâu các thuật toán lập mã và giải mã, và đặc biệt một khóa mật mã chung K để thực hiện các thuật toán đó. Người ngoài không biết các thông tin đó(đặc biệt không biết khóa K), cho dù có được c trên kênh truyền thông công cộng, cũng không thể tìm được văn bản p mà hai người A, B muốn gửi cho nhau.

1.2.2. Định nghĩa

Một sơ đồ hệ thống mật mã là 1 bộ năm:

S= (P, C, K, E, D) (1.1)

thỏa mãn các điều kiện sau đây:

P là một tập hữu hạn các ký tự bản rõ,

C là một tập hữu hạn các ký tự bản mã,

K là tập hữu hạn các khóa,

E là một ánh xa từ KxP vào C, được gọi là phép lập mã;

D là một ánh xạ từ KxC vào P, được gọi là phép giải mã.

Với mỗi $k \in K$, ta định nghĩa $e_k : P \rightarrow C$, $d_k : C \rightarrow P$ là hai hàm cho bởi:

$$\begin{cases} \forall x \varepsilon P : \ e_k(x) = E(K,x); \\ \forall y \varepsilon C : d_k(y) = D(K,y) \end{cases} \quad (1.2)$$

e_k và d_k được gọi lần lượt là hàm lập mã và hàm giải mã ứng với khóa mật mã K.

Các hàm đó phải thỏa mãn hệ thức:)x ε P : $d_k(e_k(x)) = x$

Về sau, để thuận tiện ta sẽ gọi một danh sách (1.1) thỏa mãn các tính chất kể trên là một sơ đồ hệ thống mật mã, còn khi đã chọn cố định một khóa K, thì danh sách (P, C, K, e_k, d_k) là một hệ mật mã thuộc sơ đồ đó.

Trong định nghĩa này, phép lập mã (giải mã) được định nghĩa cho từng ký tự bản rõ (bản mã). Trong thực tế, bản rõ của một thông báo thường là một dãy ký tự bản rõ, tức là phần tử của tập P*, và bản mã cũng là một dãy các ký tự bản mã, tức là phần tử của tập C*, việc mở rộng các hàm e_k và d_k lên các miền tương ứng P* và C* để được các thuật toán lập mã và giải mã dùng trong thực tế sẽ được trình bày trong phần sau. Các tập ký tự bản rõ và bản mã thường dùng là các tập ký tự của ngôn ngữ thông thường như tiếng Việt, tiếng Anh (ta ký hiệu tập ký tự tiếng Anh là A tức A= {a,b,c…,x,y,z} gồm 26 ký tự; tập ký tự nhị phân B chỉ gồm 2 ký tự 0 và 1; tập các số nguyên không âm bé hơn một số n nào đó(ta ký hiệu tập này là Zn tức Zn = {0,1,2…, n-1}). Chú ý có thể xem B = Z_2. Để thuận tiện, ta cũng thường đồng nhất tập ký tự tiếng anh A với tập gồm 26 số nguyên không âm đầu tiên Z_{26} = {0,1,2,3…,24,25} với sự tương ứng sau đây:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Đôi khi ta cũng dùng với tư cách tập ký tự bản rõ hay bản mã là các tập tích của các tập nói trên, đặc biệt là các tập A^m, B^m, Z^m_n.

1.3. Các hệ mã hóa

1.3.1. Hệ mã hóa khóa đối xứng (một số hệ mật mã cổ điển)

1.3.1.1. Mã chuyển dịch (shift cipher)

a) Sơ đồ khóa

Kí hiệu Z_m là tập các số nguyên từ 0 đến (m-1), ký hiệu đó cũng dùng cho vành các số nguyên từ 0 đến (m-1) với các phép cộng và nhân với modulo m. Như vậy, bảng chữ cái tiếng Anh có thể xem là một vành Z_{26} với sự tương ứng kể trên.

S= (P, C, K, E, D)

Trong đó: $P = C = K = Z_{26}$

$k \in K$, các ánh xạ E và D được cho bởi:

$$\forall K, x, y \in Z_{26}: \begin{cases} e_k(x) = (x+k) \bmod 26 \\ d_k(y) = (yk) \bmod 26 \end{cases} \quad (1.3)$$

b) Ví dụ

Ta dùng với khóa k = 5 để mã hóa dòng thư: ”hentoithubay”

Dòng thư đó sẽ tưng ứng với dòng số sau:

h	e	n	t	o	i	t	h	u	b	a	y
7	4	13	19	14	18	19	7	20	1	0	24

Qua phép mã hóa e_9 ta được:

16	13	22	2	23	17	2	16	3	10	9	7
q	n	w	c	x	r	c	q	d	k	j	h

bản mã sẽ là :”qnwcxrcqdkjh”

Muốn giải được bản mã đó ta sử dụng d_9 để nhận được bản rõ.

c) Ưu, nhược điểm

Cách đây 2000 năm mã dịch chuyển đã được Julius Ceasar sử dụng, với khóa k=3 mã dịch chuyển dược gọi là mã Ceasar.

Tập khóa phụ thuộc vào Zm với m là số khóa có thể, và trong tiếng Anh tập khóa chỉ có 26 khóa có thể. Do vậy việc thám mã sẽ duyệt tuần tự 26 khóa đó, vì vậy độ an toàn của mã dịch chuyển là rất thấp.

1.3.1.2. *Mã thay thế (substitution cipher)*

a) Sơ đồ khóa

S= (P, C, K, E, D)

$P=C= Z_{26}$, $K= S(Z_{26})$

Với mỗi $\pi \in K$, tức là một hóa vị trên Z_{26} ta xác định:

$$\begin{cases} e\pi(x) = \pi(x) \\ d\pi(y) = \pi^{-1}(y) \end{cases}$$

với $x,y \in Z_{26}$, π^{-1} là nghịch đảo của π.

Chú ý: khóa của mã thay thế là một hoán vị của bảng chữ cái. Gọi S(E) là tập hợp tất cả các phép hoán vị các phần tử của E.

b) Ví dụ

π được cho bởi (chữ cái thay cho các con số thuộc Z_{26})

a	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*	*n*
x	*n*	*y*	*a*	*h*	*p*	*o*	*g*	*z*	*q*	*w*	*b*	*t*	*s*

o	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*w*	*x*	*y*	*z*
f	*l*	*r*	*c*	*v*	*m*	*u*	*e*	*k*	*j*	*d*	*i*

Bản rõ: "hentoithubay" sẽ được mã hóa thành bản mã (với khóa π): "ghsmfzmgunxd".

Dễ xác định được π^{-1}, và do đó từ bản mã ta tìm được bản rõ.

c) Ưu, nhược điểm

Mã thay thế có tập khóa khá lớn, bằng số các hoán vị trên bảng chữ cái, tức số các hoán vị trên Z_{26}, hay 26!. Việc duyệt toàn bộ các hoán vị để thám mã là rất khó, ngay cả đối với máy tính. Tuy nhiên có rất nhiều các phương phấp thám mã khác nên mã thay thế cũng không thể xem là an toàn.

1.3.1.3. *Mã Anpphin*

a) Sơ đồ khóa

S= (P, C, K, E, D)

P= C = Z_{26}, K= {(a,b) $\in$ Z_{26}x Z_{26}: (a,26)=1}

Với mỗi k =(a,b) ∈ K ta định nghĩa:

$$\begin{cases} e_k(x) = ax + b \bmod 26 \\ d_k(y) = a^{-1}(y-b) \bmod 26 \end{cases}$$

trong đó x,y ∈ Z_{26}

Ta có: (a,m) =1 và a^{-1}mod m khi (a,m) =1

Với m =26 ta sẽ tìm ra a thỏa mãn (a,26) =1:

a	*1*	*3*	*5*	*7*	*9*	*11*	*15*	*17*	*19*	*21*	*23*	*25*
a^{-1}	*1*	*9*	*21*	*15*	*3*	*19*	*7*	*23*	*11*	*5*	*17*	*25*

b) Ví dụ

Lấy k =(5,6)

Bản rõ: “hentoithubay”

	h	*e*	*n*	*t*	*o*	*i*	*t*	*h*	*u*	*b*	*a*	*y*
x	*7*	*4*	*13*	*19*	*14*	*8*	*19*	*7*	*20*	*1*	*0*	*24*
y = 5x + 6 mod 26												
y	*15*	*0*	*19*	*23*	*24*	*20*	*23*	*15*	*2*	*11*	*6*	*22*
	p	*a*	*t*	*x*	*y*	*u*	*x*	*p*	*c*	*l*	*g*	*w*

Bản mã “patxyuxpclgw”

Thuật toán giải mã trong trường hợp này có dạng:$d_k(y) = 21(y - 6) \bmod 26$

c) Ưu, nhược điểm

Với mã Apphin, số các khoá có thể có bằng (số các số ≤ 26 và nguyên tố với 26) ×26, tức là 12 × 26 = 312. Việc thử tất cả các khoá để thám mã trong trường hợp này tuy khá mất thì giờ nếu tính bằng tay, nhưng không khó khăn gì nếu dùng máy tính. Do vậy, mã Apphin cũng không phải là mã an toàn.

1.3.1.4. Mã Hill

a) Sơ đồ khoá

Mã này được đề xuất bởi Lester S.Hill năm 1929. Mã cũng được thực hiện trên từng bộ m ký tự, mỗi ký tự trong bản mã là một tổhợp tuyến tính (trên vành Z_{26}) của m ký tự trong bản rõ. Như vậy, khoá sẽ được cho bởi một ma trận cấp m, tức là một phần tử của Z^{mxm}_{26}. Để phép biến đổi tuyến tính xác định bởi ma trận $k \in Z^{mxm}_{26}$ có phép nghịch đảo, ma trận k cũng phải có phần tử nghịch đảo $k^{-1} \in Z^{mxm}_{26}$. Điều kiện cần và đủ để ma trận k có ma trận nghịch đảo là định thức của nó - ký hiệu det(k),- nguyên tố với m.

S= (P, C, K, E, D)

Cho m là số nguyên dương.

$P = C = Z^m_{26}$

$K = \{ k\ Z^{mxm}_{26} :\ (det(k), 26) = 1 \}$

với mỗi $k \in K$ định nghĩa:

$$\begin{cases} e_k(x_1, x_2,\ldots, x_m) = (x_1, x_2,\ldots, x_m).k \\ d_k(y_1, y_2,\ldots, y_m) = (y_1, y_2,\ldots,y_m).k^{-1} \end{cases}$$

b) Ví dụ

Lấy m =2, và $k = \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix}$

Với bộ 2 ký tự (x1, x2), ta có mã là (y1, y2) = (x1, x2). k được tính bởi:

$$\begin{cases} y1 = 11.x1 + 3.x2 \\ y2 = 8.x1 + 7.x2 \end{cases}$$

Giả sử ta có bản rõ: “tudo”, tách thành từng bộ 2 ký tự, và viết dưới dạng số ta được 19 20 | 03 14, lập bản mã theo quy tắc trên, ta được bản mã dưới dạng số là: 09 06 | 23 18, và dưới dạng chữ là “fgxs”.

c) Ưu, nhược điểm

Độ an toàn cũng không cao

1.3.1.5. Mã Vigennère

a) Sơ đồ khóa

Mã lấy tên của Blaise de Vigenēre, sống vào thế kỷ 16. Khác với các mã trước, mã Vigenēre không thực hiện trên từng ký tự một, mà được thực hiện trên từng bộ m ký tự (m là số nguyên dương).

S= (P, C, K, E, D)

Cho m là số nguyên dương.

$P = C = K = Z^m_{26}$

với mỗi khoá $k = (k1, k2,\ldots,km) \in K$ có:

$$\begin{cases} e_k(x_1, x_2,\ldots, x_m) = (x_1 + k_1, x_2 + k_2,\ldots, x_m + k_m) \\ d_k(y_1, y_2,\ldots, y_m) = (y_1 - k_1, y_2 - k_2,\ldots, y_m - k_m) \end{cases}$$

các phép cộng phép trừ điều lấy theo modulo 26

b) Ví dụ

Giả sử m = 6 và khoá k là từ CIPHER - tức k=(2, 8, 15, 7, 4, 17).

Bản rõ: “hentoithubay”

	h	*e*	*n*	*t*	*o*	*i*	*t*	*h*	*u*	*b*	*a*	*y*
x	*7*	*4*	*13*	*19*	*14*	*8*	*19*	*7*	*20*	*1*	*0*	*24*
k	***2***	***8***	***15***	***7***	***4***	***17***	***2***	***8***	***15***	***7***	***4***	***17***
y	*9*	*12*	*2*	*0*	*18*	*25*	*21*	*15*	*9*	*8*	*4*	*15*
	j	*m*	*c*	*a*	*s*	*z*	*v*	*p*	*j*	*i*	*e*	*p*

Bản mã: “jmcaszvpjiep”

Từ bản mã đó, dùng phép giải mã dk tương ứng, ta lại thu được bản rõ.

c) Ưu, nhược điểm

Mã Vigenēre với m = 1 sẽ trở thành mã Dịch chuyển. Tập hợp các khoá trong mã Vigenēre mới m ≥ 1 có tất cả là 26m khoá có thể có. Với m = 6, số khoá đó là 308.915.776, duyệt toàn bộ chừng ấy khoá để thám mã bằng tính tay thì khó, nhưng với máy tính thì vẫn là điều dễ dàng.

1.3.1.6. *Mã hoán vị*

a) Sơ đồ khóa

Khác với các mã trước, mã hoán vị không thay đổi các ký tự trong bản rõ mà chỉ thay đổi vị trí các ký tự trong từng bộ m các ký tự của bản rõ. Ta ký hiệu Sm là tập hợp tất cả các phép hoán vị của {1, 2,…, m}.

S= (P, C, K, E, D)

Cho m là số nguyên dương.

$P = C = Z^m_{26}$, K = Sm

với mỗi $k = \pi \in Sm$, ta có

$e_k(x_1, x_2,\ldots, x_m) = (x_{\pi(1)}, x_{\pi(2)},\ldots, x_{\pi(m)})$

$d_k(y_1, y_2,\ldots, y_m) = (y_{\pi^{-1}(1)}, y_{\pi^{-1}(2)},\ldots, y_{\pi^{-1}(m)})$

trong đó π^{-1} là hoán vị nghịch đảo của π

b) Ví dụ

Giả sử m = 6, và khoá k được cho bởi phép hoán vị π

1	2	3	4	5	6
3	5	1	6	4	2

Khi đó phép hoán vị nghịch đảo π^{-1} là:

1	2	3	4	5	6
3	6	1	5	2	4

Với bản rõ: “hentoithubay”

	h	e	n	t	o	i	t	h	u	b	a	y
vt	1	2	3	4	5	6	1	2	3	4	5	6
π	1→3	2→5	3→1	4→6	5→4	6→2	1→3	2→5	3→1	1→6	5→1	6→2
vt	3	5	1	6	4	2	3	5	1	6	1	2
	n	o	h	i	t	e	u	a	t	y	b	h

Bản mã: “nohiteuatybh”

Dùng hoán vị nghịch đảo, từ bản mã ta lại thu được bản rõ.

c) Ưu nhược điểm

Mã hoán vị là một trường hợp riêng của mã Hill. Thực vậy, cho phép hoán vị π của {1, 2,…, m}, ta có thể xác định ma trận $K\pi=(k_{ij})$,

với $k_{ij} = \begin{cases} 1 \text{ nếu } i = \pi(j) \\ 0 \text{ nếu ngược lại} \end{cases}$

thì dễ thấy rằng mã Hill với khoá Kπ trùng với mã hoán vị với khoá π. Với m cho trước, số các khoá có thể có của mã hoán vị là m! Dễ nhận thấy với m = 26 ta có số khóa 26! (mã Thay thế)

1.3.2. Hệ mã hóa khóa công khai

1.3.2.1. *Hệ mật mã RSA*

a) Nguồn gốc

Hệ mật mã khóa công khai RSA được đưa ra năm 1977, là công trình nghiên cứu của ba đồng tác giả Ronald Linn Revest, Adi Shamir, Leonard Aldeman. Hệ mật mã được xây dựng dựa trên tính khó giải của bài toán phân tích một số thành thừa số nguyên tố hay còn gọi là Bài toán RSA (RSAP).

b) Định nghĩa

Bài toán RSA (RSA Problem): Cho một số nguyên dương n là tích của hai thừa số nguyên tố lẻ p và q. Một số nguyên dương b sao cho gcd(b, (p-1)(q-1)) =1 và một số nguyên c. Bài toán đặt ra: tìm số nguyên x sao cho $x^b \equiv c \pmod n$.

c) Thuật toán

- Sinh khóa cho mã khóa công khai RSA

  i. Sinh hai số nguyên tố lớn p và q có giá trị xấp xỉ nhau

  ii. Tính n = p.q, và $\varphi(n) = (p-1).(q-1)$

  iii. Chọn một số ngẫu nhiên b, $1 < b < \varphi(n)$, sao cho $\gcd(b,\varphi(n)) = 1$

  iv. Sử dụng thuật toán Euclide để tính số a, $1 < a < \varphi(n)$, sao cho $a.b \equiv 1 \pmod{\varphi(n)}$

  v. Khóa công khai là (n, b), Khóa bí mật là (a).

- Mã hóa RSA

  i. Lập mã:

  1. Lấy khóa công khai (n, b) theo thuật toán trên
  2. Chọn một bản mã x, trong khoảng [1, n-1]
  3. Tính : $y = x^b \bmod n$
  4. Nhận được bản mã y

  ii. Giải mã:

Sử dụng khóa bí mật a để giải mã : $x = y^a \bmod n$

- Ví dụ

Sinh khóa: Đối tượng A chọn các số nguyên tố: p = 2357, q = 2551, và tính n = p.q = 6012707 và $\varphi(n)= (p-1).(q-1) = 6007800$. A chọn b = 3674911 và, sử dụng thuật toán Euclide mở rộng, tìm a = 422191 sao cho $ab \equiv 1 \pmod{\varphi}$.

Khóa công khai sẽ là (n = 6012707; b = 3674911)

Khóa bí mật là (a = 422191).

Lập mã : Cho bản mã x = 5234673, B sử dụng thuật toán tính số lũy thừa lớn để tính $y = x^b \bmod n = 5234673^{3674911} \bmod 6012707 = 3650502$;

Và gửi cho A.

Giải mã : Từ bản mã y, A tính

$y^a \bmod n = 3650502^{422191} \bmod 6012707 = 5234673$;

1.3.2.2. *Hệ mật mã Elgamal*

a) Nguồn gốc

Hệ mật mã khóa công khai ElGamal được đưa ra năm 1978. Hệ mật mã này được xây dựng dựa trên tính khó giải của Bài toán logarit rời rạc

b) Định nghĩa

Bài toán logarit rời rạc (Discrete logarithm problem): Cho một số nguyên tố p và một phần tử sinh α của tập Z^*_p, một phần tử $\beta \in Z^{*p}$. Bài toán đặt ra: tìm một số nguyên x, $0 \leq x \leq (p-2)$, sao cho $\alpha^x \equiv \beta \pmod p$.

c) Thuật toán

- Sinh khóa cho mã khóa công khai Elgamal

- Sinh ngẫu nhiên một số nguyên tố lớn p và α là phần tử sinh của Z^*_p
- Chọn ngẫu nhiên một số nguyên a, $1 \leq a \leq p-2$, tính $\alpha^a \bmod p$
- Khóa công khai là (p, α, α^a). Khóa bí mật (a)

- Mã hóa RSA

- Lập mã:

a. Lấy khóa công khai (p, α, α^a) theo thuật toán trên

b. Chọn một bản mã x, trong khoảng $[0, p-1]$

c. Chọn ngẫu nhiên một số nguyên k, $1 \leq k \leq p-2$

d. Tính $\gamma = \alpha^k \bmod p$ và $\delta = x.(\alpha^a)^k \bmod p$

e. Nhận được bản mã là (γ, δ)

- Giải mã:

- Sử dụng khóa bí mật (a) và tính γ^{p-1-a} modp
- Lấy bản rõ: x= (γ^{-a}) .δmodp
- Thuật toán ElGamal lấy được bản rõ vì:
- $(\gamma^{-a}).\delta \equiv (\alpha^{-ak}).x.(\alpha^{ak}) \equiv x \pmod p$

- Ví dụ

Sinh khóa: Đối tượng A chọn một số nguyên p = 2357 và một phần tử sinh α = 2 của tập Z^*_{2357}. A chọn một khóa bí mật a = 1751 và tính:

$\alpha^a \bmod p = 2^{1751} \bmod 2357 = 1185.$

Khóa công khai của A (p=2357; α=2; α^a=1185).

Lập mã: Mã hóa bản rõ x = 2035,

B chọn một số nguyên k = 1520 và tính:

$\gamma = 21520 \bmod 2357 = 1430.$

và $\delta = 2035.11851520 \bmod 2357 = 697.$

B gửi γ = 1430 và δ = 697 cho A.

Giải mã: Để giải mã A tính:

$\gamma^{p-1-a} = 1430605 \bmod 2357 = 872.$

và lấy lại được bản rõ khi tính

$x = 872.697 \bmod 2357 = 2035.$

1.3.2.3. *Hệ mật mã Merkle – Hellman (xếp ba lô)*

a) Nguồn gốc

Hệ mật mã khóa công khai Merkle-Hellman được xây dựng trên cơ sở của bài toán tổng tập con.

b) Định nghĩa

Bài toán tổng tập con (Subset sum problem): Cho một tập {a1, a2,…, an}là các số nguyên, được gọi là tập knapsack và một số nguyên dương s. Xác định có hay

không một tập con có tổng a_j bằng s. Tương đương việc xác định có hay không các $x_i \in \{0, 1\}$, $1 \le i \le n$ sao cho $\sum_{i=1}^{n} a_i x_i = s$.

Dãy siêu tăng là một dãy {b1, b2, …, bn} là các số nguyên dương có tính chất: $b_i > \sum_{j-1}^{i-1} b_j$ với mỗi i, $2 \le i \le n$.

c) Thuật toán

➢ Lập mã

- Lấy khóa công khai (a_1, a_2, ..., a_n) theo thuật toán trên.
- Chọn một bản mã x, là một chuỗi bit có độ dài n, $x = x_1x_2...x_n$
- Tính toán $c = x_1a_1 + x_2a_2 + \dots + x_na_n$
- Nhận được bản mã là c

➢ Giải mã

- Tính $d = W^{-1}.c \bmod M$
- Giải quyết bài toán tập con để tìm ra r_1, r_2, …,r_n ,
- $r_i \in \{0, 1\}$, sao cho $d = r_1b_1 + r_2b_2 + \dots + r_nb_n$
- Bản rõ là kết quả $xi = r_{\pi(i)}$, i=1, 2, …, n

➢ Ví dụ

Sinh khóa: Cho n = 6. Đối tượng A chọn một dãy siêu tăng {12, 17, 33, 74, 157, 316}, M = 737, W = 635, và một hoán vị π của tập {1,2, 3, 4, 5, 6} được định nghĩa: π(1) = 3, π(2) = 6, π(3) = 1, π(4) = 2, π(5) = 5, π (6) =4.

Khóa công khai ({319, 196, 250, 477, 200, 559})

Khóa bí mật (π, M, W, {12, 17, 33, 74, 157, 316})

Lập mã: Cho bản mã x = 101101, B sẽ tính:

c = 319 + 250 + 477 + 559 = 1605,

và gửi c cho A.

Giải mã: A tính d = W-1. c mod M= 136, và giải quyết bài toán tổng tập con:

136 = 12r1 + 17r2 + 33r3 + 74r4 + 157r5 + 316r6

ta thấy: 136 = 12 + 17 + 33 + 74.

Vì thế, r1 = 1, r2 = 1, r3 = 1,

r4 = 1, r5 = 0, r6 = 0, áp dụng hoán vị π ta tìm được chuỗi bit gốc, x1 = r3 = 1, x2 = r6 = 0, x3 = r1 = 1, x4 = r2 = 1, x5 = r5 = 0, x6 = r6.

Kết quả x = 101101

1.4. Thám mã và tính an toàn của một hệ mật mã

1.4.1. Thám mã

Mật mã được sử dụng trước hết là để đảm bảo tính bí mật cho các thông tin được trao đổi, và do đó bài toán quan trọng nhất của thám mã cũng là bài toán phá bỏ tính bí mật đó, tức là từ bản mật mã có thể thu được dễ dàng(trên các kênh truyền tin công cộng) người thám mã phải phát hiện được nội dung thông tin bị che giấu trong bản mã bí mật đó, tốt nhất là tìm ra được bản rõ gốc của bản mật mã đó. Tình huống thường gặp là bản thân sơ dồ hệ thống mật mã, kể cả phép lập mã và giải mã không nhất thiết là bí mật, do đó bài toán quy về việc tìm chìa khóa mật mã K, hay chìa khóa giải mã K', nếu hệ mật mã có khóa phi đối xứng. Như vậy ta có thể quy ước xem bài toán thám mã cơ bản là bài toán tìm khóa mật mã K. Để giải bài toán đó, giả thiết người thám mã biết thông tin về sơ đồ hệ mật mã được dùng, kể cả phép lập mã và giải mã.

1.4.2. Tính an toàn của một hệ mật mã

Tính an toàn của hệ thống mật mã phụ thuộc vào độ khó khăn của bài toán thám mã khi sử dụng mật mã đó. Người ta đã đề xuất một số cách hiểu cho khái niệm an toàn của hệ thống mật mã, để trên cớ sở các cách hiểu đó nghiên cứu tính an toàn của nhiều hệ mật mã khác nhau.

CHƯƠNG 2: KÝ ĐIỆN TỬ VÀ VẤN ĐỀ XÁC THỰC

2.1. Khái niệm về ký điện tử

2.1.1. Định nghĩa

Một sơ đồ chữ ký gồm bộ 5 (**P, A, K, S, V**) thoả mãn các điều kiện dưới đây:

P là tập hữu hạn các bức điện (thông điệp) có thể,

A là tập hữu hạn các chữ kí có thể,

K không gian khoá là tập hữu hạn các khoá có thể,

$\mathbf{Sig_k}$ là thuật toán ký $P \rightarrow A$

$x \in P \rightarrow y = Sig_k(x)$

Ver_k là thuật toán kiểm thử: (P, A) $\rightarrow$ (Đúng, sai)

$$Ver_k(x, y) = \begin{cases} \text{Đúng} & \text{Nếu } y = Sig_k(x) \\ \text{Sai} & \text{Nếu } y \neq Sig_k(x) \end{cases}$$

2.1.2. Phân loại sơ đồ chữ ký điện tử

Chữ ký "điện tử" được chia làm 2 lớp, lớp chữ ký kèm thông điệp (message appendix) và lớp chữ ký khôi phục thông điệp (message recovery).

Chữ ký kèm thông điệp: Đòi hỏi thông điệp ban đầu là đầu vào của giải thuật kiểm tra. Ví dụ: chữ ký Elgamal.

Chữ ký khôi phục thông điệp: Thông điệp ban đầu sinh ra từ bản thân chữ ký. Ví dụ: chữ ký RSA.

2.1.3. Một số sơ đồ chữ ký đơn giản

2.1.3.1. Sơ đồ chữ ký Elgamal

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

Chọn g là phần tử sinh $\in Z^*_p$; $a \in Z^*_p$.

Tính $\beta \equiv g^a \bmod p$.

Chọn r ngẫu nhiên $\in Z^*_{p-1}$

Ký trên x: Sig(x) = (γ, δ),

Trong đó $\gamma = g^k \bmod p$, $\delta = (x - a\gamma)\, r^{-1} \bmod (p-1)$.

Kiểm tra chữ ký:

Ver(x, γ, δ)=True $\Leftrightarrow \beta^{\gamma}\, \gamma^{\delta} \equiv g^x \bmod p$

Ví dụ:

Chọn p=463; g=2; a=211;

$\beta \equiv 2^{211} \bmod 463 = 249$;

chọn r =235; $r^{-1}=289$

Ký trên x = 112

Sig(x,r) = Sig (112,235)=(γ,δ)=(16,108)

$\gamma = 2^{235} \bmod 463 = 16$

$\delta = (112-211*16)*289 \bmod (463-1) = 108$

Kiểm tra chữ ký:

Ver(x, γ, δ)=True $\Leftrightarrow \beta^{\gamma}\, \gamma^{\delta} \equiv g^x \bmod p$

$\beta^{\gamma}\, \gamma^{\delta} = 249^{16} * 16^{108} \bmod 463 = 132$

$g^x \bmod p = 2^{112} \bmod 463 = 132$

2.1.3.2. *Sơ đồ chữ ký RSA*

Chọn p, q nguyên tố lớn .

Tính n=p.q; $\phi(n)=(p-1)(q-1)$.

Chọn b nguyên tố cùng $\phi(n)$.

Chọn a nghịch đảo với b; $a=b^{-1} \bmod \phi(n)$.

Ký trên x:

Sig (x) = $x^a \bmod n$

Kiểm tra chữ ký:

Ver (x,y)= True $\Leftrightarrow x \equiv y^b \bmod n$

Ví dụ:

p=3; q=5;

n=15; $\phi(n)= 8$;

chọn b=3; a=3

Ký x =2:

Chữ ký :

$y = x^a \bmod n = 2^3 \bmod 15=8$

Kiểm tra:

$x = y^b \bmod n = 8^3 \bmod 15 =2$ (chữ ký đúng)

2.1.3.3. *Sơ đồ chữ ký Schnorr*

Chuẩn bị:

Lấy *G* là nhóm con cấp *q* của Z_n^*, với *q* là số nguyên tố.

Chọn phần tử sinh $g \in G$ sao cho bài toán logarit trên *G* là khó giải.

Chọn $x \neq 0$ làm khóa bí mật, $x \in Z_q$. Tính $y = g^x$ làm khóa công khai.

Lấy *H* là hàm băm không va chạm.

Ký trên thông điệp m:

Chọn r ngẫu nhiên thuộc Z_q

Tính $c = H(m, g^r)$

Tính $s = (r - c\,x) \bmod q$

Chữ ký Schnorr là cặp (*c*, *s*)

Kiểm tra chữ ký:

Với một văn bản *m* cho trước, một cặp (*c*, *s*) được gọi là một chữ ký Schnorr hợp lệ nếu thỏa mãn phương trình:

$$\mathbf{c = H(m, g^S * y^C)}$$

Để ý rằng ở đây, c xuất hiện ở cả 2 vế của phương trình

2.2. Vấn đề xác thực

2.2.1. Khái niệm xác thực

Xác thực là việc xác minh, kiểm tra một thông tin để công nhận hoặc bác bỏ tính hợp lệ của thông tin đó. Xác thực luôn là yêu cầu quan trọng trong các giao tiếp cần có sự tin cậy. Để đơn giản xét mô hình giao tiếp gồm hai thực thể trao đổi thông tin A và B, họ cùng mục đích trao đổi thông tin M nào đó.

Khi đó việc xác thực bao gồm:

- A cần xác minh B đúng là B và ngược lại.
- Cả A và B cần xác minh tính an toàn của thông tin M mà họ trao đổi.

Như vậy, xác thực bao gồm hai việc chính:

- Xác thực tính hợp lệ của các thực thể tham gia giao tiếp.
- Xác thực tính bảo mật và toàn vẹn của thông tin trao đổi.

Theo phương pháp truyền thống, việc thực hiện xác thực thực thể được thực thi bằng các giấy tờ như: chứng minh thư, giấy phép lái xe, hoặc các giấy tờ cá nhân khác. Việc xác thực tính an toàn của thông tin thường dựa trên chữ ký, con dấu.

2.2.2. Khái niệm xác thực số (điện tử)

Xác thực điện tử là việc chứng minh từ xa bằng phương tiện điện tử, sự tồn tại chính xác và hợp lệ danh tính của một chủ thể khi tham gia trao đổi thông tin điện tử như: các nhân, tổ chức, dịch vụ,... hoặc một lớp thông tin nào đó mà không cần biết các thông tin đó cụ thể như thế nào, thông qua thông tin đặc trưng đại diện cho chủ thể đó mà vẫn đảm bảo được bí mật của chủ thể, hoặc lớp thông tin cần chứng minh.

Xác thực điện tử là việc cần thực hiện trước khi thực sự diễn ra các cuộc trao đổi thông tin điện tử chính thức.

Việc xác thực điện tử trong hệ thống trao đổi thông tin điện tử được uỷ quyền cho một bên thứ ba tin cậy. Bên thứ ba ấy chính là CA (Certification Authority), một cơ quan có tư cách pháp nhân thường xuyên tiếp nhận đăng ký các thông tin đặc trưng đại diện cho chủ thể: khoá công khai và lưu trữ khoá công khai cùng lý lịch của chủ thể trong một cơ sở dữ liệu được bảo vệ chặt chẽ. CA chuyên nghiệp không nhất thiết là cơ

quan nhà nước. Điều quan trọng nhất của một CA là uy tín để khẳng định sự thật, bảo đảm không thể có chuyện "đổi trắng thay đen".

Mục đích của việc xác thực điện tử: chống giả mạo, chống chối bỏ, đảm bảo tính toàn vẹn, tính bí mật, tính xác thực của thông tin và mục đích cuối cùng là hoàn thiện các giải pháp an toàn thông tin.

Cơ sở ứng dụng đề xây dựng các giải pháp an toàn cho xác thực điện tử là các hệ mật mã.

Ứng dụng trong: thương mại điện tử, trong các hệ thống thanh toán trực tuyến, là nền tảng của chính phủ điện tử.

Hiện nay, xác thực điện tử được sử dụng trong khá nhiều ứng dụng, theo số liệu điều tra công bố vào tháng 8/2003 của tổ chức OASIS (Organization for the Advancement of Structured Information Standard):

- 24,1% sử dụng trong việc ký vào các dữ liệu điện tử;
- 16,3% sử dụng để đảm bảo cho e-mail;
- 13,2% dùng trong thương mại điện tử;
- 9,1% sử dụng để bảo vệ WLAN;
- 8% sử dụng đảm bảo an toàn cho các dịch vụ web;
- 6% sử dụng bảo đảm an toàn cho Web Server;
- 6% sử dụng trong các mạng riêng ảo...

Có nhiều phương pháp xác thực điện tử đã được phát triển. Tuy nhiên có 3 phương pháp xác thực chính sau đây:

a. Phương pháp thứ nhất: Xác thực dựa vào những gì mà ta "***biết***"

Phương pháp này thường sử dụng mật khẩu, mã PIN để xác thực chủ thể. Khi cần xác thực, hệ thống yêu cầu chủ thể cung cấp những thông tin mà chủ thể biết (mật khẩu, mã PIN, ...).

b. Phương pháp thứ hai: Xác thực dựa vào những gì mà ta "***có***".

Phương pháp này đòi hỏi người dùng phải sở hữu một thứ gì đó để có thể xác nhận, chẳng hạn như chứng chỉ số, thẻ ATM, thẻ SIM.

c. Phương pháp thứ ba: Xác thực những gì mà ta "***đại diện***".

Phương pháp này thường sử dụng việc nhận dạng sinh học như dấu vân tay, mẫu võng mạc, mẫu giọng nói, ... để xác thực.

Xác thực bằng mật khẩu, mã PIN có ưu điểm là tạo lập và sử dụng đơn giản, nhưng có nhược điểm lớn là người dùng thường chọn mật khẩu dễ nhớ, do vậy dễ đoán nên dễ bị tấn công. Kẻ tấn công cũng có nhiều phương pháp tấn công để đạt được mật khẩu.

2.2.3. Công cụ xác thực (chứng chỉ số)

2.2.3.1. *Khái niệm chứng chỉ số (Digital Certificate)*

Chứng chỉ số là một trong số các công cụ để thực hiện bảo toàn và bảo mật trong hệ thống thông tin.

Như đã trình bày, việc sử dụng hệ mã hoá khoá công khai trong bảo mật thông tin là rất quan trọng. Tuy nhiên, có vấn đề nảy sinh là nếu hai người không biết nhau, nhưng muốn tiến hành giao dịch, thì làm sao họ có thể có khoá công khai của nhau. Giả sử ông A muốn giao tiếp với ông B, ông ta sẽ vào website của ông B để lấy khóa công khai. Ông A gõ địa chỉ URL của ông B trên trình duyệt, tìm DNS của trang Web và gửi yêu cầu của ông A. Nhưng không may, kẻ giả mạo **B'** lại nhận yêu cầu của A và trả về trang Web của **B'** là bản sao của B, hoàn toàn giống trang web của B, khiến cho A không thể phát hiện được. Lúc này A có khoá công khai của **B'**, chứ không phải là của B. Ông A mã hoá thông điệp bằng khoá công khai của **B'**. Kẻ gian **B'** giải mã thông điệp, đọc thông tin, mã hóa lại bằng khoá công khai của B, và gửi thông điệp cho B. Như vậy cả A và B hoàn toàn không biết có kẻ thứ 3 là **B'** đã đọc được nội dung của thông điệp. Trường hợp xấu hơn, **B'** sẽ thay đổi nội dung thông điệp của A trước khi gửi cho B.

Bài toán đặt ra là phải có một giải pháp để đảm bảo rằng khoá công khai được trao đổi an toàn, không có giả mạo.

Để giải quyết vấn đề này cần có một tổ chức cung cấp chứng nhận, nó xác nhận: khoá công khai này thuộc về một người, công ty hay tổ chức nào đó. Tổ chức cung cấp các chứng nhận khoá công khai được gọi là **CA** (Certification Authority), và chứng nhận này gọi là chứng chỉ số.

Với bài toán trên, ông B muốn cho phép A và những người khác giao tiếp với mình, ông ta phải đến một tổ chức **CA** để xin giấy chứng nhận khoá công khai của ông ta. Nhà cung cấp sẽ phát hành chứng nhận và chữ ký số của nhà cung cấp. Nhiệm vụ chính của nhà cung cấp CA là gắn kết khoá công khai với tên của người đăng ký (cá nhân, công ty hay tổ chức) sở hữu khoá đó.

Chứng chỉ số là một văn bản điện tử theo định dạng chuẩn nhất định, dùng để xác minh danh tính một cá nhân, một công ty, ... hay thực thể nào đó trên mạng truyền thông công cộng, cùng với khoá công khai của họ trên Internet. Nó giống như bằng lái xe, hộ chiếu, chứng minh thư hay những giấy tờ xác minh cá nhân. Để có chứng minh thư, ta phải được cơ quan Công An sở tại cấp. Chứng chỉ số cũng vậy, phải do một tổ chức đứng ra chứng nhận những thông tin của ta là chính xác, được gọi là Nhà cung cấp chứng chỉ số (Certification Authority, viết tắt là CA). CA phải đảm bảo về độ tin cậy, chịu trách nhiệm về độ chính xác của chứng chỉ số mà họ cấp.

Trong chứng chỉ số có ba thành phần chính:

a. Thông tin cá nhân:

Đây là các thông tin của đối tượng được cấp chứng chỉ số, gồm tên, quốc tịch, địa chỉ, điện thoại, email, tên tổ chức .v.v. Phần này giống như các thông tin trên chứng minh thư của mỗi người.

b. Khoá công khai:

Trong mật mã, khoá công khai là một giá trị được CA chứng thực, đó là khoá mã hoá, kết hợp với khoá bí mật duy nhất được tạo ra từ khoá công khai, để tạo thành cặp khoá mật mã bất đối xứng.

c. Chữ ký số của CA cấp chứng chỉ:

Đây chính là sự xác nhận của CA, bảo đảm tính chính xác và hợp lệ của chứng chỉ. Muốn kiểm tra một chứng chỉ số, trước tiên phải kiểm tra chữ ký số của CA có hợp lệ hay không.

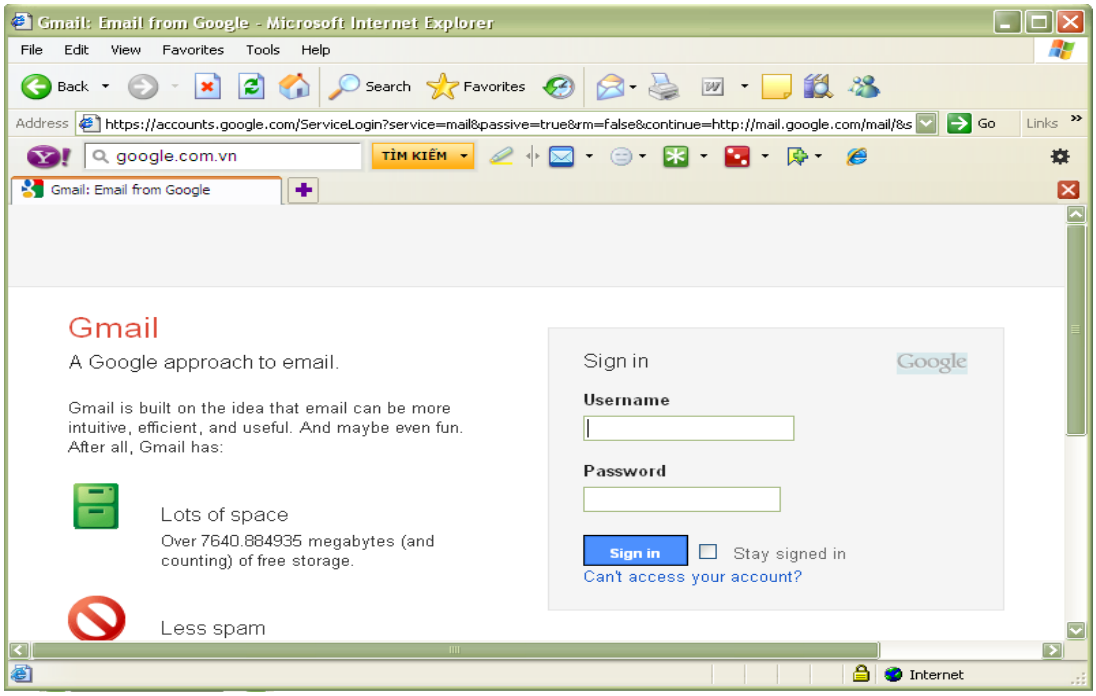
Trong cơ sở hạ tầng mật mã khoá công khai (Public Key Infrastructure - PKI), CA sẽ kiểm soát cùng với nhà quản lý đăng ký (Registration Authority - RA), để xác

minh thông tin về chứng chỉ số mà người ta yêu cầu xác thực. RA xác nhận thông tin của người cần xác thực, CA sau đó sẽ cấp chứng chỉ.

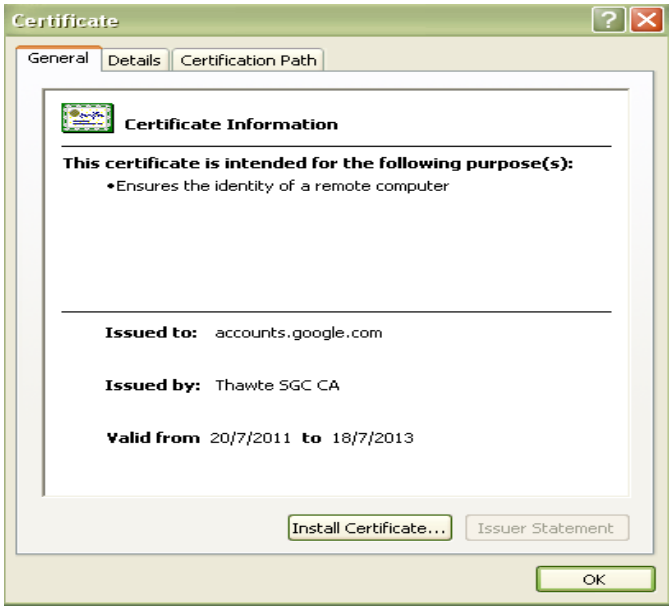
Một ví dụ thực tê trong việc sử dụng chứng chỉ số là khi ta truy cập vào một trang web : http://vnexpess.net. ….Việc truy cập vào trang web không có cơ chế mã hóa dữ liệu truyền đi giữa người dùng và trang web đó, do vậy có thể bị nghe lén → không an toàn.

Vậy, một trang web bảo mật khác ở chỗ là sử dụng chứng chỉ số, khi truy cập vào trang web đó ta không dùng địa chỉ thông thường như trên mà sử dụng : https://vnexpress.net (Hình 2.1).

Ví dụ như gmail.com, bằng trình duyệt IE truy cập vào trang web sử dụng chứng chỉ số để bảo mật t thấy dấu hiệu bảo mật là hình chiếc khóa vàng góc dưới phải màn hình (Hình 2.1). Nếu click chuột vào nó, IE sẽ hiện thị chứng chỉ số được cung cấp cho trang web này (Hình 2.2).



Hình 2.1: https://accounts.google.com



Hình 2.2: Chứng chỉ số

2.2.3.2. Định dạng X.509 của chứng chỉ số

Cơ sở hạ tầng của mật mã khóa công khai (PKI) được xây dựng để bảo đảm an toàn thông tin. Trong hệ thống này, người ta sử dụng một thành phần dữ liệu được gọi là chứng chỉ số, nó gắn thông tin về người sở hữu khóa riêng với khóa công khai tương ứng.

Hình 2.3 mô tả chứng chỉ số phiên bản 3, được định nghĩa theo chuẩn X.509, chuẩn được sử dụng phổ biến trên thế giới hiện nay.

Các thành viên tham gia hệ thống, sử dụng hệ mật mã khóa công khai hoàn toàn có thể tin rằng: Khóa công khai chứa trong chứng chỉ số là thuộc về đối tượng có thông tin trong trường đối tượng được cấp. CA sử dụng chữ ký điện tử để đảm bảo tính toàn vẹn và xác thực các thông tin có trong chứng chỉ số.

Chữ ký được tạo ra như sau:

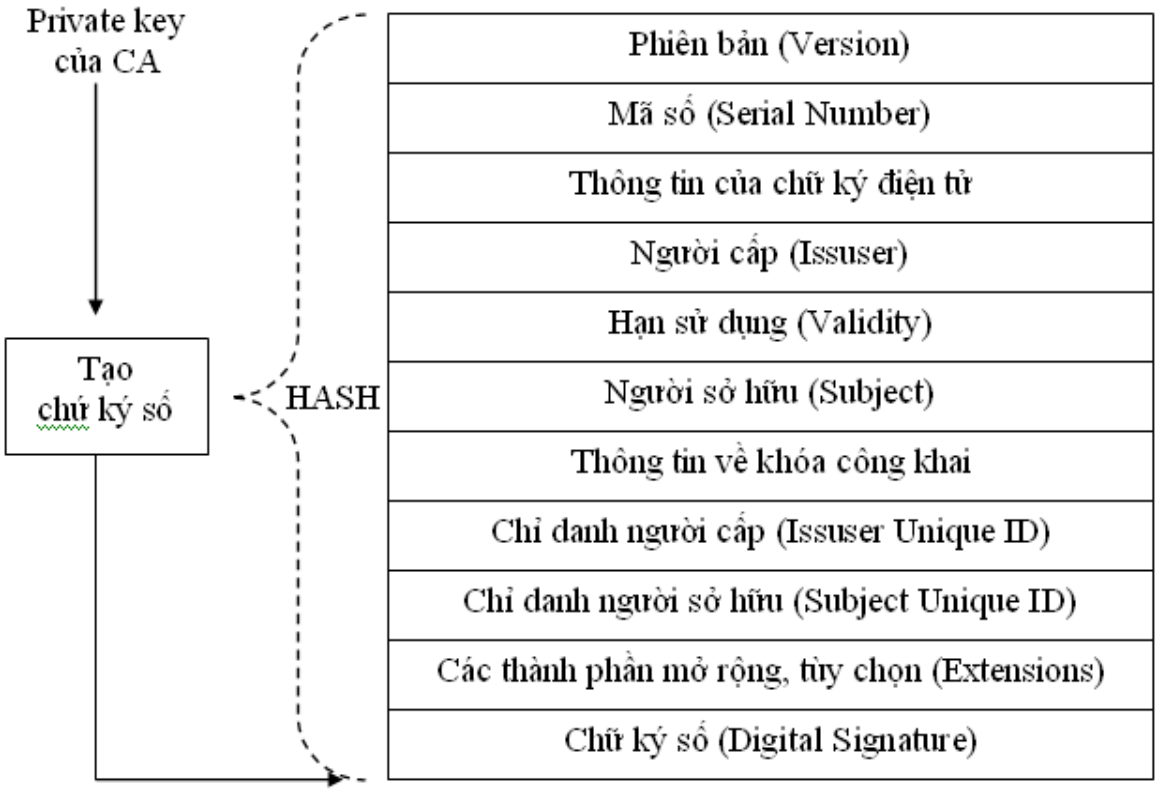
Thiết lập đại diện của toàn bộ thông tin trong chứng chỉ số (gồm các thông tin cơ bản và phần mở rộng).

CA sử dụng khóa riêng (private key) của mình ký trên đại diện vừa có được, để tạo ra chữ ký số.

Đóng gói các thông tin cùng với chữ ký trên, đó là chứng chỉ.

Sự tin tưởng của các thành viên chỉ có thể được đảm bảo khi họ tin tưởng vào CA đã tạo ra chứng chỉ đó. Mỗi chứng chỉ số đều có hạn sử dụng. Việc kiểm tra chứng chỉ số được thực hiện độc lập với hệ thống cấp chứng chỉ, nó được thực hiện tại đầu cuối, hoặc thông qua các dịch vụ kiểm tra trạng thái của chứng chỉ số. Chứng chỉ số có thể công khai.

Các trường cơ bản của một chứng chỉ số



Hình 2.3: Chứng chỉ số theo chuẩn X 509

CHƯƠNG 3: ĐẤU GIÁ ĐIỆN TỬ

3.1. Mô hình đấu giá truyền thống

3.1.1. Giới thiệu

Đấu giá là một quá trình mua và bán bằng cách đưa ra món hàng cần đấu giá, sau đó ra giá. Kết quả thu được là bán được món hàng theo giá yêu cầu của phiên đấu giá.

Có đa dạng các mặt hàng có thể được đem ra đấu giá như đồ cổ, bộ sưu tập, bất động sản, sản phẩm thương mại, thanh lý, nhượng mại….

Với lịch sử lâu đời thì đấu giá là hoạt động thương mại mang tính truyền thống. Trong thực tế ta thấy có rất nhiều kiểu đấu giá khác nhau như đấu giá tăng (đấu giá kiểu Anh), đấu giá giảm (đấu giá kiểu Hà Lan), đấu giá kín, đấu giá kép v.v. Ngoài ra còn một số đấu giá khác ngày nay rất hiếm gặp nhưng góp một phần không nhỏ vào việc tiêu thụ một số lượng sản phẩm không nhỏ trong thương mại.

3.1.2. Đấu giá kiểu Hà Lan (Dutch Auction)

Đấu giá kiểu Hà Lan hay còn gọi là đấu giá với giá giảm (Descending -Price Auction) là mô hình đấu giá áp dụng cho các mặt hàng mà số lượng được đem ra đấu là số lượng nhiều. Trong kiểu đấu giá Hà Lan, giá khởi điểm ban đầu là rất cao sau đó giá sẽ được giảm từ từ và người tham chỉ đưa ra số lượng mà mình muốn mua vào lúc giá thích hợp nhất (giá mà họ cảm thấy có khả năng mua được). Quá trình này sẽ diễn ra liên tục cho đến khi tất cả số lượng hàng đã được bán. Và kết quả thu được là có các mức giá khác nhau giành cho những người mua khác nhau và dĩ nhiên người mua đầu tiên sẽ phải trả với mức giá cao nhất .

Đấu giá theo kiểu Hà Lan chỉ áp dụng đối với những mặt hàng có thời gian tồn tại ngắn như hoa, rau… Đấu giá kiểu này thường diễn ra rất nhanh do đó những người tham gia phải nhanh chóng có quyết định nếu họ thực sự muốn mua món hàng.

3.1.3. Đấu giá kiểu Anh (English Auction)

Đấu giá kiểu Anh cũng được biết đến như là đấu giá với giá tăng (Ascending - Price auction). Giá khởi điểm của mô hình này là một giá rất thấp sau đó người mua sẽ ra giá tăng dần một cách lần lượt cho món hàng. Cuộc đấu giá vẫn tiếp tục cho đến khi

không còn ai đưa ra giá cao hơn một mức giá nào đó hoặc thời gian đã kết thúc. Vào thời điểm đó người chủ trì sẽ gõ một cái búa xuống bàn và chỉ định người ra giá cao nhất là người thắng cuộc.

Đấu giá kiểu Anh thường được áp dụng đối với các mặt hàng có giá trị lớn như các tác phẩm nghệ thuật, rượu vang, hợp đồng và các mặt hàng khác có thời gian tồn tại không giới hạn. Trong hình thức này người thắng cuộc luôn luôn phải trả giá cao nhất để có thể sở hữu món hàng.

3.1.4. Đấu giá kín và chọn giá cao nhất (Sealed bid first price auction)

Đặc điểm chính của hình thức đấu giá này là nó không phải là một hình thức đấu giá mở (open bid auction), nghĩa là giá đưa ra đấu được giấu không cho những người khác tham gia đấu giá biết. Quá trình tiến hành đấu giá trải qua hai giai đoạn: giai đoạn đặt giá trong đó tất cả giá đưa ra được tập hợp lại, và giai đoạn quyết định kết quả trong đó danh sách giá đưa ra sẽ được tiến hành kiểm tra và quyết định người chiến thắng. Suốt giai đoạn đặt giá, mỗi người tham gia đấu giá chỉ ra giá một lần dựa vào kinh nghiệm hay số tiền mà họ có, họ không biết ai là những người đặt giá và giá những người khác đưa ra là bao nhiêu. Trong giai đoạn quyết định kết quả, tất cả các giá được mở và sắp xếp từ cao nhất tới thấp nhất. Nếu món hàng được đem bán chỉ có một thì người đặt giá cao nhất sẽ được mua, còn nếu món hàng đem bán có số lượng nhiều thì nó sẽ được bán theo thứ tự giá từ cao xuống cho tới khi hết hàng. Hình thức này thường được sử dụng cho tín dụng tái huy động vốn và thị trường ngoại hối.

3.1.5. Đấu giá kín và chọn giá cao thứ 2 (Second bid first price auction)

Loại hình đấu giá này được phát triển bởi William Vickrey, người đã đạt giải Nobel kinh tế năm 1996, hình thức tham gia đấu giá chỉ dựa vào sự phán đoán, họ không biết gì về giá những người khác đưa ra này còn được gọi là đấu giá Vickrey (Vickrey auction).

Trong Vickrey auction, các mức giá tham gia cũng được giấu kín và việc ra giá của những người tham gia đấu giá. Điểm khác nhau giữa hình thức này với đấu giá kín và chọn giá cao nhất (Sealed bid first price auction) nằm ở chỗ người chiến thắng trong cuộc đấu giá sẽ trả mức giá cao nhất thứ hai tức là mức giá cao nhất trong số các mức giá của những người không chiến thắng. Vì lí do đó mà người chiến thắng sẽ phải trả

thấp hơn so với giá mà anh ta đưa ra. Vickrey Auction cũng được sử dụng tái huy động vốn và trao đổi ngoại hối.

- Tóm lại

Mô hình đấu giá	**Đặc điểm**	**Đối tượng tham gia**	**Quy trình đấu giá**	**Bảo mật**	**Xác thực**
Đấu giá Anh	Người tham gia trả giá công khai, giá đưa ra sau phải lớn hơn giá đưa ra trước đó. Phiên đấu giá sẽ kết thúc khi không còn ai đưa ra giá cao hơn mức giá trước, khi đó ng ra mức giá cao nhất sẽ mua được món hàng.	Các thương nhân, nhà doanh nghiệp lớn, nhỏ. Người mua hàng…	B1: Chuẩn bị đấu giá. B2: Tổ chức cho xem hàng. B3: Tiến hàng đấu giá. B4: Ký kết hợp đồng, giao hàng.	Thông tin người tham gia.	B4
Đấu giá Hà Lan	Người điều khiển cuộc đấu giá sẽ đưa ra giá	Các thương nhân, nhà doanh nghiệp lớn, nhỏ.			

	khởi điểm rất cao, sau đó sẽ hạ thấp dần cho đến khi người tham dự chấp nhận ma với giá đó. Được đặt tên sau những vụ đấu giá củ hoa tulip vào TK 17. Dựa trên hệ thống định giá đưa ra bởi nhà kinh tế học đoạt giải Nobel William Vickrey.	Người mua hàng…			
Đấu giá kín theo giá thứ nhất	Người tham gia đấu giá sẽ đặt giá đồng thời và được giữ kín. Người ra giá cao nhất sẽ là người thắng cuộc.				
Đấu giá kín theo giá thứ 2	Tương tự như giá thứ nhất nhưng người thắng cuộc sẽ mu được hàng hóa với mức giá cao thứ 2 chứ ko pải mức giá cao nhất do mình đặt ra.				
Đấu giá với giá duy nhất	Một mức giá duy nhất cao				

	nhất hay thấp nhất từ các mức giá được ra giá sẽ là người thắng cuộc.				

3.2. Mô hình đấu giá điện tử

3.2.1. Giới thiệu về đấu giá điện tử

Ngày nay khoa học kỹ thuật phát triển mạnh mẽ trên nhiều phương diện trong đó có công nghệ thông tin và viễn thông. Sự ra đời của internet đã làm cho thương mại điện tử phát triển nhanh chóng và chi phối sâu sắc đến đời sống con người trên nhiều lĩnh vực khác nhau. Một trong những lĩnh vực đạt thành công rực rỡ nhất đó là đấu giá (auction). Điển hình cho những thành công đó không thể không kể đến những sàn đấu giá nổi tiếng như ebay, ubid v.v. Còn ở Việt Nam tuy thương mại điện tử còn mang tính trải nghiệm nhưng đã xuất hiện các sàn đấu giá như chodientu.com, chodaugia.com, heya.com...

Không phải ngẫu nhiên mà thương mại điện tử lại thành công đến vậy, điều này có thể giải thích bằng những lợi ích mà thương mại điện tử mang lại nhờ sự kết hợp giữa đấu giá truyền thống và sức mạnh thương mại điện tử. Đó là khả năng tạo ra môi trường cạnh tranh công bằng, người mua và người bán có quyền bình đẳng như nhau. Người mua có thể tìm kiếm, tiếp cận với nhiều mặt hàng và có cơ hội được ra giá. Còn người bán có cơ hội giới thiệu, quảng cáo các mặt hàng của mình và bán được chúng với giá mong muốn. Như vậy một lần nữa ta có thể khẳng định rằng sự kết hợp gữa đấu giá truyền thống và thương mại điện tử là sự kết hợp đúng đắn nó đáp được nhu cầu của cả 2 bên mua và bán đồng thời nó cũng phản ánh đúng quy luật cung cầu trên thị trường một yếu tố cơ bản để tạo nên sự thành công rực rỡ. Do vậy nên việc phổ biến

hình thức đấu giá trên mạng hay còn gọi là đấu giá điện tử thực sự được coi là cần thiết.

Đấu giá điện tử là hình thức đấu giá được tiến hành trực tuyến, giống như đấu giá thông thường ngoại trừ nó được tiến hành trên máy tính. Chính vì sự khác nhau này làm cho đấu giá điện tử phải tuân theo những quy tắc cũng như những đặc tính của thương mại điện tử và có những đặc thù riêng.

Cũng giống như các cuộc đấu giá truyền thống đấu giá điện tử cũng cần phải có người bán và người mua. Thông thường người bán có hai hình thức tham gia vào website đấu giá. Thứ nhất họ là chủ của những mặt hàng được đem đấu giá cũng chính là chủ website. Thứ hai chủ website và chủ của những mặt hàng đem ra đấu giá là hai người riêng biệt điều đó có nghĩa là chủ của các mặt hàng đem đấu giá phải thuê mặt bằng trên website để phục vụ nhu cầu kinh doanh của riêng mình. Để đỡ tốn kém cho việc thuê mặt bằng trên website thì người chủ các mặt hàng có thể tự xây dựng cho mình một website riêng như thế có thể chủ động trong việc kinh doanh. Tuy nhiên trong lĩnh vực đấu giá cũng giống như trong lĩnh vực kinh doanh thì càng nhiều người tới thăm website của mình thì sự thành công càng tăng và cơ hội bán hàng sẽ càng nhiều. Trong khi đó không phải là bất kỳ trang web nào xây dựng cũng thu hút được sự quan tâm của khách hàng do đó chấp nhận trả chi phí để có mặt trong một website nổi tiếng vẫn là một chiến lược của các các chủ hàng.

3.2.2. Các thành phần tham gia vào đấu giá điện tử

Gồm các nhân tố: Người chủ trì cuộc đấu giá (auctioneer) có chức năng tạo điều kiện cho nhà cung cấp hàng (supplier hay seller) gặp gỡ với khách hàng (buyer hay bidder) bên trong một quy trình tổng thể và hơn thế nữa là các mặt hàng đem ra đấu giá (trade objects) hay các luật (rule base) cần thiết áp dụng trong suốt quá trình giao dịch điều này thì tương tự như mô hình chung của đấu giá truyền thống. Tuy nhiên điểm khác là toàn bộ quy trình đấu giá được thực hiện với công nghệ thông tin trên môi trường web.

3.2.3. Quy trình hoạt động chung

Để đưa hàng lên bán tại một trang web đấu giá, người chủ hàng hóa phải là chủ của trang web hoặc phải trả một khoản phí nhất định cho một đối tác thứ ba cung cấp dịch vụ này. Những mặt hàng được lựa chọn đem đấu giá thường được đi kèm với các

thông tin liên quan và tuân thủ những quy tắc nhất định để có thể bán đấu giá được như số lượng, tính độc đáo, tính lịch sử, văn hóa hay tính cá nhân của sản phẩm. Để mua hàng tại các trang web đấu giá trước hết người mua sẽ chọn các mặt hàng mình muốn theo danh mục các mặt hàng được trình bày rõ tại các trang web. Sau khi lựa chọn mặt hàng muốn mua, người mua sẽ phải tham gia đấu giá với những người mua khác bằng cách cung cấp một số thông tin như là đặt giá cho mặt hàng muốn mua và số lượng muốn mua mặt hàng đó. Trang web sẽ tự động làm việc, và khi thời hạn kết thúc, hệ thống sẽ thông báo kết quả đấu giá đến cho những người liên quan.

3.2.4. Các luật trong đấu giá điện tử

Trong thương mại điện tử, cũng tùy vào từng sàn giao dịch mà có các ràng buộc khác nhau, các nguyên tắc phải tuân thủ khác nhau, và mọi hoạt động trong lĩnh vực này đều phải tuân theo pháp luật về thương mại điện tử. Tuy nhiên có một số quy định mà hầu như các sàn giao dịch đấu giá điện tử đều tuân thủ như sau:

Thời hạn kết thúc đấu giá với một mặt hàng: Để tránh tình trạng có quá nhiều mặt hàng tồn đọng trên trang web, khi một mặt hàng được đưa lên bán đấu giá, chủ hàng phải xác định thời hạn chấm dứt đấu giá. Thời hạn càng lưu lên trang web lâu, mức phí chủ hàng phải trả cho chủ trang web càng lớn.

Ví dụ mặt hàng được đưa lên vào đầu tháng 04/2006 thì chủ hàng sẽ có thông báo rằng mặt hàng đó chỉ được đấu giá đến ngày 01/05/2006 muốn để mặt hàng đấu giá đến hết tháng 01/2006 chủ hàng phải trả thêm một chi phí nữa cho website

Thắng lợi trong đấu giá điện tử: Không phải khi nào việc đấu giá cũng cho ra kết quả rõ ràng người thắng người thua. Vì thế việc xác định người nào thắng trong đấu giá cũng được các sàn đấu giá xây dựng thành luật một cách kỹ lưỡng. Nói vắn tắt, quy định về người thắng trong đấu giá là "giá cả trước, số lượng sau và thời gian sau cùng".

Cũng giống như trong đấu giá truyền thống, môt mặt hàng khi được đấu giá trên mạng sẽ được đặt mức giá tối thiểu (reserve price). Đơn đấu giá nào có mức giá cao nhất và vượt mức tối thiểu sẽ là đơn chiến thắng .Trong trường hợp hai hay nhiều đơn đấu giá có cùng mức giá, đơn nào mua số lượng hàng lớn hơn sẽ là đơn chiến thắng. Nếu các đơn cùng đặt mức giá và số lượng như nhau, đơn nào đặt sớm hơn sẽ là đơn chiến thắng. Sau quá trình đấu giá kết thúc, hàng sẽ được bán cho người thắng lợi trong đấu giá. Với khả năng sau đơn mua của người thắng đầu tiên, chủ hàng vẫn còn hàng,

hàng sẽ được bán cho người chiến thắng trong số những người còn lại và tiếp tục như vậy, hàng sẽ được bán cho đến hết hoặc đến đơn đấu giá cuối cùng vượt mức giá tối thiểu. Như vậy người chiến thắng cuối cùng có thể không mua được số lượng hàng như mong muốn. Trong trường hợp không có đơn đấu giá nào vượt mức giá tối thiểu, cuộc đấu giá vẫn được coi là thành công mà không có người mua hàng.

3.2.5. Các giai đoạn đấu giá điện tử

Để tiến hành phiên đấu giá điện tử, phải thực hiện các giai đoạn sau:

- **Giai đoạn 1: Đăng ký**

Khi người mua và người bán muốn tham gia đấu giá, họ phải đăng ký với hệ thống tùy theo mục đích của từng người. Người mua muốn đăng ký tham gia vào phiên đấu giá và mua được món hàng ưng ý với giá rẻ nhất, người bán đăng ký sản phẩm của mình, để có thể bán được hàng với số lượng lớn, đồng thời đảm bảo lợi nhuận cao.

Đối với giai đoạn đăng ký: cần *xác thực những thông tin* của hai bên tham gia.

Đối với người mua, hệ thống phải xác thực những thông tin như: họ tên, ngày tháng năm sinh, số CMT, email …đặc biệt là phải xác thực về tài khoản của người mua, xem tài khoản đó có thực hay không? Nếu có thì tài khoản đó có đủ để tham gia vào phiên đấu giá đó không?

Đối với người bán, hệ thống tập trung xác thực vào các sản phẩm người chủ hàng cần đấu giá. Khi người bán đăng ký sản phẩm, sẽ có bộ phận xác định xem sản phẩm đó có hay không, là hàng thật hay hàng giả, giá trị thực tế là bao nhiêu.

Thông tin của người đấu giá sau khi đăng ký hoàn toàn được giữ kín cho đến khi kết thúc phiên đấu giá. Nếu anh ta là người thắng cuộc thì danh tính của anh ta mới được tiết lộ để mọi người có thể kiểm tra. Nếu không phải là người thắng cuộc thì danh tính của anh ta sẽ khôgn bị lộ diện. Như vậy, phiên đấu giá đảm bảo được tính ẩn danh người đấu giá.

- **Giai đoạn 2: Giới thiệu sản phẩm và thiết lập phiên đấu giá.**

Ở giai đoạn này, hệ thống và người bán một lần nữa thẩm định lại giá trị của sản phẩm. Sau đó mô tả sản phẩm đấu giá một cách chi tiết nhất để làm nổi bật giá trị của sản phẩm, nhằm thu hút những khách hàng tiềm năng. Đồng thời đưa ra các quy tắc đấu giá đối với người tham gia như là giải thích các quy luật đấu giá được sử dụng (đấu

giá mở, đấu giá kín, đấu giá kiểu Hà Lan, đấu giá kiểu Anh…), những con số được đưa ra đàm phán (giá khởi điểm, ngày giao hàng, cách thanh toán…), thời gian bắt đầu cuộc đấu giá, điều kiện để cuộc đấu giá kết thúc. Dựa vào quảng cáo và các quy tắc của cuộc đấu giá, người mua có thể tìm kiếm để lựa chọn sản phẩm đấu giá và các kiểu đấu giá phù hợp.

- **Giai đoạn 3: Đấu giá.**

Ở giai đoạn này cuộc đấu giá mới thực sự bắt đầu. Đầu tiên người tham gia tìm kiếm sản phẩm đấu giá, khi chọn được sản phẩm ưng ý thì họ đăng nhập những thông tin cần thiết. Hệ thống phải *xác thực thông tin* đó, dựa trên việc xác thực khi người mua đăng ký. Xác thực thành công, thì giá của người mua đối với sản phẩm mới có hiệu lực.

Trong giai đoạn trả giá, hệ thống phải làm hai nhiệm vụ chính: thứ nhất là làm thế nào để biết giá đó là của người nào, thứ hai là làm thế nào để những thông tin về giá cả được đảm bảo an toàn và bí mật trong suốt quá trình đấu giá (không biết chính xác giá là bao nhiêu).

Cũng trong giai đoạn này, hệ thống phải phát hiện được những người đấu giá nhiều lần.

- **Giai đoạn 4: Kết thúc cuộc đấu giá và công bố người thắng cuộc**

Có một khoảng thời gian nhất định đối với mỗi vòng đấu giá. Khi thời gian của mỗi vòng đã hết, thì hệ thống chỉ công bố giá cao nhất cho những người tham gia đấu giá. Hệ thống kiểm tra tất cả các giá cao nhất tại vòng cuối cùng, giá nào cao nhất sẽ là giá bán sản phẩm. Trường hợp hai hay nhiều đơn đấu giá có cùng mức giá, thì đơn nào mua với số lượng lớn hơn, sẽ là đơn chiến thắng. Nếu các đơn cùng đặt mức giá và số lượng lớn như nhau, thì đơn nào đặt sớm hơn sẽ là đơn chiến thắng.

CHƯƠNG 4: ỨNG DỤNG ĐẤU GIÁ ĐIỆN TỬ

4.1. Giới thiệu về mã nguồn mở WeBid

WeBid là một gói đấu giá kịch bản là mã nguồn mở. Mặc dù vẫn còn trong giai đoạn thử nghiệm nhưng WeBid là một trong các giải pháp mã nguồn mở tốt nhất cho một trang web đấu giá, chạy một cách nhanh chóng và rẻ.

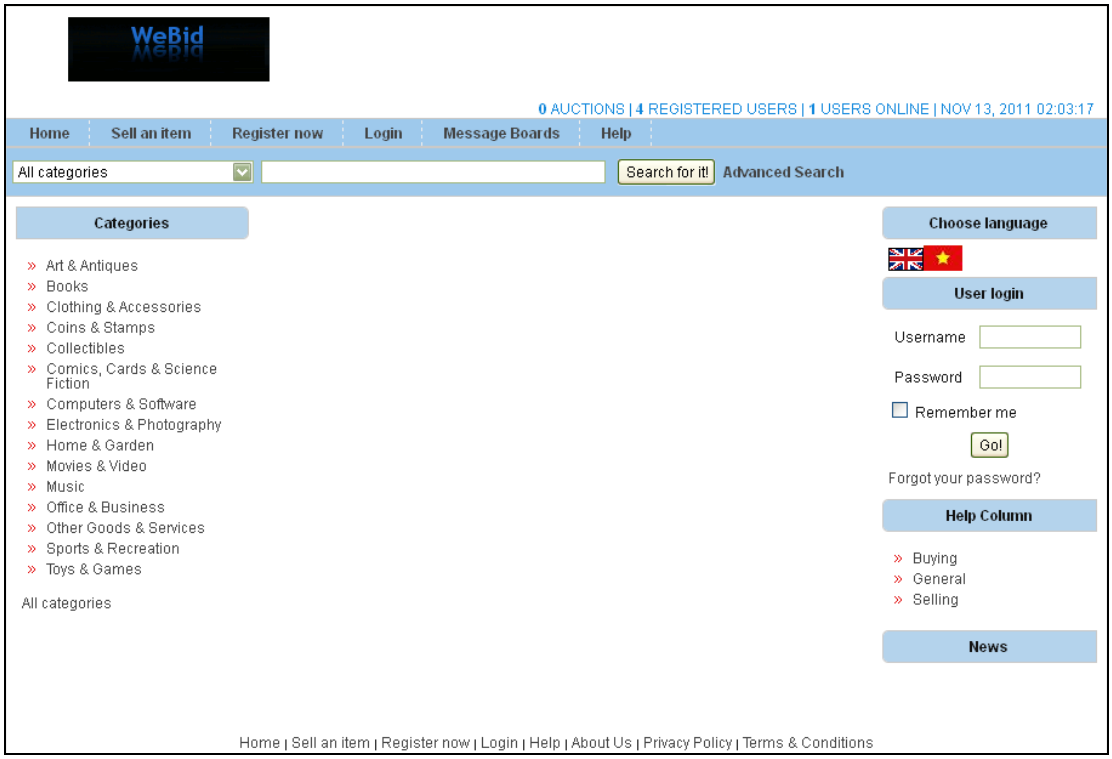
WeBid được viết bằng một ngôn ngữ kịch bản phổ biến php và với một bộ sưu tập lớn các tính năng tùy biến cao. WeBid là một lựa chọn để thiết lập bất kỳ trang web đấu giá nào.

Một trong số những tính năng quan trọng mà làm cho WeBid là một sự lựa chọn tuyệt vời là nó dễ dàng sử dụng bảng điều hành chính, quá trình cài đặt thân thiện cho phép bạn có trang web bán đấu giá của riêng bạn được hình thành trong vài phút. Một hệ thống thanh toán sẵn có cho phép người dùng của bạn dễ dàng thanh toán các mặt hàng được mua với các cổng thanh toán ưa thích của họ (như PayPal, Authorize.net). Và một điều nữa là vô cùng dễ dàng chỉnh sửa WeBid theo ý thích của bạn.

4.2. Việt hóa giao diện

4.2.1. Thư mục language

Ngôn ngữ mặc định của WeBid là tiếng Anh (Hình 4.1)



Hình 4.1: Home

Tạo một thư mục giống thư mục "language\EN" với tên thích hợp là "VI"

Ngôn ngữ tiếng Việt cần có một lá cờ đại diện cho nó, đặt tên cờ là VI.gif và đưa vào trong thư mục "include\flags". Kết quả thu được xem hình 4.2

Hình 4.2: Trang chủ

4.2.2. File từ điển

Tiến hành chỉnh sửa file *messages.inc.php*.

Đổi ***$CHARSET = UTF-8*** (chính là đổi font chữ). UTF-8 thích hợp với hầu như tất cả các ngôn ngữ.

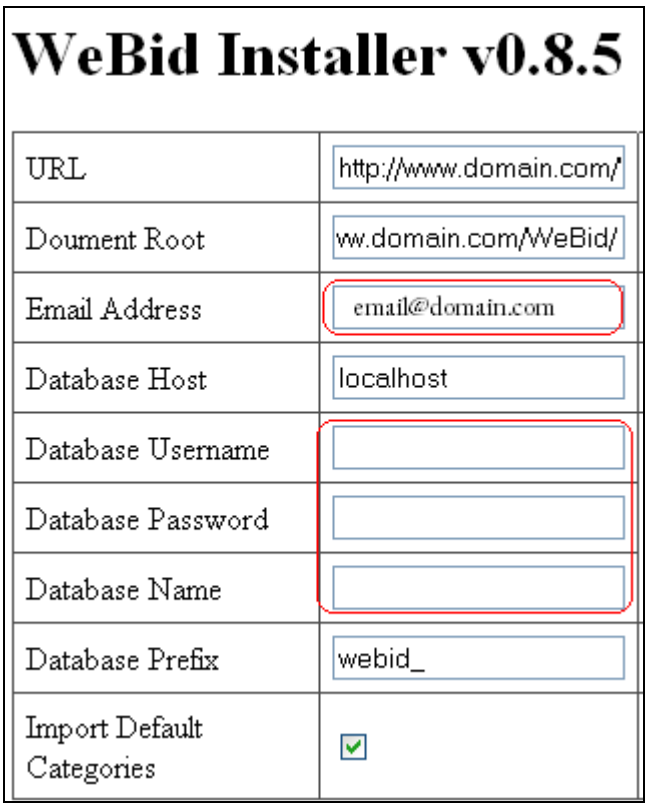
Chỉnh ***$DOCDIR*** chính là xác định hướng đọc tài liệu (từ trái qua phải hay ngược lại).

Sau khi thay đổi 2 biến trên, dịch tất cả các thông báo lỗi và giao diện người dùng trong *messages.inc.php*.

4.3. Qúa trình cài đặt

Đầu tiên, bạn cần tạo ra một CSDL MySQL và chỉ định một tên người dùng mà mật khẩu cho nó.

Tiếp theo, bạn phải tải các tập tin kịch bản của bạn đến máy chủ web bằng các sử dụng bất kỳ phần mềm FTP (ví dụ FileZilla). Bây giờ trên trình duyệt nơi mà bạn đã tải lên các tập tin của Webid có trang như hình 4.3:



Dbhost: "localhost"
Dbusername: "root"
Dbpassword: ""
Dbname:"auction"

Hình 4.3 Cài đặt bước 1

Tiếp theo bạn phải kiểm traxem các tệp tin và thư mục của bạn có thể ghi. Một báo động đỏ có nghĩa là bạn nên xem xét lại lỗi của nó và sửa lại (chủ yếu ở tên file). Nếu chính xác thì sẽ có ảnh dưới đây (Hình 4.4):

File Checks:	
cache/:	Found, Writable
uploaded/:	Found, Writable
uploaded/banners/:	Found, Writable
uploaded/cache/:	Found, Writable
includes/config.inc.php:	Found, Writable
includes/countries.inc.php:	Found, Writable
includes/currencies.php:	Found, Writable
includes/membertypes.inc.php:	Found, Writable
language/EN/categories.inc.php:	Found, Writable
language/EN/categories_select_box.inc.php:	Found, Writable
GD Support:	Found

install

Hình 4.4: Cài đặt bước 1 (tiếp)

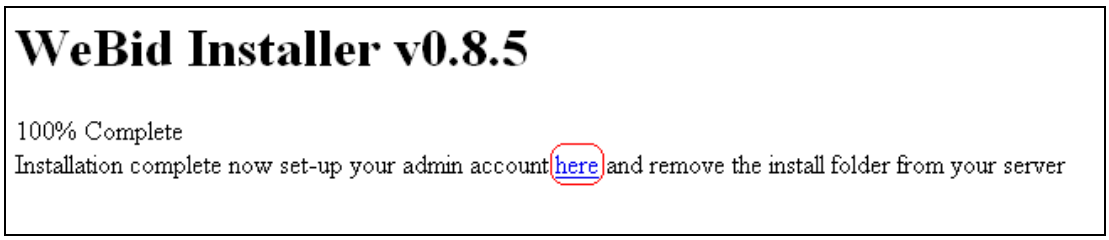
Bây giờ. nhấn nút "INSTALL". Tiếp theo bấm vào liên kết "step 2" (Hình 4.5)

WeBid Installer v0.8.5

Step 1: Writing config file...
Complete, now to step 2

Hình 4.5: Cài đặt bước 2

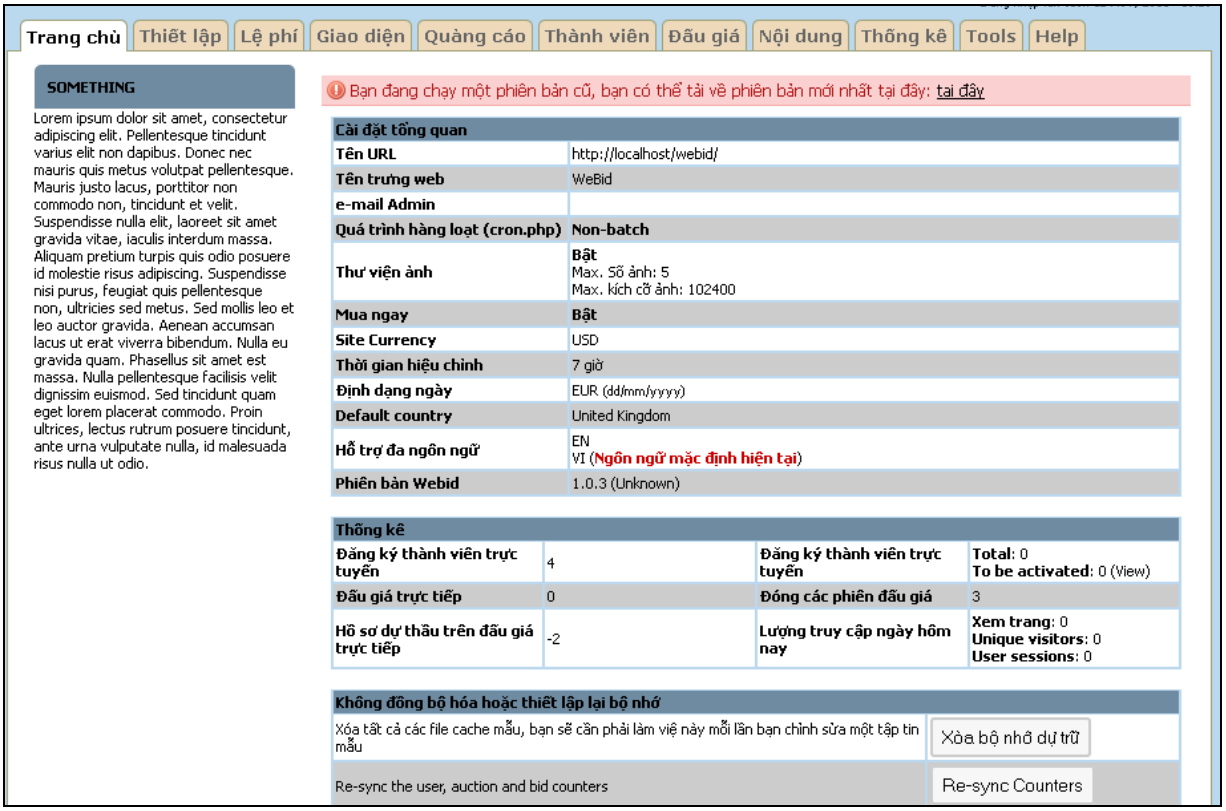
Chờ cho đến khi các kịch bản được cài đặt đầy đủ, sau đo nhấn vào liên kết "here" để truy cập vào admin của web và bạn có thể quản lý trang web của mình (Hình 4.6).



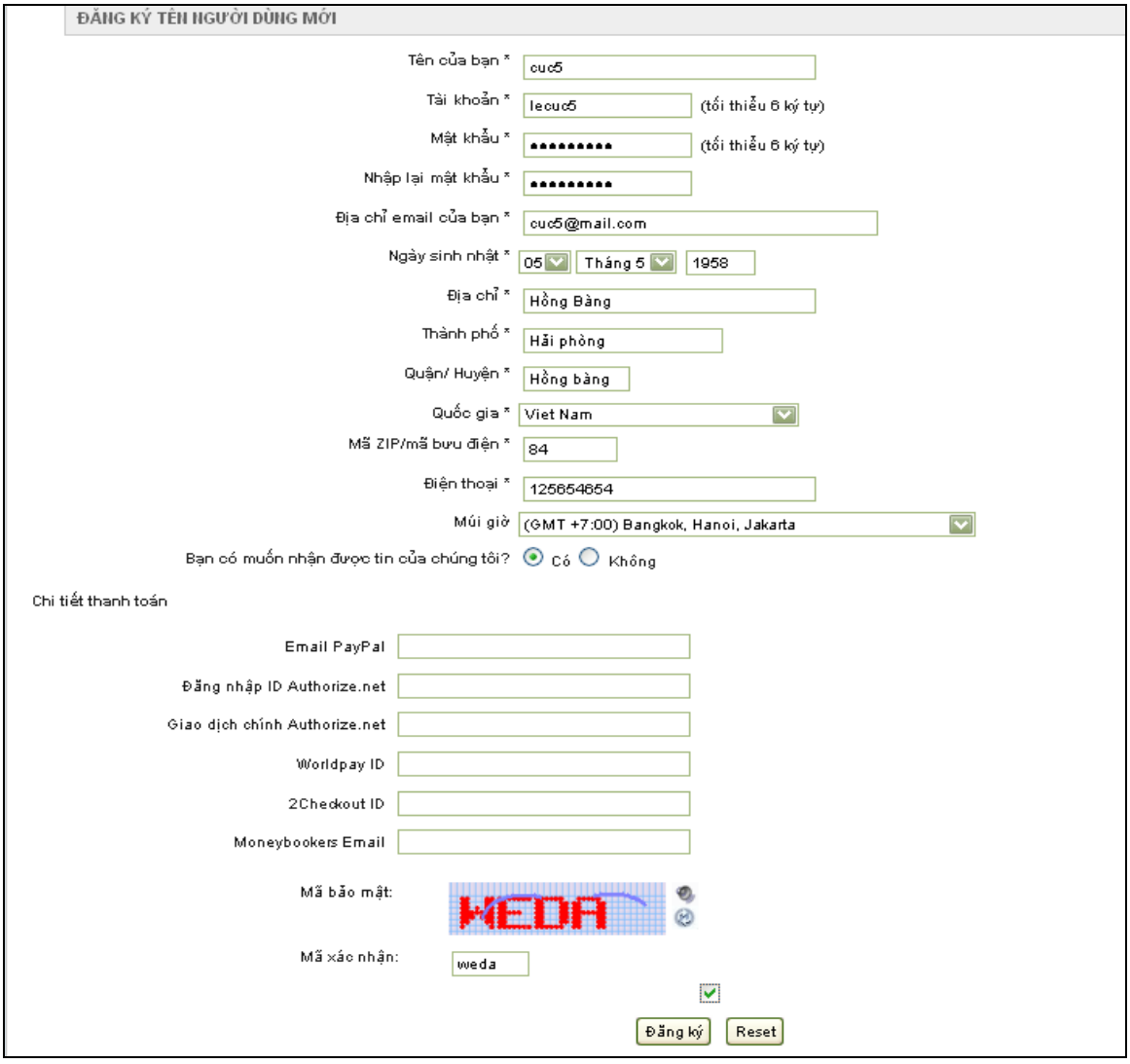
Hình 4.6: Cài đặt bước 3

Bước cuối cùng là xóa thư mục Install đi

4.4. Cấu hình website đấu giá



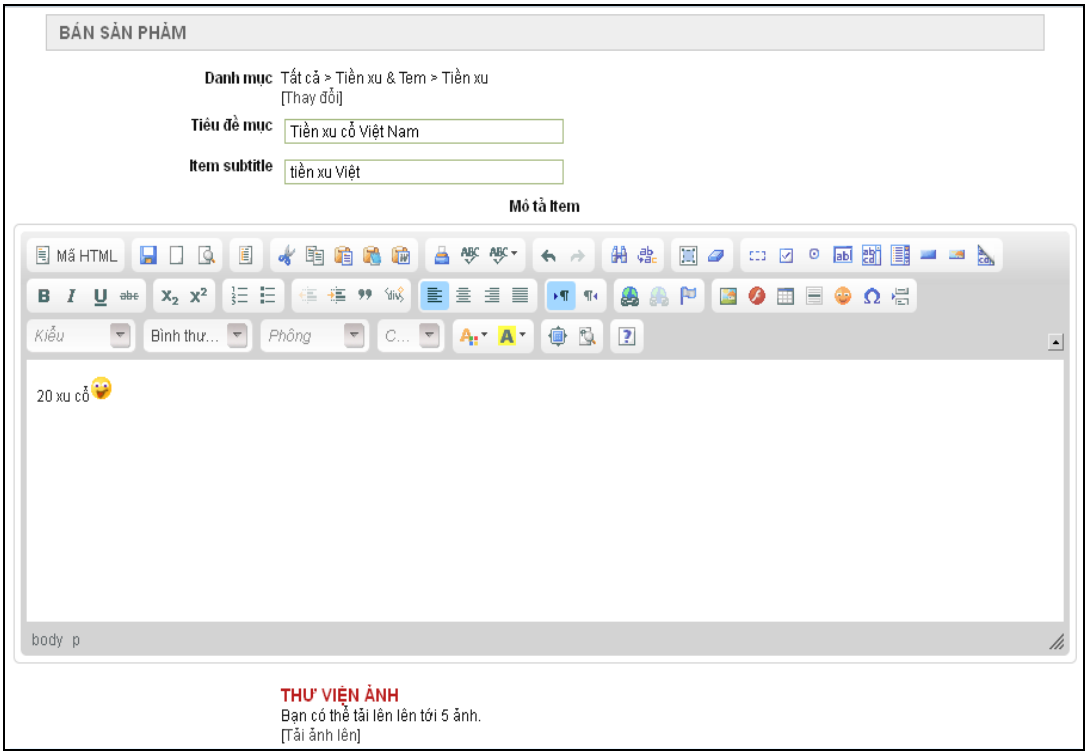
Hình 4.7: Trang chủ admin



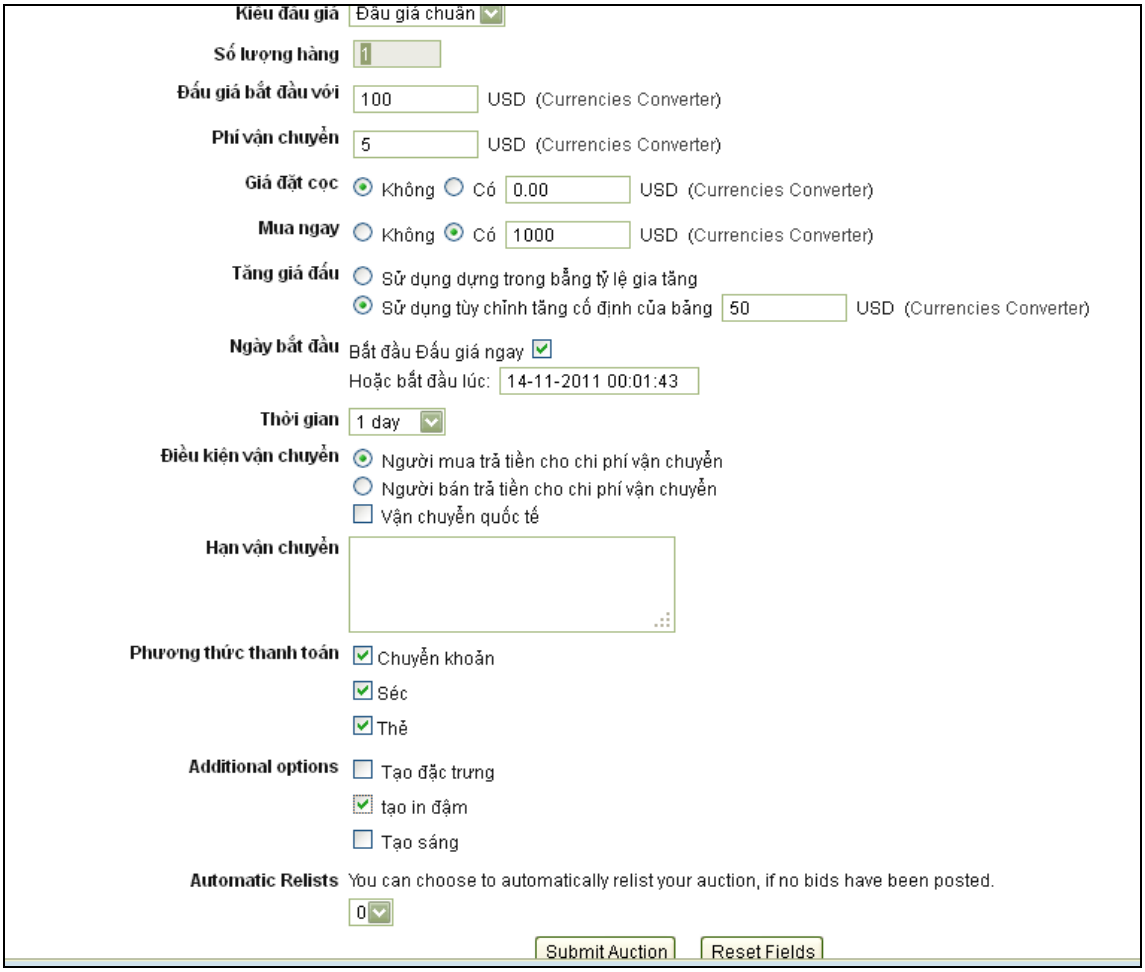
Hình 4.8 Trang Đăng ký

4.5. Cấu hình một phiên đấu giá

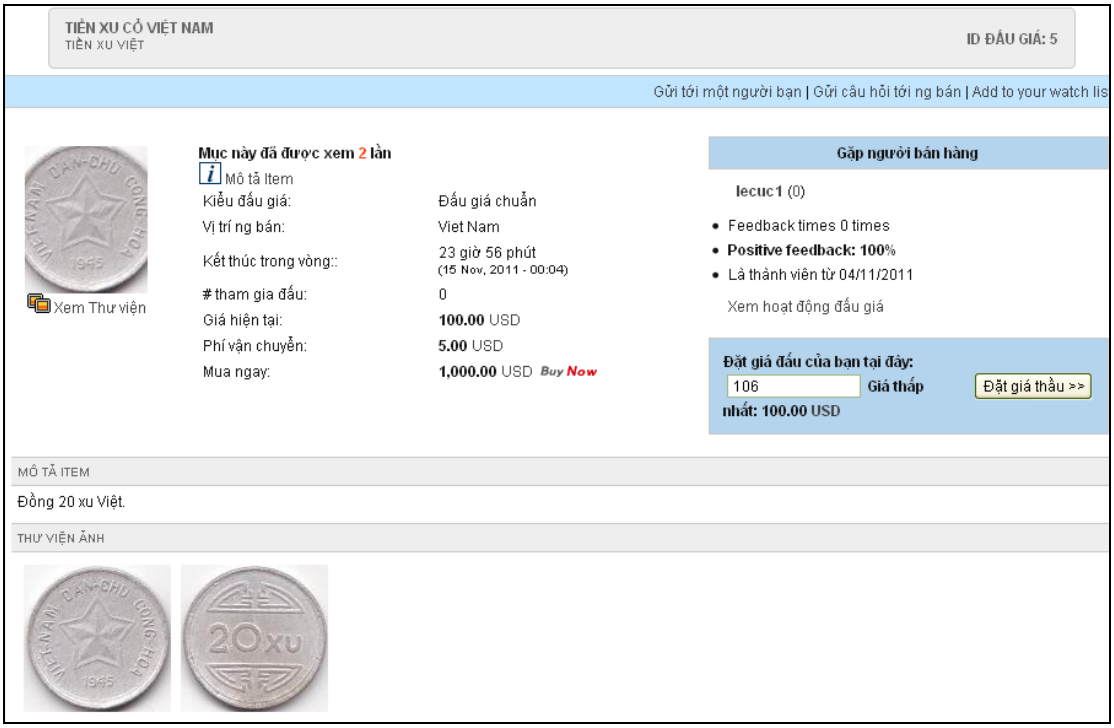
Hình 4.8: Đăng sản phẩm cần bán



Hình 4.9: Nhập thông tin và hình ảnh của mặt hàng



Hình 4.10: Thiết lập phiên đấu giá



Hình 4.11: Đặt giá đấu.

Hình 4.12: Xác nhận

Hình 4.13: Hoàn tất việc đấu giá

KẾT LUẬN

Đồ án tập trung vào tìm hiểu mô hình đấu giá điện tử, tìm hiểu các mã nguồn mở về đấu giá điện tử để qua đó phát triển ứng dụng đấu giá điện tử phù hợp. Về cơ bản đã đạt được những mục tiêu đề ra. Tuy nhiên, nếu có thêm cơ hội em mong muốn có thể được tiếp tục phát triển thêm đề tài này. Sau đây là kết quả đã làm được:

Kết quả cơ bản đã đạt được

- Về mặt lý thuyết
  - Nắm bắt được các kiến thức cơ bản về mật mã
  - Các kiến thức về chữ ký điện tử
  - Tìm hiểu một số mô hình đấu giá điện tử
- Về mặt ứng dụng

Xây dựng chương trình đấu giá điện tử với mã nguồn mở.

Định hướng phát triển trong tương lai:

- Việt hóa giao diện website.
- Hoàn thiện các chức năng, cải tiến giao diện người dùng.
- Tìm kiếm để đưa ra các chức năng mới phù hợp hơn.
- Tăng cường tính bảo mật trong giao dịch điện tử…

TÀI LIỆU THAM KHẢO

[1]. Douglas R. Stinson, *Cryptography. Theory and Practice*, CRC Press,1995.

[2]. A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.

[3]. Kazumasa Omote (2002), *A study on Electronic Auction*, Japan Advanced Institute of Science and Technology.

[4]. Phan Đình Diệu, Lý thuyết mật mã & An toàn thông tin; ĐH Quốc gia Hà Nội, khoa Công nghệ.