LỜI CẢM ƠN

Làm Đồ án tốt nghiệp là cơ hội để sinh viên ngành CNTT vận dụng những kiến thức trong quá trình học tập vào thực tiễn.

Trong quá trình làm Đồ án em đã được sự giúp đỡ tận tình của các thầy cô giáo, các cơ quan nơi em thực tập và xin tài liệu. Em xin chân thành gửi lời cảm ơn tới Ban giám hiệu trường Đại học Dân lập Hải Phòng, các thầy cô giáo; em xin chân thành cảm ơn TSKH Thầy giáo Hồ Văn Canh đã tận tình chỉ bảo và giúp đỡ em trong quá trình tiếp cận đề tài và thực hiện hoàn thành đồ án tốt nghiệp;

Đồ án tốt nghiệp là kết quả từ sự cố gắng, nỗ lực của em sau một thời gian nghiên cứu và tìm hiểu đề tài, là bước tập dượt cần thiết và bổ ích cho công việc của em trong tương lai. Mặc dù đã có nhiều cố gắng song khả năng của bản thân có hạn nên đồ án của em còn nhiều thiếu sót, em mong nhận được sự đóng góp ý kiến, chỉ bảo của các thầy cô giáo, các bạn sinh viên để em có thể rút ra những kinh nghiệm bổ ích cho bản thân.

Em xin chân thành cảm ơn!

Hải Phòng, ngày ... tháng ... năm 2010

Sinh viên

Bùi Đức Tuấn

MỤC LỤC

DANH MỤC CÁC TỪ VIẾT TẮT

BAC	Basic Access Control – Phương pháp kiểm soát truy cập cơ bản
DES	Data Encryption Standard – Thuật toán mã hóa dữ liệu chuẩn
CSCA	Country signing Certificate Authority – Cơ quan có thẩm quyền cấp phát chữ kí quốc gia
CA	Certificate Authority – Cơ quan có thẩm quyền cấp phát chữ kí số
CRL	Certificate Revocation List – Danh sách chứng chỉ bị thu hồi
PKC	Public Key Crytography – Thuật t oán mã hóa khóa công khai
DV	Document Verifier – xác thực tài liệu
EAC	Advanced Access Control – Phương pháp kiểm soát truy cập nâng cao
PKI	Public Key Infrastructure – Cơ sở hạ tầng khóa công khai
PKD	Public Key Directory – Thư mục khóa công khai do ICAO thiết lập để các nước thành viên truy cập sử dụng
ICAO	International Civil Aviation Orgnization – Tổ chức hàng không dân dụng quốc tế
ICC	Intergrated Circuit Chip – Vi mạch tích hợp
SHA	Secure Hash Standard – Thuật toán băm dữ liệu chuẩn
IS	Inspection System – Hệ thống kiểm soát tại các cửa khẩu quốc tế
ISO	International Organization for Standardization – Tổ chức tiêu chuẩn quốc tế
LDS	Logical Data Structure – Cấu trúc dữ liệu lôgic
NIST	National Institute of Standard and Technology – Học viện quốc gia về kĩ thuật và tiêu chuẩn (thuộc Mỹ)
MRZ	Machine Readable Zone – Vùng đọc được bằng máy trên hộ chiếu
RFIC	Radio Frequency Integrated Chip – Vi mạch tích hợp có khả năng trao đổi dữ liệu bằng sóng vô tuyến (radio)
RFID	Radio Frequency Identification – Nhận dạng bằng sóng vô tuyến

LỜI NÓI ĐẦU

Hiện nay, công nghệ sinh trắc học nói riêng và các công nghệ bảo vệ hộ chiếu, thị lực, các loại giấy tờ lien quan xuất nhập cảnh nói chung đang được nghiên cứu, phát triển rất mạnh mẽ trên thế giới. Đặc biệt là sau sự kiện 11/9/2001 nước Mĩ bị tấn công khủng bố, tất cả các nước trên thế giới đều rất quan tâm đến việc củng cố hệ thống an ninh, áp dụng nhiều biện pháp kĩ thuật nghiệp vụ để bảo vệ, chống làm giả hôh chiếu giấy tờ xuất nhập cảnh, đồng thời tăng cường kiểm tra, kiểm soát tại các cửa khẩu quốc tế để kịp thời phát hiện và ngăn chặn các phần tử khủng bố quốc tế. Mặt khác tình hình xuất nhập cảnh trái phép cũng diễn ra phức tạp. Hộ chiếu truyền thống không đáp ứng được hết yêu cầu đặt ra về tính tiện lợi của loại giấy tờ mang tính tương tác toàn cầu đó là độ an toàn và bảo mật thông tin, tránh làm giả và phải dễ dàng thuận tiện cho cơ quan kiểm soát xuất nhập cảnh cũng như công dân các quốc gia khi xuất nhập cảnh. Vì vậy trong bản nghị quyết của Tổ chức hàng không dân dụng thế giới (ICAO) phát hành năm 2003, tất cả các thành viên của tổ chức này sẽ triển khai ứng dụng hộ chiếu điện tử trước năm 2010.

Ngày nay, với những ứng dụng của CNTT, hộ chiếu điện tử đã nghiên cứu và đưa vào triển khai ,ứng dụng thực tế tại nhiều nước phát triển trên thế giới như Mỹ, Châu Âu,… Việc sử dụng hộ chiếu điện tử được xem như là 1 trong những biện pháp có thể tăng cường khả năng xác thực, bảo mật và an ninh cho cả người mang hộ chiếu cũng như quốc gia.

Việt Nam đang trên con đường hội nhập toàn diện với quốc tế, Chính phủ Việt Nam sẽ triển khai hộ chiếu điện tử trước năm 2010. Việc nghiên cứu công nghệ, xây dựng mô hình bảo mật hộ chiếu điện tử của Việt Nam đang được đặt ra. Với thực tế đó em đã mạnh dạn nghiên cứu về bảo mât thông tin trong hộ chiếu điện tử và phát triển thành luận văn tốt nghiệp với đề tài:

" Nghiên cứu, tìm hiểu chữ ký số và ứng dụng của nó để kiểm soát, xác thực và bảo vệ thông tin trong hộ chiếu điện tử".

Chương 1:

TỔNG QUAN HẠ TẦNG CƠ SỞ MÃ HÓA CÔNG KHAI VÀ CHỮ KÍ SỐ

1.1. TỔNG QUAN HẠ TẦNG CƠ SỞ MÃ HÓA CÔNG KHAI

1.1.1 Giới thiệu về mật mã học

1.1.1.1. Giới thiệu

Lý thuyết mật mã là khoa hoc nghiên cứu về cách viết bí mật, trong đó bản rõ được biến đổi thành bản mã, quá trình biến đổi đó được gọi là sự mã hóa. Quá trình ngược lại biến đổi bản mã thành bản rõ được gọi là sự giải mã.

Quá trình mã hóa được sử dụng chủ yếu để đảm bảo tính bí mật của các thông tin quan trọng, chẳng hạn như công tác tình báo, quân sự hay ngoại giao cũng như các bí mật về kinh tế, thương mại. Trong những năm gần đây lĩnh vực hoạy động của kĩ thuật mật mã đã được mở rộng: mật mã hiện đại không chỉ duy nhất thực hiện giu bí mật mà còn cung cấp cơ chế cho nhiều hoạt đông khác và có 1 loạt các ứng dụng như: chứng thực khóa công khai, chữ kí số, bầu cử điện tử hay thanh toán điênh tử.

Cả hai quá trinh mã hóa và giải mã đều được điều khiển bởi một hay nhiều khóa mật mã. Mã hóa và giải mã dễ dàng khi khóa đã biết, nhưng giải mã gần nhue không thể nếu không sử dụng khóa. Quá trình tìm thử một phương pháp ngắn gọn để giải mã bản mã khi khóa chưa biết gọi là "thám mã".

1.1.1.2. Các yêu cầu an toàn bảo mật thông tin

Hiện nay các biện pháp tấn công ngày càng tinh vi, đe dọa tới sự an toàn và bảo mật thông tin. Vì vậy chúng ta cần thiết lập các phương pháp đề phòng cần thiết. Mục đích cuối cùng của an toàn bảo mật là bảo vệ các thông tin và tài nguyên theo các tiêu chí sau:

1/. Tính bí mật

Đảm bảo dữ liệu đươc truyền đi một cách an toàn và không thể bị lộ thông tin nếu như có ai đó cố tình muốn có được nội dung của dữ liệu gốc ban đầu. Chỉ có người nhận đã xác thực mới có thể lấy ra được nội dung của thông tin của dữ liệu đã được mã hóa.

2/. Tính xác thực

Thông tin không thể bị truy nhập trái phép bởi những người không có thẩm quyền, giúp cho người nhận dữ liệu xác định được chắc chắn dữ liệu họ nhận được là dữ liệu gốc ban đầu của người gửi. Kẻ giả mạo không thể có khả năng để gỉa dạng một người khác hay nói cách khác là không thể mạo danh để gửi dữ liệu. Người nhận có khả năng kiểm tra nguồn gốc thông tin mà họ nhận được.

3/. Tính toàn vẹn

Thông tin không thể bị sửa đổi, bị làm giả bởi những người không có thẩm quyền, giúp cho người nhận dữ liệu kiểm tra được rằng dữ liệu không bị thay đổi trong quá trình truyền đi. Kẻ giả mạo không thể có khả năng thay thế dữ liệu dữ liệu ban đầu bằng dữ liệu giả mạo.

4/. Tính không thể chối bỏ

Thông tin được cam kết về mặt pháp luật của người cung cấp. Người gửi hay người nhận không thể chối bỏ sau khi đã gửi hoặc nhận thông tin .

5/. Đảm bảo tính sẵn sàng

Thông tin luôn sẵn sàng để đáp ứng sử dụng cho người có thẩm quyền. Người gửi không thể bị từ chối việc gửi thông tin đi.

6/. Tính chốnưg lặp lại

Không cho phép gửi thông tin nhiều lần đến người nhận mà người gửi không hề hay biết.

1.1.2 Hệ thống mã hóa (cryptosystem)

1). Định nghĩa:

Hệ mật mã là một hệ gồm có 5 thành phần: M, C, K, E, D

M (Message): là tập hữu hạn các bản rõ.

C (Ciphertext): là tập hữu hạn các bản mã.

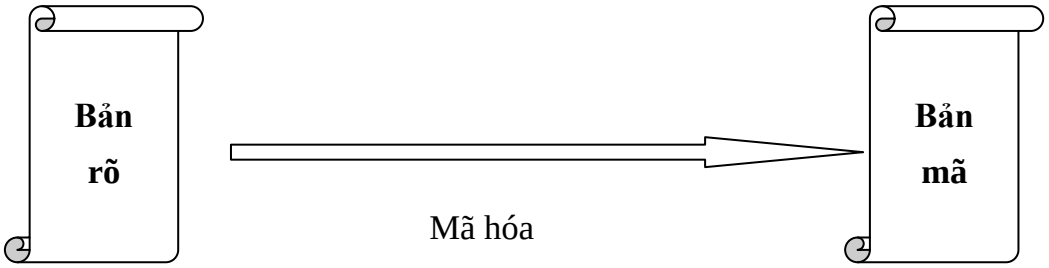
K (key): là tập các khóa.

E (Encryption): là tập các quy tắc mã hóa có thể

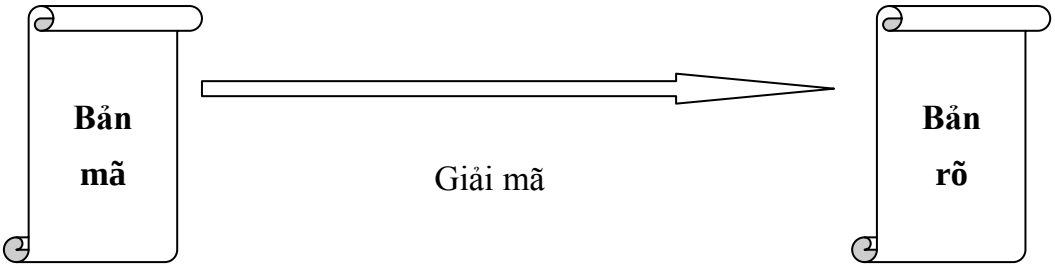
D (Decryption): là tập các quy tắc giải mã.

$C = E_k(P)$ và $P = D_k(C)$;

2). Sơ đồ



Hình 1.1: Quá trình mã hóa $C = E_k(P)$



Hình 1.2: Quá trình giải mã $M = D_k(C)$

1.1.2.1. Mã hóa đối xứng

Là phương pháp mã hóa sử dụng một cặp khóa đỗi xứng nhau: biết được khóa gửi thì cũng suy ra được khóa nhận và ngược lại. Vì vậy đòi hỏi cả hai khoá đều phải được giữ bí mật, chỉ có người gửi và người nhận biết.

Đây là phương pháp mã hóa sơ khai nhất, điển hình là phương pháp mã hóa Caesar: thay mỗi kí tự trong thông điệp bởi một kí tự đứng trước hoặc sau nó k vị trí trong bảng chữ cái hoặc mã hóa theo phương pháp thay thế. Việc mã hóa được thực hiện dựa trên một bảng chữ cái và một bảng chữ cái thay thế tương ứng.

Các phương pháp mã hóa đối xứng là:

- Mã dịch vòng (shift cipher):

Giả sử M = C = K với 0<k<25, định nghĩa:

$E_k(M) = M + k \bmod 26$

Và $D_k(M) = C + k \bmod 26$

Với M, C Є Z_{25} (nếu k = 3, hệ mật thường gọi là mã Caesar).

Ta sẽ sử dụng mã dịch vòng (với modulo 26) để mã hóa một văn bản tiếng anh thông thường bằng cách thiết lập sự tương ứng giữa các kí tự và các số dư theo modulo 26 như sau: A ⟷ 0, B ⟷ 1, … Z ⟷ 25.

Ví dụ khóa cho mã dịch vòng là k = 11 và bản rõ là: wewillmeetatmidnight

Trước tiên biến đổi bản rõ thành dãy các số nguyên nhờ dùng phép tương ứng trên. Ta có:

w-22, e-4, w-22, i-8, l-11, m-12, e-4, e-4, t-19, a-0, t-19, m-12, i-8, d-3, n-13, i-8, g-6, h-7, t-19.

Sau đó cộng 11 vào mỗi giá trị rồi rút gọn tổng theo modulo 26:

7 15 7 19 22 22 23 15 15 4 11 4 23 19 14 24 19 17 18 4

Cuối cùng biến đổi dãy số nguyên này thành các kí tự và thu được bản mã sau:

HPHTWWXPPELEXTOYTRSE

Và để giải bản mã này, người nhận sẽ biến đổi bản mã thành dãy các số nguyên, rồi trừ mỗi giá trị cho 11 (rút gọn theo modulo 26) và cuối cùng biến đổi lại dãy thành các kí tự.

- ***Mã thay thế (M, C, K, E, D)***

M = C = $Z_{26,}$ K = S (Z_{26}). Ta có:

$e_\pi(x) = \pi(x)$,

$d_\pi(y) = \pi^{-1}(y)$, với mọi x Є M, y Є C, π Є K

là một phép hoán vị trên Z_{26}.

Ta thường đồng nhất Z_{26} với bảng kí tự tiếng Anh, do đó phép hoán vị trên Z_{26} cũng được hiểu là một phép hoán vị trên tập hợp các kí tự tiếng Anh, Ví dụ một phép hoán vị π được cho bởi bảng:

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
X	N	Y	A	H	P	O	G	Z	Q	W	B	T	S	F	L	R	C	V	M	U	E	K	J	D	I

Với hệ mật mã thay thế có khóa π, bản rõ

x= hengapnhauvaochieuthubay

sẽ được chuyển thành bản mật mã

y= ghsoxlsgxuexfygzhumgunxd

Thuật toán giải mã với khóa π, ngược lại sẽ biến y thành bản rõ x.

- ***Mã Affine.*** Mã dịch vòng là một trường hợp đặc biệt của mã thay thế chỉ gồm 26 trong số 26! các hoán vị có thể của 26 phần tử. Một trường hợp đặc biệt khác của mã thay thế là mã Afine.

- ***Mã Vigenère.***

Các phương pháp mã hóa sơ khai này có ưu điểm là việc mã hóa và giải mã đơn giản tuy nhiên rất dễ bị phá mã dựa trên việc tính toán xác suất xuất hiện của các chữ cái được sử dụng cùng với các kiến thức về ngôn ngữ và nhất là được trợ giúp đắc lực của các máy tính có tốc độ cao hiện nay.

Để khắc phục nhược điểm này, hầu hết các các thuật toán cải tiến khóa đối xứng cuối thế kỉ XX đều dựa trên nguyên lí của Claude Shannon về sự ***hỗn loạn*** *(confiusion)* và ***khuyếch tán*** *(diffusion)* thông tin. Tính hỗn loạn giúp phá vỡ mối quan hệ giữa thông điệp nguồn và thông điệp mã hóa, còn sự khuyếch tán sẽ phá vỡ và phân tán các phần tử trong các mẫu xuất hiện trong thông điệp nguồn để không thể phát hiện ra các mẫu này trong thông điệp sau khi mã hóa. Shanmon cho rằng có thể sử dụng ***phép thay thế*** và ***biến đổi tuyến tính*** để tạo ra sự hỗn loạn và khuyếch tán thông tin. Hiện nay, hai kiến trúc chính của các phương pháp mã hóa theo khối là mạng thay thế - hoán vị (substitution Permutation Network - SPN) và mạng Feistel. DES (**Data Encryption Standard**) là một trong số các thuật toan đó. Đây là thuật toán dựa trên kiến trúc mạng Fiestel được Viện tiêu chuẩn và Công nghệ Quốc gia **(National Institute of Standard and Technology - NIST)** của Mĩ đưa ra giữa thập kỉ 1970. Theo đó, khóa là một số nhị phân có độ dài 56bits và dữ liệu cần mã hóa là một số nhị phân có đọ dài 64 bits. Thời gian đầu, DES được ứng dụng rộng dãi và được đầu tư nghiên cứu rất nhiều. Tuy nhiên, với sự phát triển của các thế hệ máy tính, phương pháp này đã trở lên không còn đủ an toàn để bảo vệ các thông tin quan trọng và nhạy cảm. Vào năm 1997, có tài liệu đã công bố rằng với độ dài khóa là 54bits khóa DES có thể bị bẻ trong vòng 4 tháng bởi brute-force attack.

Đó là lí do để năm 1997 NIST đã kêu gọi các nhà nghiên cứu xây dựng thuật toán mã hóa theo khối an toàn hơn để chọn ra thuật toán chuẩn mã hóa nâng cao ASE (Advanced Encryption Standaed). Ngày 2 tháng 10 năm 2000, phương pháp Rijndael của hai tác giả người Bỉ và Vincent Rijmen và Joan Daemen, được xây dựng theo kiến trúc SPN, đã chính thức được chọn trở thành chuẩn AES (tên của một thuật toán được lấy từ các chữ cái đầu trong tên của hai tác giả). Rijndael là phương pháp mã hóa theo

khối có kích thước khối và khóa thay đổi linh hoạt với các gía trị 128, 192 hay 256 bit. Như vậy, ta có 9 khả năng chọn lựa kích thước khối và khóa cho thuật toán này. Tuy nhiên, tài liệu đặc tả chuẩn AES đã giới hạn lại kích thước khối và khóa đều là 128 bit. Như vậy, khi đề cập đến chuẩn AES, chúng ta đang nói đến trường hợp có kích thước khối và khóa ngắn nhất của thuật toán Rijndael; còn khi nhắc đến phương pháp Rijndael, chúng ta đang đề cập đến thuật toán gốc với khả năng thay đổi kích thước khối và khóa.

Người ta cũng đã chứng minh được rằng nếu giả sử thời gian để brute-force bẻ một khóa DES khóa 56-bits là 1 giây thì phải mất tới 149 nghìn tỉ (trillion -10^{12}) năm mới có thể bẻ được một khóa ASE.

1.1.2.2. Mã hóa công khai

Ta đã biết, trong các thuật toán mã hóa đối xứng, khóa mã và khóa giải mã đối xứng với nhau, người gửi và người nhận cần phải thỏa thuận trước và giữ bí mật cặp khóa này, nếu cặp khóa này được trao đổi qua các môi trường khác thì cũng có khả năng bị "ăn cắp" .Chính vì thế ý tưởng về t hệ thống mã hóa công cộng đã được Whitfield Diffie và Martin Hellman đưa ra và giải quyết vào năm 1976.

Bản chất của các thuật toán khóa công khai (PKC- Public Key Crytography) là mỗi bên (người gửi, người nhận) sử dụng một cặp khóa (một khóa dùng để mã hóa và một khóa dùng để giải mã). Trong đó khóa mã được công khai (PK- Public key), khóa giải mã là bí mật (SK- secret key), người gửi không cần biết không cần biết khóa bí mật của người nhận.

Quá trình truyền và sử dụng mã hóa khóa công khai được thực hiện như sau:

- Bên gửi yêu cầu cung cấp hoặc tự tìm khóa công khai của bên nhận trên một máy chủ chịu trách nhiệm quản lí khóa.

- Sau đó bên gửi sử dụng khóa công khai của bên nhận cùng với thuật toán đã thống nhất để mã hóa thông tin được gửi đi.

- Khi nhận được thông tin đã mã hóa, bên nhận sử dụng khóa bí mật của mình để giải mã và lấy ra thông tin ban đầu.

Sau đây em xin trình bày về một số hệ mật khóa công khai như: hệ mật xếp ba lô (Knapsack), hệ RSA, Elgamal.

A. Hệ RSA

Năm 1978, Rivest, Sharmir và Adleman (RSA) là những người đầu tiên công bố việc thực hiện hệ mật khóa công khai dựa trên cơ sở tính các lũy thừa trong số học modulo. Tính mật của hệ dựa trên đọ khó của việc phân tích ra thừa số nguyên tố. Nhiều hệ mật khóa công khai sau này đã được phát triển nhưng đều thua kém hệ RSA.

a. Phương pháp lập mã và giải mã

- Tạo khóa

Trước khi lập mã và giải mã phải tạo một cặp khóa gồm khóa công khai và khóa bí mật. Giả sử Alice cần trao đổi thông tin với Bob thì Bob cần tính các bước sau:

1. Chọn 2 số nguyên tố lớn *p* và *q* với $p \neq q$, lựa chọn ngẫu nhiên và độc lập.
2. Tính $n = pq$
3. Tính giá trị hàm số Ơle*:* $\varphi(n)= (p - 1)(q - 1)$.
4. Chọn một số tự nhiên *e* sao cho $1< e < \varphi(n)$ và là số nguyên tố cùng nhau với $\varphi(n)$.
5. Tính: *d* sao cho $de \equiv 1 \pmod{\varphi(n)}$.

Cặp số nguyên dương (n,e) gọi là khóa lập mã công khai, số d gọi là khóa giải mã bí mật.

- Mã hóa

Để mã hóa thông báo M, đầu tiên biểu diễn thông báo M như là một số nguyên giữa 0 và n-1 bằng cách sử dụng mã ASCII tương ứng (từ 0 đến 255). Chia khối thông báo thành một dãy các khối có kích thước thích hợp. Một kích thước thích hợp của khối là số nguyên i nhỏ nhất thỏa mãn $10^{i-1} <n < 10^i$. Sau đó ta mã hóa từng khối riêng biệt bằng cách nâng nó lên lũy thừa e modulo n. Bản mã C là kết quả của phép tính $C= E(M)= M^e \bmod n$.

- Giải mã

Sau khi nhận được bản mã C, Bob sẽ dùng khóa bí mật d của mình để giải mã theo công thức:

$M= D(C)= C^d \bmod n$.

b. Ví dụ

Mã hóa bản rõ AGRICULTURES với p =113, q = 83

Ta có: n = p*q = 9379 và φ(n) = (p-1)*(q-1) = 9184

Chọn e = 157 ta có $d = e^{-1} = 117$

Cặp (n,e) = (9379, 157) làm thành khóa lập m ã công khai và d = 117 là khóa giải mã bí mật.

Vì $10^3 < n < 10^4$, do đó ta sẽ chia bản rõ thành các khối, mỗi khối gồm 4 chữ số

Bản rõ ban đầu được chuyển thành:

6571 8273 6785 7684 8582 6983

- Lập mã:

$6571^{157} \bmod 9379 = 6783$

$8273^{157} \bmod 9379 = 8000$

…….

$6983^{157} \bmod 9379 = 2101$

Giải mã:

$6783^{117} \bmod 9379 = 6571$

$8000^{117} \bmod 9379 = 8273$

…….

Ta thu được bản rõ.

B. Hệ mật xếp ba lô

a. Mô tả hệ mật xếp ba lô

Cho một tập hợp các số nguyên dương s. Hãy xác định xem có hay không một tập hợp con các a_j mà tổng của chúng bằng s. Một cách tương đương , hãy xác định xem có hay không các $x_i \in \{0,1\}$ $(1 \le i \le n)$ sao cho $\sum_{i=1}^{n} a_i x_i = s$.

Bài toán quyết định tổng các tập con là một bài toán NP đầy đủ. Điều kiện đó có nghĩa là trong số các thuật toán khác nhau, không có một thuật toán với thời gian đa thức nào tìm được quyết định lựa chọn phù hợp. Điều này cũng đúng với bài toán tìm tổng các tập con. Song ngay cả khi một bài toán không có thuật giải với thời gian đa thức nói chung thì vẫn có những trường hợp nhất định có thể giải với thời gian đa thức nói chung thì vẫn có những trường hợp nhất định có thể giải với thời gian đa thức. Điều này cũng đúng với trường hợp bài toán tổng các tập con. Tuy nhiên nếu ta hạn chế bài toán trên các dữ liệu $I = (\{a_1,a_2,...,a_n\},T)$, trong đó $\{a_1,a_2,...,a_n\}$ là dãy *siêu tăng,* tức là dãy thỏa mãn điều kiện:

$\forall$ j = 2,3,…,n: $a_j > \sum_{i=1}^{j-1} a_i$, tức là các thành phần được sắp

xếp tăng dần và từ thành phần thứ hai trở đi nó sẽ lớn hơn tổng các thành phần đứng trước nó thì việc tìm câu trả lời là khá dễ dàng, chẳng hạn có thể bằng thuật toán đơn giản trước đây:

1. **for** $i = n$ **downto** 1 **do**
   if $T > a_i$ **then**
   $T = T - a_i$
   $x_i = 1$
   else
   $x_i = 0$
2. **if** $\sum_{i=1}^{n} x_i.a_i = T$ **then**
3. $X = (x_1,..,x_n)$ là giải pháp cần tìm
   Else Không có giải pháp.

Bây giờ, để chuẩn bị xây dựng một sơ đồ hệ mật xếp ba lô, ta chọn trước một số nguyên dương *n* và một số nguyên tố *p* đủ lớn. Với mỗi người tham gia sẽ được chọn một bộ khóa K = (K', K"), trong đó khóa bí mật K" =

(A, p, a) gồm một dãy siêu tăng A = $\{a_1, a_2, \ldots, a_n\}$ thỏa mãn $\sum_{i=1}^{n} a_i < p$, và

một số a, $1 \le a \le p-1$; khóa công khai K' = $\{b_1,\ldots, b_n\}$ với $b_i = a.a_i \bmod p$.

Sơ đồ hệ mật xếp ba lô:

$$S = (M, C, K, E, D)$$

Trong đó $P = \{0,1\}^n$, $C = \{0,1,\ldots, n(p-1)\}$, là tập hợp các bộ khóa $K = (K',K")$ như được xây dựng ở trên. Các thuật toán lập mật mã và giải mã được xác định bởi:

Với mọi $x = (x_1,..., x_n) \in P$, thuật toán lập mã cho ta:

$$E(K',x) = \sum_{i=1}^{n} x_i.b_i ;$$

và với mọi y Є *C* tức $0 \leq y \leq n(p-1)$, ta xác định $z = a^{-1}y \bmod p$, rồi sau đó giải bài toán sắp ba lô đối với dữ liệu $I=(\{a_1,a_2,..., a_n\}, z)$ ta sẽ được lờ giải $(x_1,...,x_n)$, lời giải đó là giá trị của $D(K'', y) = (x_1,\ldots, x_n) = x$.

b. Thực thi hệ mật xếp ba lô

Chọn n = 6, khóa bí mật có p = 737, A= {12, 17, 33, 74, 157, 316}, a=635. Tính được khóa công khai là {250, 477, 319, 559, 200, 196}. Với bản rõ *x* = 101101 ta có bản mã tương ứng là y = 1324.

Khi Bob nhận được bản mã y, đầu tiên anh ta tính:

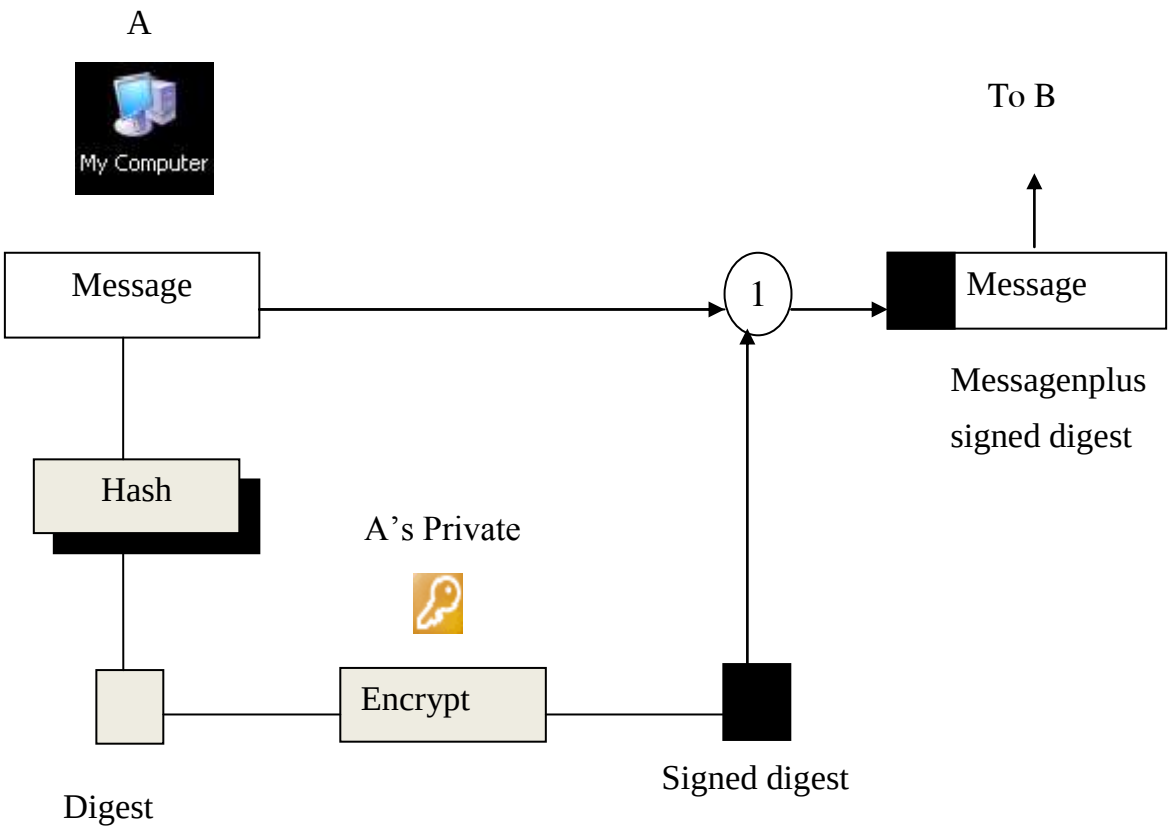
$z = a^{-1}y \bmod p = 635^{-1}.1324 \bmod 737 = 435$

sau đó, Bob sẽ giải trường hợp *I* =(a, z) của bài toán sắp ba lô với dãy siêu tăng a và z ta được:

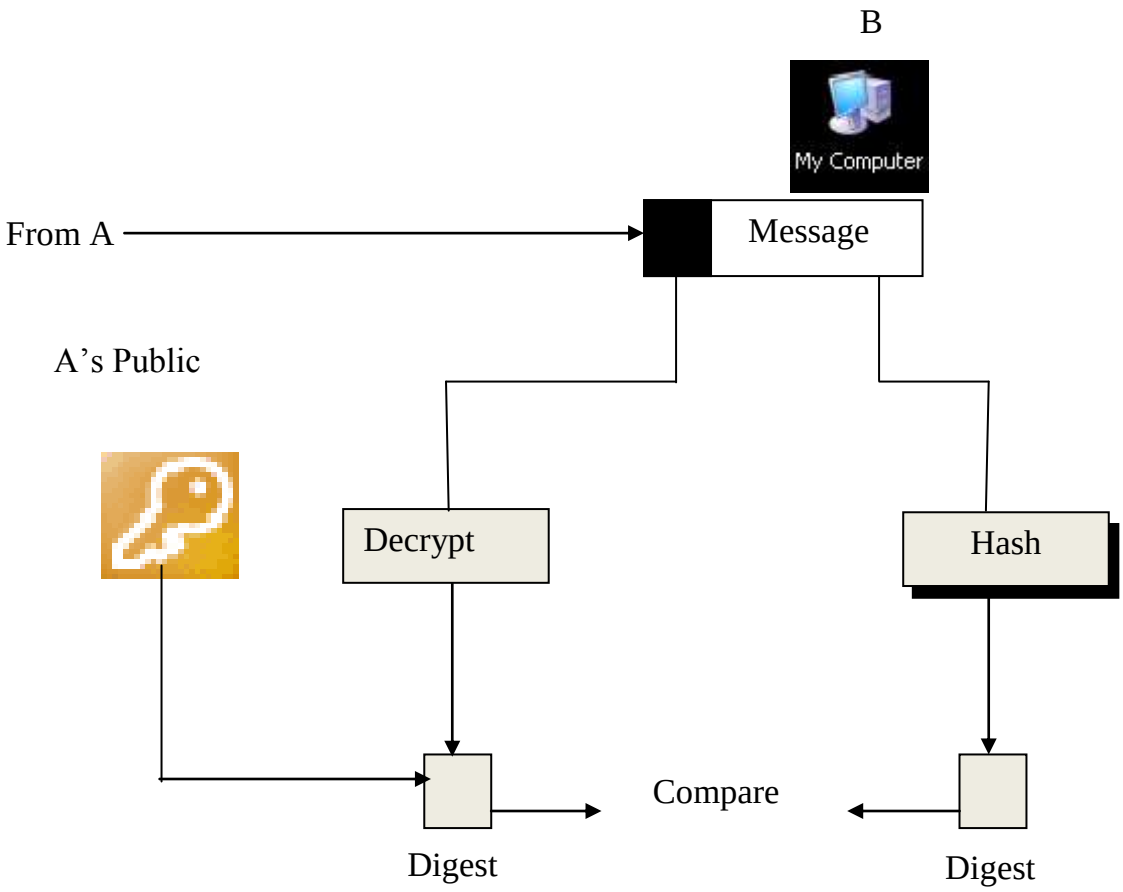
435 = 12 + 33 +74 + 316, tức được lời giải *x* = (1,0,1,1,0,1).

1.1.3. Hàm băm

Hàm băm mật mã là hàm toán học chuyển đổi một thông điệp có độ dài bất kì thành một chuỗi bit có độ dài cố định (tùy thuộc vào thuật toán băm). Dãy bit này được gọi là thông điệp rút gọn (message digest) hay giá trị băm (hash value), đại diện cho thông điệp ban đầu.



Hình 1.3: Mô hình sử dụng hàm băm bên gửi



Hình 1.4: Mô hình sử dụng hàm băm bên nhận

Một số tính chất của hàm băm:

- Các thuật toán băm là hàm một chiều, do đó rất khó để xây dựng lại thông điệp ban đầu từ thông điệp rút gọn.
- Tuy nhiên hàm băm *h* không phải là một song ánh. Do đó, với thông điệp *x* bất kì, tồn tại thông điệp *x' ≠ x* sao cho *h*(x) = *h*(x'). Lúc này, ta nói rằng "có sự đụng độ xảy ra " – Đây cũng là môt đăc điểm dễ bị lợi dụng để mã hóa các hàm băm, khi không tìm được thông điệp gốc x, các thuật toán phá khóa sẽ đi tìm các hàm *x' ≠ x* sao cho *h(x) = h(x').*

Một hàm băm *h* được gọi là an toàn (hay "ít bị đụng độ") khi không thể xác định được (bằng cách tính toán) cặp thông điệp *x và x'* thỏa mãn *x' ≠ x* và *h(x) = h(x').*

- Hàm băm giúp xác định được tính toàn vẹn dữ liệu của thông tin: mọi thay đổi, dù là rất nhỏ, trên thông điệp cho trước, ví dụ như đổi giá trị 1 bit, đều làm thay đổi thông điệp rút gọn tương ứng. Tính chất này hữu ích trong việc phát sinh, kiểm tra chữ kí điện tử, các đoạn mã chứng nhận thông điệp, phát sinh số ngẫu nhiên, tạo ra khóa cho quá trình mã hóa…

Thuật toán băm phổ biến :

- ***Thuật toán Secure Hash Standard*** (SHS)
- Thuật toán Secure Hash Standard (SHS) do NIST và NSA (National Security Agency) xây dựng được công bố trên Federal Rigister vào ngày 31 tháng 1 năm 1992 và sau đó chính thức trở thành phương pháp chuẩn từ ngày 13 tháng 5 năm 1993. Thông điệp rút gọn có độ dài 160 bit.
- Ngày 26 tháng 8 năm 2002, Viện tiêu chuẩn và Công nghệ quốc gia của Hoa Hỳ (National Institue of Standard and Technology - NIST) đã đề xuất hệ thống chuẩn hàm băm an toàn (Secure Háh Standard) gồm 4 thuật toán hàm băm SHA-1, SHA-256, SHA-384, SHA- 512. Đến 25/03/2004, NIST đã chấp nhận them thuật toán hàm băm SHA-224 vào hệ thống chuẩn hàm băm. Các thuật toán hàm băm do NIST đề xuất được đặc tả trong tài liệu FIPS180-2.

Các thuật toán hàm băm SHA gồm 2 bước: tiền xử lí và tính toán giá trị băm.

❖ *Bước tiền xử lí bao gồm các thao tác:*

- Mở rộng thông điệp
- Phân tích thông điệp đã mở rộng thành các khối m bit
- Khởi tạo giá trị băm ban đầu

❖ *Bước tính toán giá trị băm bao gồm các thao tác:*

➢ Làm n lần các công việc sau:

▪ Tạo bảng phân bố thông điệp (message schedule) từ khối thứ *i.*

▪ Dùng bảng phân bố thông điệp cùng với các hàm, hằng số, các thao tác trên từ để tạo ra giá trị băm *i.*

➢ Sử dụng giá trị băm cuối cùng để tạo thông điệp rút gọn.

Thông điệp *M* được mở rộng trước khi thực hiện băm. Mục đích của việc mở rộng này nhằm đảm bảo thông điệp mở rộng có độ dài là bội số 512 hoặc 1024 bit tùy thuộc vào thuật toán.

Sau khi thông điệp đã mở rộng thông điệp cần được phân tích thành N khối m-bit trước khi thực hiện băm.

Đối với SHA-1 và SHA-256, thông điệp mở rộng được phân tích thành N khối 512-bit $M^{(1)}$, $M^{(2)}$,..., $M^{(n)}$. Do đó 512 bit của khối dữ liệu đầu vào có thể được thể hiện bằng 16 từ 64-bit, $M_0^{(i)}$ chứa 32 bit đầu của khối thông điệp *i*, $M_1^{(i)}$ chứa 32 bit kế tiếp…

Đối với SHA-384 và SHA-512, thông điệp mở rộng được phân tích thành N khối 1024-bit $M^{(1)}$, $M^{(2)}$, ..., $M^{(n)}$. Do đó 1024 bit của khối dữ liệu đầu vào có thể được thể hiện bằng 16 từ 64-bit, $M_0^{(i)}$ chứa 64 bit đầu của khối thông điệp *i*, $M^{(i)}$ chứa 64 bit kế tiếp…

Trước khi thực hiện băm, với mỗi thuật toán băm an toàn, giá trị băm ban đầu $H^{(0)}$ phải được thiết lập. Kích thước và số lượng từ trong $H^{(0)}$ tùy thuộc vào kích thước thông điệp rút gọn.

Các cặp thuật toán SHA-224 và SHA-256; SHA-384 và SHA-512 cáo các thao tác thực hiện giống nhau, chỉ khác nhau về số lượng bit kết quả của thông điệp rút gọn. Nói cách khác, SHA-224 sử dụng 224 bit đầu tiên trong kết quả thông điệp rút gọn sau khi áp dụng thuật toán SHA-256. Tương tự SHA-384 sử dụng 384 bit đầu tiên trong kết quả thông điệp rút gọn sau khi áp dụng thuật toán SHA-512.

Trong các hàm băm SHA, chúng ta cần sử dụng thao tác quay phải một từ, ký hiệu là ROTR, và thao tác dịch phải một từ, ký hiệu là SHR.

Nhận xét:

Mỗi thuật toán có bảng hằng số phân bố thông điệp tương ứng.Kích thước bảng hằng số thông điệp (scheduleRound) của SHA-224 và SHA-256 là 64, kích thước bảng hằng số thông điệp của SHA-384 và SHA-512 là 80.

Chuẩn SHA đặc tả 5 thuật toán băm an toàn SHA-1, SHA-224[1], SHA-256, SHA-384 và SHA-512.

Sự khác biệt chính của các thuật toán là số lượng bit bảo mật của dữ liệu băm – điều này có ảnh hưởng trực tiếp đến chiều dài của thông điệp rút gọn. Khi một thuật toán băm được sử dụng kết hợp với thuật toán khác đòi hỏi phải cho kết quả số lượng bit tương ứng. Ví dụ, nếu một thông điệp được kí với thuật toán chữ kí điện tử cung cấp 128bit thì thuật toán chữ kí đó có thể đòi hỏi sử dụng một thuật toán băm an toàn cung cấp 128bit như SHA-256.

Thuật toán	**Kích thước (bit)**				**Độ an toàn[2] (đơn vị: bit)**
	Thông điệp	Khối	Từ	Thông điệp rút gọn	
SHA-1	$< 2^{64}$	512	32	160	80
SHA-224	$< 2^{64}$	512	32	224	112
SHA-256	$< 2^{64}$	512	32	256	128
SHA-384	$< 2^{128}$	1024	64	384	192
SHA-512	$< 2^{128}$	1024	64	512	256

Các tính chất của thuật toán băm an toàn

Tuy nhiên, tháng 2 năm 2005 SHA-1 bị tấn công và giải mã bởi 3 chuyên gia người Trung Quốc thông qua phương pháp tính phân bổ.

1.2. CHỮ KÍ SỐ

1.2.1. Giới thiệu về chữ kí số

Để hiểu về chữ kí số trước tiên ta tìm hiểu thế nào là chữ ký điện tử?

Chữ ký điện tử là thông tin đi kèm dữ liệu (văn bản, hình ảnh, video,…) nhằm mục đích xác định người chủ của dữ liệu đó.

Ta cũng có thể sử dụng định nghĩa rộng hơn, bao hàm cả mã nhận thực, hàm băm và các thiết bị bút điện tử.

Chữ ký khóa số công khai (hay hạ tầng khóa công khai) là mô hình sử dụng các mật mã để gắn với mỗi người sử dụng một cặp khóa công khai – bí mật và qua đó có

thể ký các văn bản điện tử cũng như trao đổi các thông tin mật. Khóa công khai thường được phân phối thông qua chứng thực khóa công khai. Quá trình sử dụng chữ ký số bao gồm 2 quá trình: tạo chữ ký và kiểm tra chữ ký.

Khái niệm chữ ký điện tử mặc dù thường được sử dụng cùng nghĩa với chữ ký số nhưng thực sự có nghĩa rộng hơn. Chữ ký điện tử chỉ đến bất ký phương pháp nào (không nhất thiết là mật mã) để xác định người chủ của văn bản điện tử. Chữ ký điện tử bao gồm cả địa chỉ telex và chữ ký trên giấy được truyền bằng fax.

Khi nhận được một văn bản bằng giấy, các khía cạnh sau đây thường được xem xét từ phía người nhận:

- Ai là người viết ra, có trách nhiệm với văn bản này?
- Từ khi được gửi đi từ người viết đến khi nhận được từ người đọc, nội dung văn bản có bị thay đổi gì không?
- Người viết văn bản không chối bỏ những nội dung mà mình đã viết ra và gửi đi.
- Từ khi được gửi đi từ người viết đến khi nhận được từ người đọc, nội dung văn bản không bị đọc từ người thứ ba khác?

Nếu được diễn giải dưới góc độ chuyên môn của an toàn thông tin (Information Security), văn bản này được xem xét dưới các khía cạnh:

- Tính xác thực của người gửi (Authentication)
- Tính toàn vẹn của văn bản (Integrity)
- Tính chống từ chối, chống chối bỏ (Non-repudiation)
- Tính bí mật hay tính riêng tư (Privace)

Quay lại một văn bản bằng giấy, các vấn đề trên được giải quyết như thế nào:

- Ai là người viết ra, có trách nhiệm với văn bản này: kiểm tra họ, tên người kí văn bản
- Từ khi được gửi đi từ người viết đến khi nhận được từ người đọc, nội dung văn bản có bị thay đổi gì không: xem xét các chữ kí trên từng trang, tính liên tục của đánh số trang,…
- Người viết văn bản không chối bỏ những nội dung mà mình viết ra và gửi đi: kiểm tra chữ kí cuối cùng của văn bản là chữ kí hợp lệ của người gửi, so sánh chữ kí này với chữ kí mẫu của người đó mà mình đã có.
- Từ khi văn bản được gửi đi từ người viết đến khi người nhận nhận được văn bản đó thì nội dung văn bản không bị đọc bởi một người thứ ba khác: kiểm tra phong bì đựng văn bản có còn nguyên trạng không?

Khi trao đổi một "văn bản" trong môi trường điện tử (một email, một đoạn dữ liệu trong giao dịch, một file dữ liệu,…) cả bốn khía cạnh nêu trên cũng cần được xem xét trong điều kiện không có "chữ kí", "phong bì",… Tuy nhiên các vấn đề nêu trên đã được giải quyết về mặt công nghệ khi các tiến trình và giải thuật sử dụng khóa phi đối xứng

(asymmetric key) được phát triển và hoàn thiện. Sau đây em xin trình bày về tiến trình xử lý kí và xác thực chữ kí số như sau:

1.2.2. Quá trình kí và xác thực chữ kí

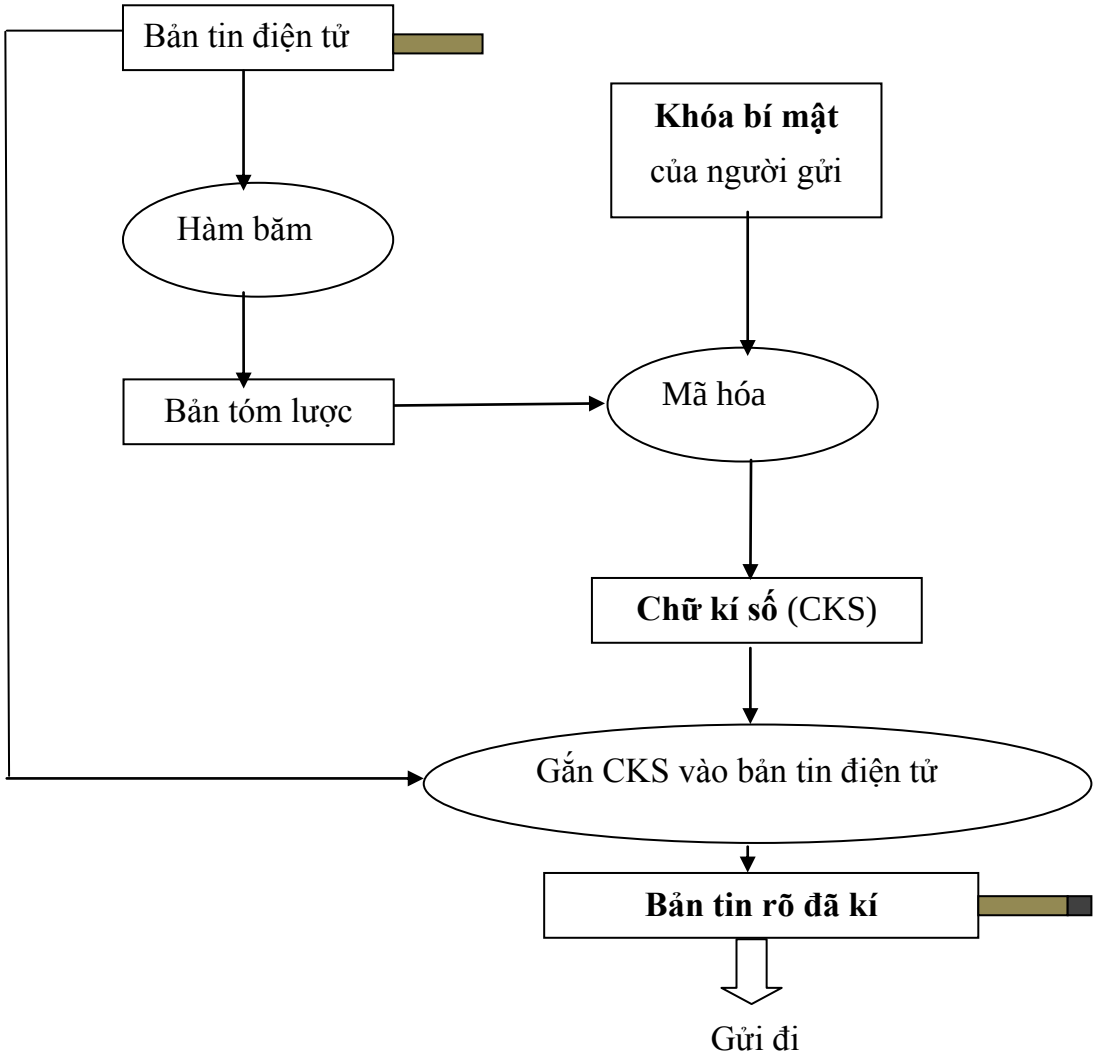
1.2.2.1. Quá trình kí

- Đoạn dữ liệu cần được bảo mật được đưa qua hàm băm (hashing), kết quả của hàm băm là một đoạn bit đảm bảo 2 tính chất:

- Tính duy nhất: mỗi một đoạn dữ liệu khác nhau thì sẽ có một đoạn bit khác nhau, không trùng lặp, có đọ dài không đổi.
- Tính một chiều: Từ đoạn bit đặc trưng này không suy ngược lại được nội dung văn bản.

- Đoạn bit đặc trưng này được mã hóa bằng khóa bí mật của người gửi và được đính kèm vào "văn bản", rồi gửi đến người nhận – **đoạn bit được mã hóa này chính là chữ kí số (digital signature)**

Lược đồ kí được mô tả bằng hình vẽ dưới đây:



Hình 1.5 Lược đồ kí

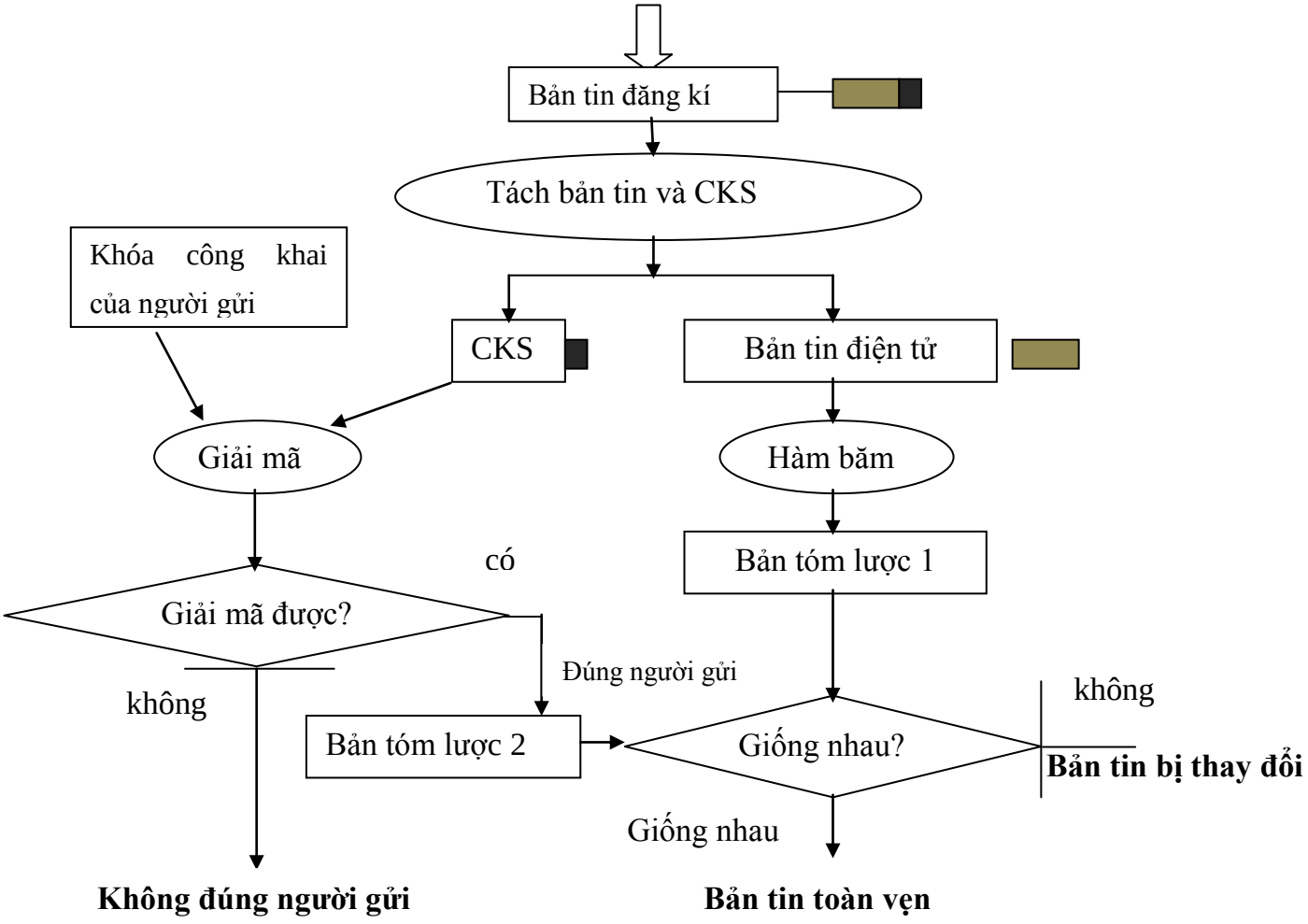
1.2.2.2. Quá trình kiểm tra chữ kí số

Người nhận khi nhận được văn bản có kèm chữ kí số, tiến trình kiêm tra sẽ thực hiện như sau:

- Lấy đoạn dữ liệu gốc, đưa qua hàm băm đã nói ở trên, thu được một đoạn bit là kết quả băm.
- Lấy đoạn bit được mã hóa (chữ kí số), giải mã bằng khóa công khai của người gửi, thu được đoạn bit đăc trưng
- So sánh đoạn bit vừa thu được với đoạn bit thu được trong bước 1, nếu 2 đoạn trùng nhau và tin rằng khóa công khai chắc chắn là do người gửi phát hành thì kết luận:

- Dữ liệu nhận được có tính toàn vẹn (vì kết quả băm là duy nhất, một chiều)
- Dữ liệu nhận được là do chính người gửi gửi đi vì chỉ duy nhất người nhận được xác thực mới có khóa bí mật phù hợp với khóa công khai đã được sử dụng để giải mã. Như vậy tính chống từ chối và tính xác thực được kiểm tra và xác nhận. Lúc này người nhận tin rằng, khóa công khai đó đại diện hợp pháp cho người gửi.

Lược đồ xác thực chữ kí số được mô tả bằng hình vã dưới đây:



Hình 1.6: Lược đồ xác thực

Sau khi kí "văn bản",nếu cần thiết phải cho vào "phong bì" nhằm bảo đảm tính bí mật khi gửi đi, toàn bộ dữ liệu gốc và chữ kí có thể đưa vào mã hóa bằng khóa đối xứng, chìa khóa của mã khóa đối xứng được mã 1 lần bởi khóa công khai của người nhận "văn bản". Khi nhận được, người nhận sẽ sử dụng khóa bí mật của mình đang sở hữu để giải mã và lấy được khóa mã, tiếp tục sử dụng khóa mã này để giải mã được văn bản. Như vậy, tính bí mật của giao dịch sẽ được đảm bảo từ người gửi đến người nhận.

1/. Lược đồ chữ kí số RSA

Lược đồ chữ kí số RSA được xây dựng dựa theo phương pháp mã khóa công cộng RSA. Ở phần tiếp theo này, em sẽ trình bày về lược đồ chữ kí RSA.

Lược đồ chữ kí RSA được mô tả như sau:

Cho n=pq, p và q là các số nguyên tố lớn khác nhau.

Cho $M = C = Z_n$ và định nghĩa

$K = \{(n,p,q,a,b): n = pq, p, q \text{ nguyên tố}, ab \equiv 1(\mod \varphi(n))\}$

$\varphi(n) = (p-1)(q-1)$

Các giá trị n và b công khai, các giá trị p, q, a là bí mật.

Với K = (n,p,q,a,b), ta định nghĩa :

$Sig_k(x) = x^a \mod n$ (a là khóa bí mật của người gửi)

Và $ver_k(x,y) = true \Leftrightarrow x \equiv y^b \mod n$.

$(x,y \in Z_n)$.

2/. Lược đồ chữ kí Elgamal

Phương pháp chữ kí điện tử Elgamal được giới thiệu vào năm 1985. Sau đó viện tiêu chuẩn và công nghệ Quốc gia Hoa Kì đã sửa đổi bổ sung phương pháp này thành chuẩn chữ kí điện tử DSS (Digital Sigital Signature Standard). Nó được thiết kế với mục đích dành riêng cho chữ kí số.

Lược đồ chữ kí Elgamal được mô tả như sau:

Cho p là số nguyên tố sao cho bài toán logarit rời rạc trong Z_p là khó và giả sử $\alpha \in Z_p^*$ là phần tử nguyên thủy.

Cho $P = Z_p^*$, $A = Z_p^* \times Z_{p-1}$ và định nghĩa:

$= \{(p,\alpha,a,\beta) : \beta \equiv \alpha^a \pmod p\}$

Các giá trị p, α, β là công khai, còn a là bí mật.

Với K = (p, α, a, β) và một số ngẫu nhiên bí mật $k \in Z^*_{p-1}$, ta định nghĩa chữ kí số: $sig_k(x,k) = (\gamma,\delta)$←→

Trong đó: $\gamma = \alpha^k \mod p$

Và $\delta = (x - a\gamma) \cdot k^{-1} \mod(p-1)$

Nếu chữ kí được thiết lập đúng thì xác minh sẽ thành công vì :

$\beta^{\gamma} \gamma^{\delta} \equiv \alpha^{a\gamma} a^{k\delta} \pmod{p} \equiv \alpha^{x} \pmod{p}$.

Ở đây ta dùng hệ thức:

$a\gamma + k\delta \equiv x \pmod{p-1}$.

Người dùng tính chữ kí bằng cách dùng cả giá trị mật (là một phần của khóa) lẫn số ngẫu nhiên mật k (dùng để kí lên bức điện x). Việc xác minh có thể thực hiện duy nhất bằng thông tin công khai.

Ta xét một ví dụ sau:

Giả sử: Cho p = 467, α = 2, a = 127 khi đó:

$$\beta = \alpha^{a} \bmod p$$
$$= 2^{127} \bmod 467$$
$$= 132.$$

Nếu người gửi muốn kí lên bức điện x = 100 và chọn số ngẫu nhiên k = 213

(chú ý là UCLN(213,466)=1 và $213^{-1} \bmod 466 = 431$). Khi đó:

$\gamma = 2^{213} \bmod 467 = 29$

và: $\delta = (100 - 127 \cdot 29).431 \bmod 466 = 51$

Bất kì ai cũng có thể xác minh chữ kí này bằng cách kiểm tra:

$132^{29} 29^{51} \equiv 189 \pmod{467}$

Và: $2^{100} \equiv 189 \pmod{467}$

Vì thế chữ kí hợp lệ.

Kết chương

Trong chương này em đã tập trung giới thiệu về mật mã học, cơ sở hạ tầng khóa công khai. Với mục đích sử dụng cho việc xác thực hộ chiếu điện tử nên em đã đặc biệt tập trung giới thiệu về hàm băm và chữ kí số. Trong đó em đi sâu vào hệ mã hóa công khai RSA và chữ kí sử dụng thuật toán RSA để ứng dụng bảo vệ thông tin trong con chip của hộ chiếu điện tử. Chương tiếp theo em đi vào trình bày những quy định của ICAO về hộ chiếu điện tử và cách thức lưu trữ dữ liệu trong hộ chiếu điện tử. Đây là một phần rất quan trọng, phải hiểu rõ về hộ chiếu điện tử và con chip của nó để xác định được cách thức bảo vệ hiệu quả nhất.

Chương 2:

CÁCH THỨC LƯU TRỮ VÀ XỬ LÝ THÔNG TIN TRONG CON CHIP ĐIỆN TỬ

2.1. HỘ CHIẾU ĐIỆN TỬ

2.1.1. Hộ chiếu điện tử là gì?

Hộ chiếu là một loại giấy tờ tùy thân xác nhận công dân mang quốc tịch của một quốc gia. Thông thường, hộ chiếu chứa các thông tincow bản như họ tên, ngày sinh, quê quán, quốc tịch, ảnh khuôn mặt, các thông tin về cơ quan cấp hộ chiếu, ngày cấp, thời hạn có giá trị…

Với sự ra đời của chip khổng tiếp xúc sử dụng công nghệ nhận dạng tần số radio RFID (Radio frequency identification), rõ rang những thông tin cá nhân thể hiện trong một hộ chiếu của công dân hoàn toàn có thể được lưu trữ trên chip không tiếp xúc. Việc lưu trữ những thông tin cá nhân của hộ chiếu trong chip không tiếp xúc cho phép nâng cao hiệu quả của quy trình cấp phát, kiểm duyệt hộ chiếu thông qua các hệ thống xác thực tự động. Các tiếp cận này cho phép xây dựng và phát triển mô hình hộ chiếu mới: "Hộ chiếu điện tử"(HCDT).

Hộ chiếu điện tử là hộ chiếu tích hợp chip điện tử ICC (Integrated Cỉcuit Chip) có chức năng mã hóa và lưu trữ thông tin cá nhân người dùng. Thông tin cá nhân người dùng này phải được bảo vệ chống truy nhập trái phép và phải được xác thực tính chính xác, duy nhất của hộ chiếu. Một trong những công cụ bảo vệ dữ liệu mà hiện nay trên thé giới sử dụng đó là phương pháp mã hóa dữ liệu. Chữ kí số được sử dụng để kí vào các dữ liệu cơ bản và chúng được lưu trữ trong chip.

Trong hộ chiếu điện tử lưu trữ những thông tin cá nhân trong đó có cả những cơ sở dữ liệu sinh trắc học của người mang hộ chiếu. Vì lí do này mà hộ chiếu điện tử còn có tên gọi khác là hộ chiếu sinh trắc học (biometric passport).

Hiện nay yêu cầu về tiêu chuẩn cho hộ chiếu điện tử đã được cung cấp bởi tổ chức hang không dân dụng quốc tế ICAO (International Civil Aviation Organization). Và các yêu cầu này sẽ đáp ứng được an ninh tại cửa khẩu, kiểm tra tại biên giới các nước. Hộ chiếu điện tử tích hợp 3 công nghệ:

- Nhận dạng tần số Radio (RFID)
- Sinh trắc (vân tay, mống mắt)
- Cơ sở hạ tầng khóa công khai PKI (Public key infrastructure).

Trong khi nhận dạng tần số RFID được sử dụng cho các lí do thực tế trong công việc giao tiếp vật lí với các hệ thống kiểm tra, thì việc nhận dạng thông tin sinh trắc và cơ sở hạ tầng khóa công khai PKI được coi là có khả năng giảm thiểu gian lận và tăng cường an ninh trên toàn thế giới trong kĩ thuật nhận dạng số. Do vậy yêu cầu cấp thiết đặt ra cho mỗi nước xây dựng hộ chiếu điện tử là phải xây dựng được một hạ tầng cơ sở khóa công khai quốc gia.

2.1.2. Sự cần thiết phải triển khai hộ chiếu điện tử

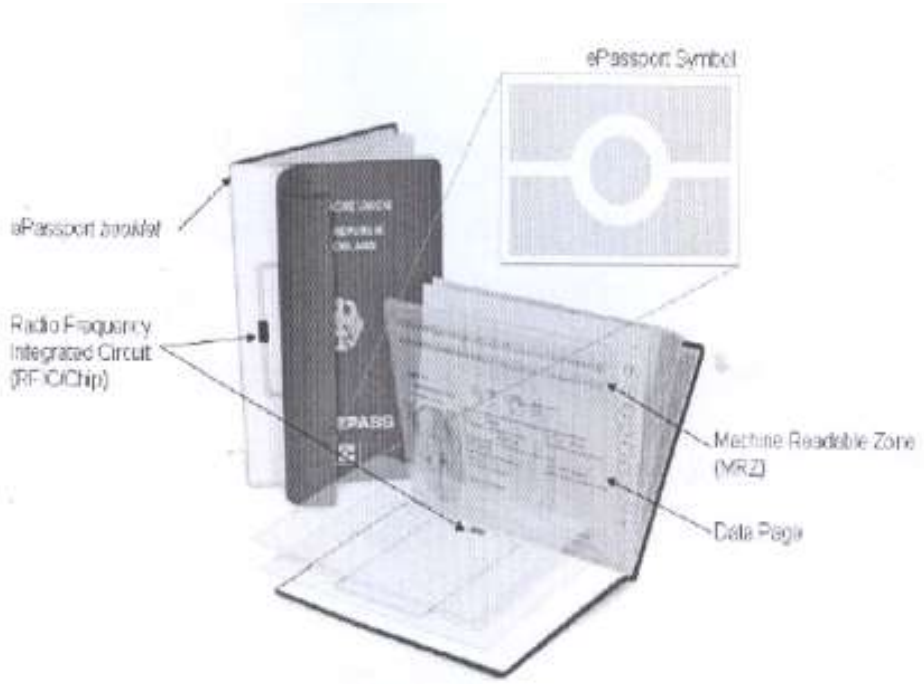
- Việc lưu trữ trong trang nhân thân như hiện nay đã đạt tới mức giới hạn. Trong khi đó, để lưu trữ các đặc điểm sinh trắc học và các thông tin liên quan đòi hỏi khả năng lưu trữ lớn. ICAO đã đưa ra cách lưu trữ chuẩn là sử dụng chip không tiếp xúc (Contactless IC) theo chuẩn ISO/IEC 14443. Đầu đọc có thể đọc dữ liệu trong chip trong khoảng cách < 10cm, không cần phải tiếp xúc trực tiếp với chip. Chip có thể được gắn trong trang nhân thân, trang bìa, hoặc một trang dành riêng trong quyển hộ chiếu.

- Để chống làm giả hoặc sửa đổi thông tin bất hợp pháp, dữ liệu lưu trong chip được bảo vệ bằng chữ kí điện tử sử dụng phương pháp mã hóa khóa công khai – PKI với các thuật toán chuẩn được đưa ra bởi ICAO. Kỹ thuật mã hóa này đã được sử dụng trong một số lĩnh vực yêu cầu độ tin cậy cao như giao dịch ngân hàng, thanh toán trực tuyến…

Ở Việt Nam, tuy lượng hộ chiếu Việt Nam bị thay đổi bất hợp pháp hoặc làm giả bị phát hiện không nhiều. Nguyên nhân co thể là nền kinh tế của ta chưa phát triển cao nên lượng người nhập cư bất hợp pháp còn ít. Tuy nhiên theo chương trình của khối APEC (Việt Nam là thành viên) dự kiến đến năm 2008, toàn khối sẽ hoàn tất lộ trình áp dụng hộ chiếu điện tử. Đồng thời trong tình hình an ninh thế giới đang diễn ra phức tạp, việc duy trì thế mạnh ổn định an ninh chính trị trong nước là sự cần thiết. Ngoài ra, khi các nước đã áp dụng hộ chiếu điện tử, nếu công dân Việt Nam mang hộ chiếu thông thường như hiện nay khi nhập cảnh các nước có nền kinh tế phát triển sẽ bị xem xét, kiểm tra cẩn thận, thậm chí còn bị gây khó dễ. Vì vậy việc nghiên cứu ứng dụng và triển khai hộ chiếu điện tử là 1 vấn đề rất cấp thiết đối với Việt Nam ta.

2.2. TIÊU CHUẨN CỦA ICAO VỀ HỘ CHIẾU ĐIỆN TỬ

2.2.1. Cấu trúc và tổ chức hộ chiếu điện tử



Hình 2.1 Các thành phần của hộ chiếu điện tử

Hộ chiếu điện tử được tổ chức dựa trên cấu trúc của hộ chiếu thông thường, được chia thành hai thành phần: phần tài liệu vật lí – booklet (quyển hộ chiếu) và phần vi mạch tích hợp RFIC (thể hiện dưới dạng chip không tiếp xúc).

Phần tài liệu vật lí – booklet (quyển hộ chiếu):

Booklet gần tương tự như hộ chiếu truyền thống, nó chỉ khác ở chỗ có thêm biểu tượng HCĐT ở trang bìa và dòng ICAO (MRZ – vùng đọc được bằng máy đọc hộ chiếu) ở cuối trang dữ liệu.

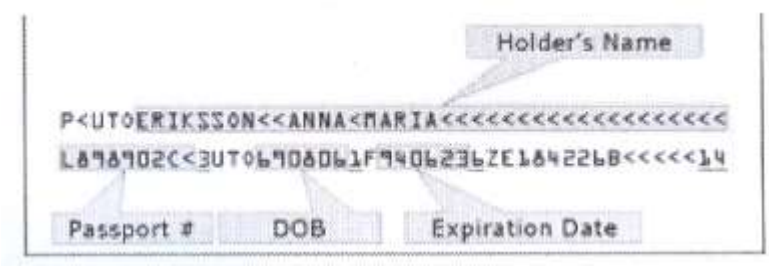
Hình 2.2 Biểu tượng hộ chiếu điện tử

Biểu tượng hộ chiếu điện tử phải được in ở phía ngoài của booklet.

MRZ được thiết kế để đọc bằng máy đọc quang học và có 2 dòng liên tục phía dưới của trang dữ liệu. Mỗi dòng này đều phải có 44 kí tự và được sắp xếp theo phông OCR-B in hoa gồm bốn thông tin quan trọng:

- Tên người mang hộ chiếu: Xuất hiện dòng trên từ kí tự thứ 6 đến kí tự thứ 44.
- Số hộ chiếu: Được xác định bởi 9 kí tự đầu tiên của dòng thứ 2.
- Ngày sinh của người mang hộ chiếu: Xác định từ kí tự 14 đến 19 của dòng 2 theo định dạng: YYMMDD.
- Ngày hết hạn: Được xác định từ kí tự 22 đến 29 của dòng 2.

Ngoài ra, 3 trường số còn có 1 kí tự kiểm tra đứng ngay sau giá trị của trường tương ứng.



Hình 2.3 Mô tả MRZ

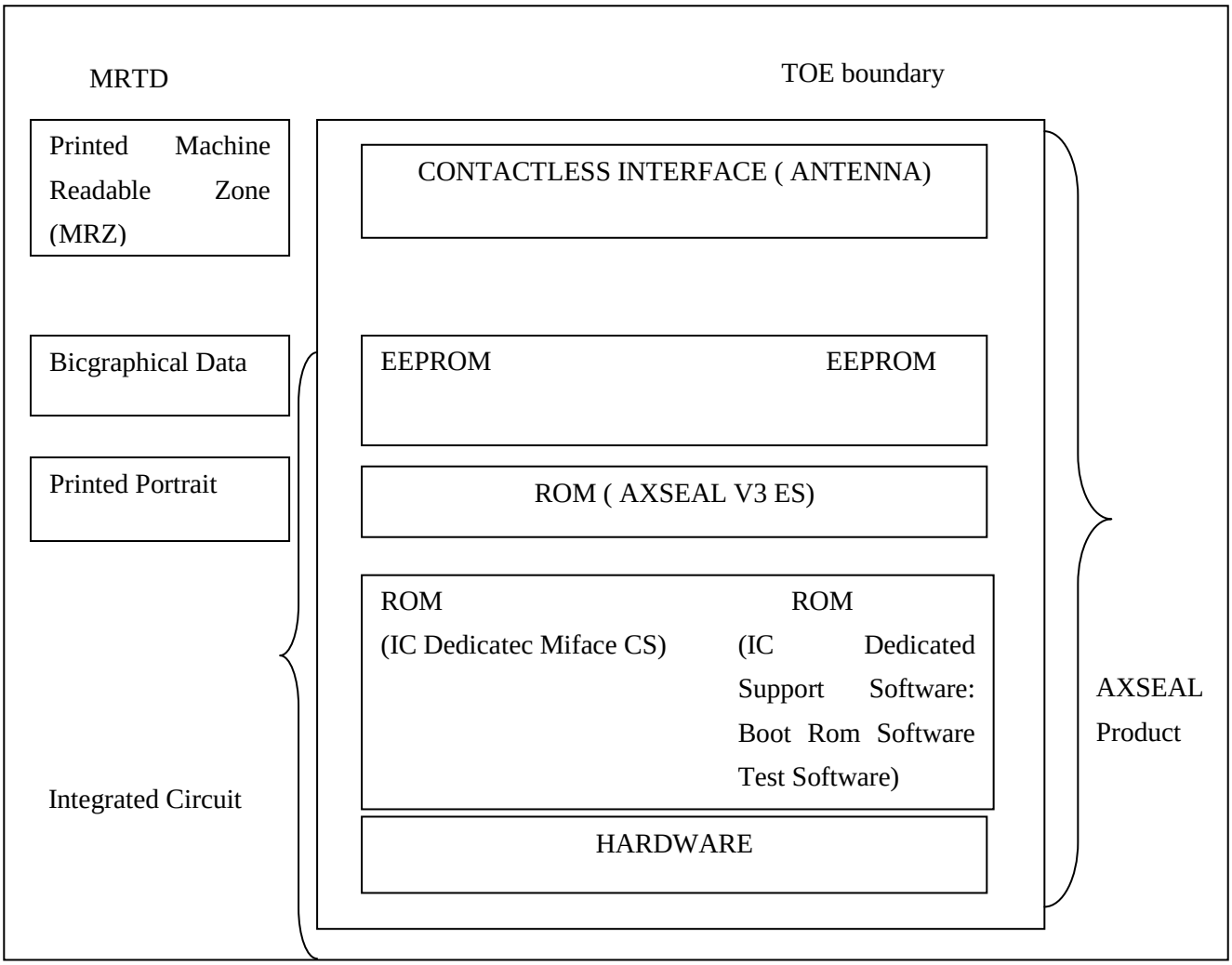
Phần vi mạch tích hợp tần số radio (RFIC):

Chip được đưa vào HCĐT phải tuân theo chuẩn ISO/IEC 14443,trong đó chỉ ra khoảng cách đọc được chính xác trong khoảng 10cm.

Mạch RFIC gồm có chip và một anten vòng không những dùng để kết nối mà còn dùng để nhận biết tín hiệu từ đầu đọc. Đây là yếu tố quyết định HCĐT không có nguồn điện trong. Năng lượng hoạt động cho chip thu nhận qua anten.

Mạch RFIC có thể được đưa vào một trong các vị trí khác nhau trong booklet, thông thường nằm ở trang bìa hoặc trang dữ liệu và cần đảm bảo rằng chip không bị hư hại và tách rời khỏi booklet, đồng thời cũng không thể truy cập hoặc gỡ bỏ.

Cấu trúc chíp không tiếp xúc



Hình 2.4: Cấu trúc chip không tiếp xúc

2.2.2. Cấu trúc dữ liệu của chip ICC

Cấu trúc dữ liệu lưu trữ trong chip của hộ chiếu được in ra làm 2 phần:

1). User Files

Đây là phần dành cho việc phát triển sau này. Phần User Files có thể ghi được và nó cho phép có thể gắn visa điệ tử . . .

2). Cấu trúc dữ liệu logic LDS (Logical Data Structure)

Mục đích của việc chuẩn hóa các thành phần dữ liệu trong hộ chiếu điện tử để có được sự thống nhất trên phạm vi toàn cầu. Tổ chức hàng không dân dụng quốc tế (ICAO) khuyến nghị cấu trúc các thành phần dữ liệu trong HCĐT và phân nhóm logic các thành phần dữ liệu này. Ngoài những thành phần bắt buộc phải có trong HCĐT còn có các thành phần dữ liệu tùy chọn.

Phần LDS chỉ cho phép truy cập dữ liệu, nó bao gồm các khóa mật mã, dùng để hỗ trợ cho các cớ chế kiểm soát truy cập cơ bản BAC (Basic Access Cotrol) và xác thực chủ động AA (Active Authentication). LDS có trường EF-COM lưu trữ thông tin chung của chính LDS như version, danh sách các datagroup, chứa các thông tin của người dùng và các dữ liệu sinh trắc.

Một số yêu cầu đối việc tổ chức dữ liệu logic

- Phải đảm bảo hiệu quả và các điều kiện thuận lợi cho người sở hữu HCĐT hợp pháp;
- Phải đảm bảo sự bảo vệ đối với các thông tin đã lưu trong chip;
- Cho phép tương tác phạm vi toàn cầu đối với dữ liệu mở rộng dựa trên cấu trúc dữ liệu của HCĐT;
- Định vị các thông tin tùy chọn mở rộng theo nhu cầu của tổ chức hoặc chính phủ các quốc gia phát triển hộ chiếu;
- Cung cấp khả năng mở rộng dung lượng lưu trữ theo nhu cầu của người dùng và sự phát triển của công nghệ;
- Hỗ trợ số lượng lớn các lựa chọn bảo vệ dữ liệu;
- Hỗ trợ các tổ chức và chính phủ cập nhật thông tin vào HC ĐT;
- Tận dụng các chuẩn quốc tế hiện có đồng thời mở rộng tối đa khi có các chuẩn sinh trắc học nổi lên.

Để đảm bảo tính tương tác toàn cầu, ICAO quy định cấu trúc dữ liệu trong các chip điện tử phải tuân thủ theo nguyên tác dưới đây:

Nhóm dữ liệu	Bắt buộc (M) / Tùy chọn (O)	Thành phần dữ liệu	
Thông tin chi tiết lưu trong vùng dữ liệu đọc được bằng máy			
1	M	Dữ liệu vùng đọc được bằng máy (dòng ICAO)	
Thông tin xác thực hỗ trợ bởi máy – Các đặc điểm xác định được mã hóa			
2	M	Đặc điểm trao đổi công khai	Ảnh mặt
3	O	Thông tin bổ sung	Ảnh vân tay
4	O	Thông tin bổ sung	Ảnh tròng mắt
Thông tin xác thực hỗ trợ bởi máy – Các đặc điểm xác định thể hiện rõ			
5	O	Ảnh mặt rõ	
6	O	Dữ trữ dùng trong tương lai	
7	O	Ảnh chữ ký rõ hoặc đặc điểm đánh dấu thường dùng	
Xác định đặc điểm bảo mật hỗ trợ máy – Các thông tin bảo mật được mã hóa			
8	O	Đặc điểm dữ liệu	
9	O	Đặc điểm cấu trúc	
10	O	Đặc điểm thay thế	
Các thông tin bổ sung về các nhân			
11	O	Các chi tiết dữ liệu bổ sung cho thông tin về cá nhân	
Các thông tin bổ sung về tài liệu			
12	O	Các chi tiết dữ liệu bổ sung cho thông tin về tài liệu	
Các thông tin tùy chọn			
13	O	Các chi tiết tùy ý do cơ quan cấp phát quy định	
Dự trữ dùng trong tương lai			
14	O	Dự trữ dùng trong tương lai	
15	O	Thông tin khóa công khai xác thực chủ động	
Những điều cần chú ý			
16	O	Chi tiết dữ liệu về những người cần chú ý	

Như vậy là trong quy định đối với cấu trúc dữ liệu logic, chỉ có phần dữ liệu đọc được bằng máy (dòng ICAO) được ghi trong nhóm dữ liệu thứ nhất và ảnh mặt (được ghi trong nhóm dữ liệu 2) là bắt buộc, còn các thông tin khác đều là tùy chọn.
Ngoài ra trong một HCĐT theo chuẩn còn cần thiết phải có thông tin bảo mật để xác định tính toàn vẹn của dữ liệu được ghi trong chip. Thông tin này được chứa trong nhóm dữ liệu 1. Thông tin bảo mật bao gồm giá trị băm của các nhóm dữ liệu được sử dụng.

Nếu như ảnh hiện thị rõ trong trang nhân thân là tương đối khác biệt (hoặc thực chất là một ảnh khác – trường hợp có hai ảnh mặt) so với ảnh lưu trong nhóm dữ liệu 2, thì phải lưu trữ ảnh đó ở nhóm dữ liệu 5.

Nếu cơ quan cấp phát thực hiện lưu trữ thông tin tùy chọn là vân tay và cho phép đọc công khai thì ít nhất phải lưu trữ một ảnh tròng mắt tại nhóm dữ liệu 3.

Nếu cơ quan cấp phát thực hiện lưu trữ thông tin tùy chọn là tròng mắt và cho phép đọc công khai thì ít nhất phải lưu trữ một ảnh tròng mắt tại nhóm dữ liệu 4.

Trong con chip điện tử, ngoài các thông tin dữ liệu còn có các thông tin bảo mật, được cơ quan phát hành số hóa, lưu trữ và chỉ cung cấp cho các cơ quan chức năng có thẩm quyền để phục vụ kiểm tra, kiểm soát và xác thực về người mang hộ chiếu.

2.2.3. Lưu trữ vật lý

Dữ liệu lưu trữ trong RFIC theo các tệp ứng với từng nhóm dữ liệu, các tệp này là các tệp cơ bản có tên bắt đầu bằng ‘ EF’. Ngoài ra còn có một số tệp đặc biệt như DF1 là tệp chứa thông tin khai báo, EF.SO_D (SO_D: security object) là tệp chứa thông tin phục vụ quá trình xác thực bị động - Passive Authentication. Trong mỗi tệp (nhóm dữ liệu), các trường thông tin phân tách nhau bởi các thẻ Tag đánh dấu bắt đầu và kết thúc giá trị của trường thông tin.

MF

--------DF – LDS REQUIRED

--------K_{ENC} OPTIONAL

--------K_{MAC} OPTIONAL

--------KPr_{AA} OPTIONAL

--------EF – COM REQUIRED

--------EF - SO_D REQUIRED

--------EF – Datagroup_1 (MRZ) REQUIRED

--------EF – Datagroup_2 (Encoded Face) REQUIRED

--------EF – Datagroup_n OPTIONAL

HÌnh 2.5: Tổ chức vật lý thông tin trong hộ chiếu điện tử

Bốn nhóm thành phần dữ liệu bắt buộc:

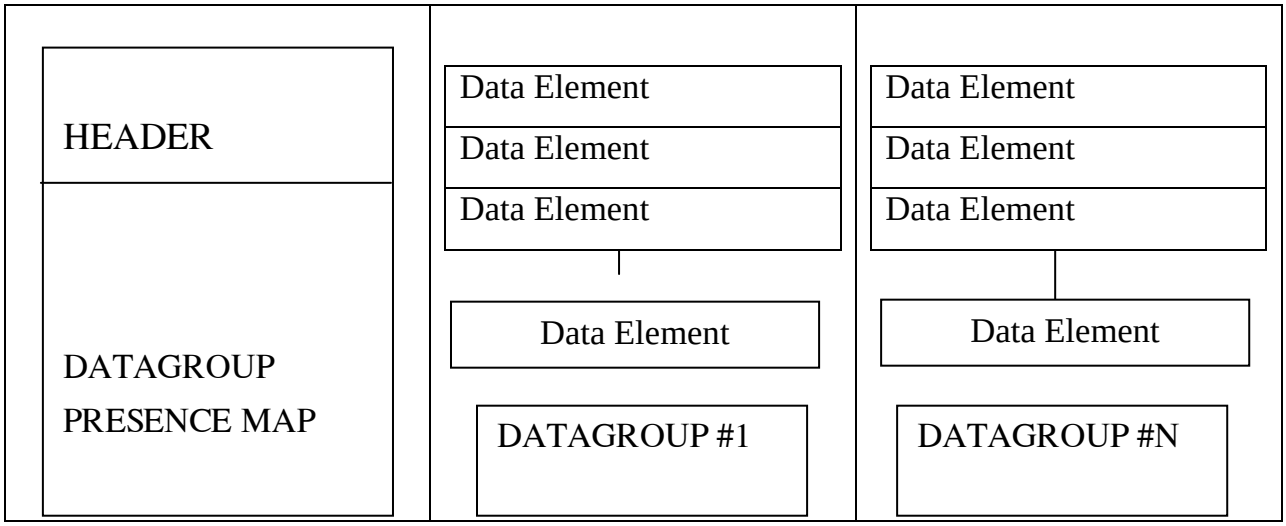
- Phần thông tin MRZ (Machine Readable Zone) tương ứng với nhóm dữ liệu DH1.
- Ảnh khuôn mặt của người mang hộ chiếu.
- EF.COM lưu trữ thông tin chung của chính LDS như: version, List of DataGroup . . .
- $EF.SO_D$ chứa thông tin phục vụ xác thực và toàn vẹn.

Khi thẻ không tiếp xúc đi qua vùng giao tiếp của đầu đọc, quá trình đọc diễn ra theo chuẩn ISO 14443.

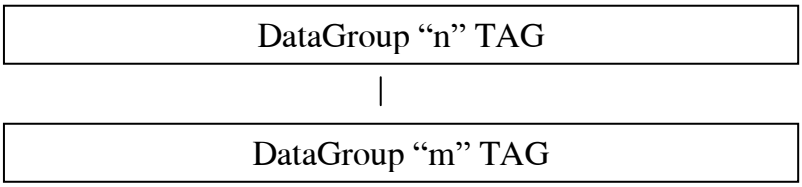
Để kiểm tra sự toàn vẹn của các nhóm thông tin, một số thông tin chữ ký được đưa thêm vào và ghi trong tệp cơ sở có tên $EF.SO_D$.

Cách thức lưu trữ các nhóm và thành phần dữ liệu theo mô hình thứ tự ngẫu nhiên. Cách thức lưu trữ này phù hợp với kỹ thuật mở rộng dung lượng tùy chọn cho phép duy trì các thành phần dữ liệu ngay cả khi nó được ghi vượt quá. Các thành phần dữ liệu có độ dài không xác định được mã theo cặp giá trị length/ value theo hệ thập lục phân.

Để định vị và giải mã các nhóm và thành phần dữ liệu lưu trong các nhóm đã ghi bởi cơ quan cấp hộ chiếu, đầu đọc dựa vào các phần thông tin Header trong tệp EF.COM (hình 2.5). Việc xác định nhóm dữ liệu nào có trong chip căn cứ vào thông tin Data Presence Map chứa trong tệp EF.COM thông qua các thẻ TAG, mỗi thẻ chỉ định lưu trữ nhóm thông tin tương ứng (hình 2.6).



Hình 2.6 Thông tin định vị nhóm dữ liệu lưu trong chip

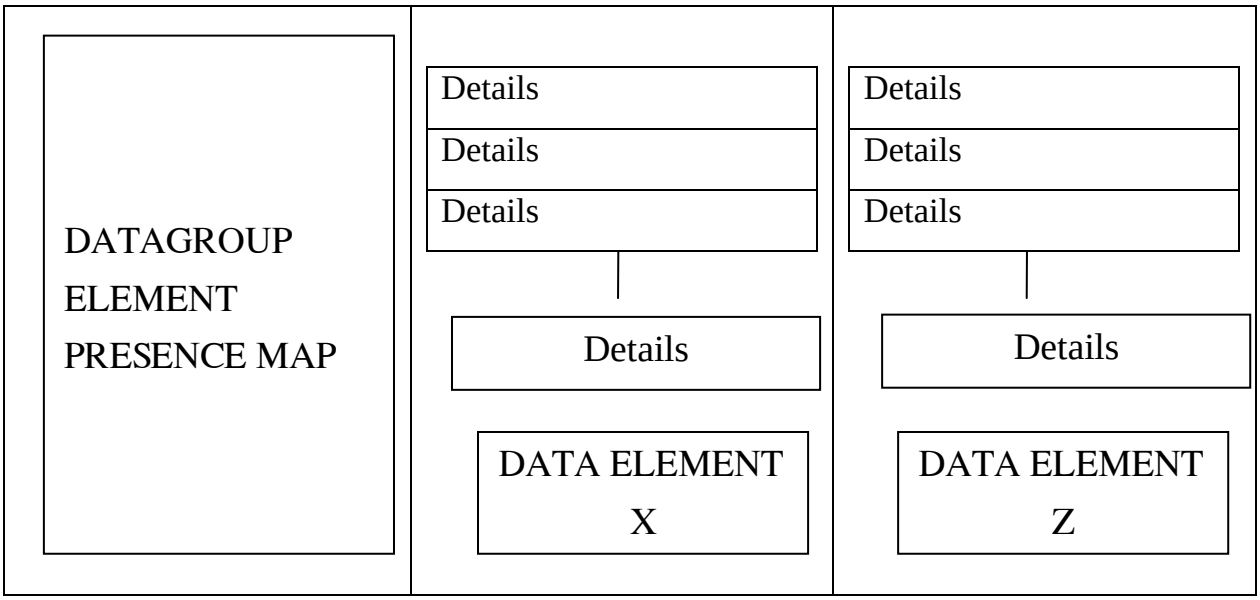


Presence of TAG = Data Group Present

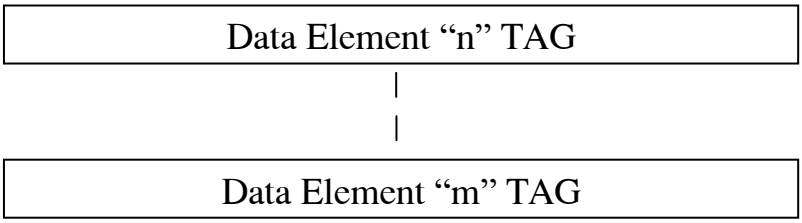
Absence of TAG = Data Group Not Present

Hình 2.7 Thông tin chỉ thị sự tồn tại của nhóm dữ liệu trong chip

Với các thành phần dữ liệu trong mỗi nhóm (trường thông tin), đầu đọc nhận diện sự tồn tại của chúng thông qua Data Element Presence Maps, và định vị dữ liệu thông qua các TAG.



Hình 2.8 Thông tin chỉ thị sự tồn tại thành phần dữ liệu trong một nhóm



Presence of TAG = Data Element Present

Absence of TAG = Data Element Not Present

Hình 2.9: Thông tin xác định vị trí thành phần dữ liệu trong nhóm

Kết chương

Trong phạm vi chương này em tập trung giới thiệu về hộ chiếu điện tử, cấu trúc vật lý của con chip và việc tổ chức dữ liệu điện tử trong chip RFID theo quy định của CIAO. Ở chương này em đặc biệt đi sâu về cấu trúc dữ liệu logic cùa con chip trong hộ chiếu điện tử để xác định cách thức bảo vệ dữ liệu của con chip. Chương tiếp theo em sẽ trình bày các cơ chế bào mật hộ chiếu do CIAO đưa ra. Trên cơ sở phân tích những ưu điểm, nhược điểm của cơ chế, em sẽ đề xuất mô hình bảo mật hộ chiếu điện tử trên cơ sở những khuyến cáo của CIAO.

Chương 3:

ỨNG DỤNG CỦA CHỮ KÝ SỐ VÀO VIỆC KIỂM SOÁT, XÁC THỰC VÀ BẢO VỆ THÔNG TIN TRONG HỘ CHIẾU ĐIỆN TỬ

3.1. MỤC ĐÍCH, YÊU CẦU CỦA VIỆC BẢO MẬT HỘ CHIẾU ĐIỆN TỬ

Vấn đề bảo mật HCĐT trong các quy trình cấp phát, kiểm duyệt luôn là 1 trong những vấn đề tối quan trọng đối với an ninh quốc gia. Vấn đề này cần phải thỏa mãn được 6 yêu cấu sau đây:

- *Tính chân thực*

Cơ quan cấp hộ chiếu phải ghi đúng thông tin của người được cấp hộ chiếu, không có sự nhầm lẫn trong quá trình ghi thông tin khi cấp hộ chiếu. Đây là điều đương nhiên bắt buộc phải có trong khuôn khổ luận van này, giả thiết mục tiêu này luôn được đảm bảo

- *Tính không thể nhân bản*

  Mục tiêu này phải đảm bảo không thể tạo ra bản sao chính xác của RFIC

- *Tính nguyên vẹn và xác thực*

Cần chứng thực tất cả thông tin lưu trên trang dữ liệu và trên RFIC do cơ quan hộ chiếu tạo ra(*xác thực*). Hơn nữa cần chứng thực thông tin đó k bị thay đổi từ lúc được lưu(*nguyên vẹn*).

- *Tính liên kết người - hộ chiếu*

Cần phải chứng minh rằng HCĐT thuộc về người mang nó hay nói một cách khác các thông tin trong hộ chiếu mô tả con người sở hữu hộ chiếu.

- *Tính liên kết hộ chiếu – chip*

  Cần phải khẳng định booklet khớp với mạch RFIC nhúng trong nó.

- *Kiểm soát truy cập*

Đảm bảo việc truy cập thông tin lưu trong chip phải được sự đồng ý của người sở hữu nó, hạn chế truy cập đến các thông tin sinh trắc học nhạy cảm và tránh mất mát thông tin cá nhân.

3.2. CƠ CHẾ BẢO MẬT HỘ CHIẾU ĐIỆN TỬ DO ICAO ĐƯA RA

Tài liệu mô tả về hộ chiếu điện tử của CIAO[*Doc 9303, Ninth Draft: Machine Readable Travel Documents, July 2005*] đề cập đến các cơ chế bảo mất cho hộ chiếu điện tử gồm:

- *Xác thực bị động(Passive Authentication)*

Mục đích là để kiểm tra tính xác thực và toàn vẹn của thông tin lưu trong chip RFID thông qua việc kiểm tra chữ ký của cơ quan cấp hộ chiếu trên các thông tin lưu trong chip.

- *Xác thực chủ động (Active Authentication)*

Mục đích để tránh sao chép và thay thế chip trong hộ chiếu điện tử. Bằng cách trao đổi khóa xác thực quan hệ giữa hệ thống kiểm soát và con chip.

- *Kiểm soát truy cập cơ bản(Basic Access Control-BAC)*

Mục đích để chống đọc lén thông tin trong chip và nghe trộm thông tin truyền giữa chip RFID và đầu đọc

Nếu không có cơ chế BAC thì một dâu đọc bất kỳ theo chuẩn ISO/IEC 14443 đều có thể đọc nội dung thông tin lưu trong chip RFID. Như vậy sẽ không đảm bảo yêu cầu bảo vệ thông tin cá nhân. Hơn thế nữa, BAC còn giúp mã hóa dữ liệu truyền giữa đầu đọc và chip RFID để tránh nghe lén thông tin trên đường truyền

- *Điều khiển truy cập mở rộng*(*Extended Access Control-EAC*)

Mục đích của EAC để tăng cường bảo vệ các thông tin sinh trắc học nhạy cảm (vân tay, mống mắt) đồng thời khắc phục hạn chế của quá trình xác thực chủ động. Cơ chế này bao gồm hai quá trình:

- Xác thực chip (Chip Authentication)
- Xác thực đầu đọc (Terminal Authentication)

Tuy nhiên CIAO chỉ đề cập đến cơ chế này dưới dạng mở để các quốc gia, giới khoa học tiếp tục nghiên cứu, bổ sung.

Hơn thế nữa, trong các cơ chế được đề cập ở trên, CIAO khuyến nghị chỉ bắt buộc sử dụng cơ chế xác thực bị động để kiểm tra tính toàn vẹn và xác thực của thông tin. Xác thực chủ động và điều khiển truy cập cơ sở chỉ là các tùy chọn không bắt buộc sử dụng trong quá trình xác thực hộ chiếu.

Dưới đây là bảng tổng kết các phương thức bảo mật thông tin trong hộ chiếu điện tử:

PHƯƠNG THỨC BẢO MẬT CƠ BẢN				
Phương thức	CQ cấp phát	CQ kiểm soát	Ưu điểm	Nhược điểm
Xác thực bị động	Bắt buộc	Bắt buộc	Đảm bảo xác thực thông tin trong chip điện tử không bị thay đổi	Không chống được việc sao chép toàn nội dung con chip hoặc thay thế bằng một chip khác. Không có khả năng chống trộm.
CÁC PHƯƠNG THỨC BẢO MẬT NÂNG CAO				
So sánh giữa thông tin trong dòng ICAO và thông tin trong chip điện tử	Khôn sử dụng	Tùy chọn	Đảm bảo thông tin của chip điện tử và dòng ICAO là đồng nhất.	Làm tăng tính phức tạp của hệ thống. Không có khả năng chống sao chép thông tin trong chip và trang nhân than.
Xác thực chủ động	Tùy chọn	Tùy chọn	Có khả năng chống sao chép nội dung thông tin của chip điện tử. Có khả năng chống thay thế chip.	Làm tăng tính phúc tạp của hệ thống. Cần con chip có khả năng xử lý.
Kiểm soát khả năng truy cập cơ bản	Tùy chọn	Tùy chọn	Chống đọc trộm thông tin trong chip. Chống thu tín hiệutrong quá trình truyền tin giữa chip và máy đọc (khi sử dụng kênh truyền có mã hóa).	Không có khả năng chống sao chép và thay thế chip. Làm tăng tính phức tạp của hệ thống. Cần con chip có khả năng xử lý.
Kiểm soát truy cập mở rộng	Tùy chọn	Tùy chọn	Chống truy cập bất hợp pháp các thông tin sinh trắc mở rộng. Chống đọc trộm các thông tin sinh trắc mở rộng.	Đòi hỏi quản lý và cấp phát them khóa. Không có khả năng chống sao chép và thay thế chip. Làm tăng tính phức tạp của hệ thống. Cần con chip có khả năng xử lý.
Mã hóa thông tin	Tùy chọn	Tùy chọn	Bảo mật các thông tin sinh trắc mở rộng. Không yêu cầu chip điện tử phải có khả năng xử lý tính toán.	Cần quản lý khóa giải mã thông tin. Không có khả năng chống sao chép và thay thế chip. Làm tăng tính phức tạp của hệ thống.

3.2.1. Các thuật toán được sử dụng trong hệ thống bảo mật

3.2.1.1. Quy định chung

Tất cả các quốc gia phải sử dụng một thuật toán đồng nhất để sinh khóa (chứng chỉ) bảo mật cấp quốc gia, khóa bảo mật hộ chiếu và ứng dụng trong các đối tượng bảo mật(SO_D), tuy vậy độ dài của mã khóa là khác nhau tương ứng với các cấp độ bảo mật khác nhau.

Các quốc gia phải hỗ trợ tất cả các thuật toán bảo mật tại các cửa khẩu quốc tế để xác thực tính hợp lệ của hộ chiếu do các quốc gia khác phát hành.

Dưới đây là khuyến cáo đối với độ dài mã khóa tương ứng với từng thuật toán và giả định hộ chiếu có thời hạn là 10 năm.

3.2.1.2. RSA

- Khóa mã cấp quốc gia có độ dài tối thiểu là 3072 bit(số nguyên tố Mođulô n).
- Khóa mã cấp hộ chiếu có độ dài tối thiểu 2048 bit.
- Khóa mã đánh cho phương thức xác thực chủ động có độ dài tối thiểu là 1024 bit.

3.2.1.3. DSA

- Khóa mã cấp quốc gia có độ dài tối thiểu là 3072 và 256 bit (tương ứng với cặp số n và q).
- Khóa mã cấp hộ chiếu có độ dài tối thiểu là 2048 và 224 bit.
- Khóa mã dành cho phương thức xác thực chủ động có độ dài tối thiểu là 1024 và 160 bit

3.2.1.4. Đường cong elip DSA (ECDSA)

- Khóa mã cấp quốc gia có độ dài tối thiểu 256 bit.
- Khóa mã cấp hộ chiếu có độ dài tối thiểu 224 bit.
- Khóa mã dành cho phương thức xác thực chủ động có độ dài tối thiểu là 1024 và 160 bit.

3.2.1.5. Các thuật toán băm(SHA-1, SHA-256, SHA-384, SHA-512)

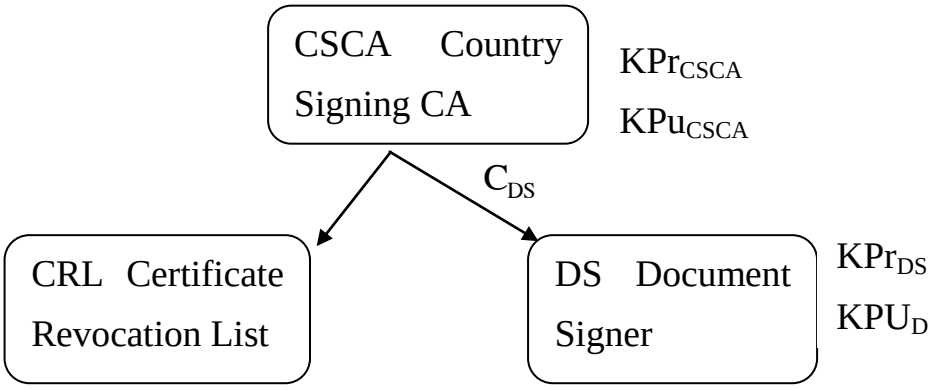
Độ dài khóa mã của thuật toán băm nên lựa chọn cho phù hợp với thuật toán ký tương ứng. Ví dụ:

- SHA-1 cùng với RSA 1024
- SHA-224 cùng với ECDSA 224

3.2.2. Hệ thống cấp phát và quản lý chữ ký số trong hộ chiếu điện tử

3.2.2.1 Danh mục khóa công khai

ICAO tổ chức mô hình danh mục khóa công khai – PKD(Public Key Directory) nhằm lưu trữ tập trung, phân phối chứng chỉ(khóa công khai), danh sách chứng chỉ thu hồi – CRL(Certificate Revocation List) đến các quốc gia thành viên.



Hình 3.1: Danh mục khóa công khai

Với ý tưởng này, mỗi quốc gia có một cơ quan cấp chứng chỉ số quốc gia(ký hiệu là CSCA-Country Signing Certificate Authority), với khóa bí mật là KPr_{CSCA} và khóa công khai Kpu_{CSCA}. Những khóa này được sử dụng để chứng thực cho chứng chỉ của cơ quan cấp hộ chiếu (ký hiệu là C_{DS}). Mô hình tổ chức chứng chỉ như trên hình 2.9. Trong cây phân cấp quản lý khóa, chứng chỉ khóa ở cấp cao nhất được phát hành để xác thực tính hợp lệ của tất cả các khóa mã do một quốc gia phát hành. Chứng chỉ cấp cao nhất này được viết tắt C_{CSDA}. C_{CSDA} được khởi tạo và phát hành bởi Cơ quan phát hành chứng chỉ khóa cấp quốc gia (CSCA).

ICAO khuyến cáo rằng tất cả các cặp khóa do CSCA phát hành (Kpu_{CSCA}, KPr_{CSCA}) đều phải được phát sinh và lưu trữ trong môi trường bảo mật cao nhất.

Tất cả các chứng chỉ khóa cấp quốc gia C_{CSCA} đều phải được cấp phát và vận chuyển bằng đường ngoại giao bảo mật (không cung cấp trên đường truyền).

Mỗi chứng chỉ khóa cấp quốc gia C_{CSCA} sau khi được phát sinh và sử dụng cần phải gửi cho ICAO (để xác thực tính hợp lệ của các chứng chỉ số hộ chiếu C_{DS}).

Thư mục khóa công khai (Public Key Directory - PKD) là nơi tập trung các chứng chỉ của cơ quan cấp hộ chiếu (C_{DS}), ICAO sẽ tập hợp chứng chỉ của quốc gia thành viên và quản lý, cung cấp trực tuyến. Được xây dựng với mục đích chia sẻ các Chứng chỉ hộ chiếu đối với tất cả các quốc gia thành viên, ICAO đã xây dựng và cung cấp dịch vụ thư mục khoa công khai (PKD) cho tất cả các quốc gia thành viên truy cập. Dịch vụ này cho phép

nhận các thông tin về khóa công khai từ tất cả các quốc gia, lưu trữ vào trong một thư mục, và cho phép các thanh viên truy nhập để lấy thông tin về.

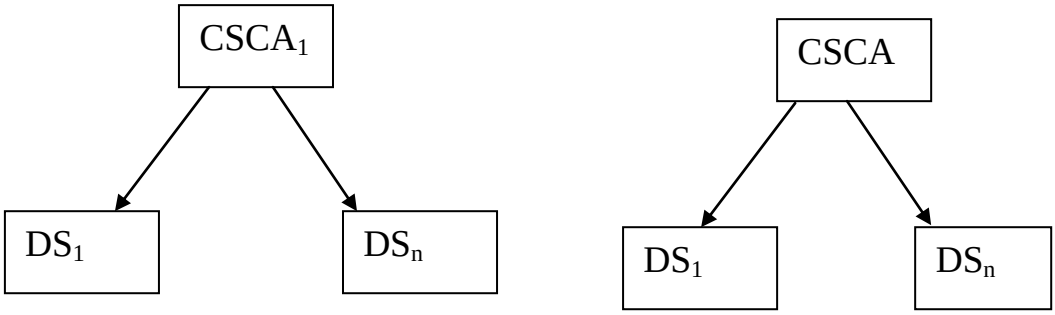
Việc truy cập để cập nhật PKD được giới hạn chỉ trong các quốc gia thành viên ICAO.

Ngoài các quốc gia, thì mọi truy cập khác vào PKD để đọc thông tin là không được phép.

Một phần hết sức quan trọng cần thường xuyên cập nhật với PKD là danh sách những chứng chỉ bị thu hồi (CRL). Do các khóa bí mật của cơ quan cấp hộ chiếu dùng để ký một số lượng lớn các HCĐT và sử dụng trong một khoảng thời gian dài nên nếu sảy ra trường hợp khóa bí mật này bị lộ, không thể hủy giá trị sử dụng của toàn bộ các HCĐT đã được ký bởi khóa này. Các HCĐT đã ký bằng khóa nằm trong CRL vẫn còn nguyên giá trị sử dụng. Khi nói đến giá trị của chữ ký số là muốn nói đến thời điểm cuối cùng của nó trong khoảng thời gian có giá trị. Một khi khóa bí mật của một cơ quan cấp hộ chiếu bị lộ, chính phủ đó phải nhanh chóng cảnh báo cho tất cả các quốc gia khác.

3.2.2.2. Mô hình phân cấp CA phục vụ quá trình xác thực bị động

Tổ chức mô hình CA thành hai cấp, cấp quốc gia và cơ quan trực tiếp cấp hộ chiếu.



Hình 3.2: Mô hình tổ chức phân cấp CA phục vụ quá trình Passive Authentication

CSCA – Country Signing Certifivcate Authority là CA cấp quốc gia, CA này cấp chứng chỉ chứng thực khóa công khai cho các DS – Document Signer. DS là các cơ quan ký hộ chiếu điện tử hay cũng chính là cơ quan cấp hộ chiếu điện tử.

Mô hình tổ chức CA này không có CA cấp cao nhất phạm vi toàn cầu hay CA chứng thực cho các CA cấp quốc gia. Mỗi CSCA trong mô hình đóng vai trò là root CA, nó là CA tự xác thực. Khóa công khai của các CSCA trao đổi cho các CSCA khác theo đường công hàm hoặc tuân theo PKD của ICAO.

DS ký hộ chiếu điện tử mà nó cấp khóa bí mật, khóa công khai tương ứng lưu trong chip dưới dạng 1 chứng chỉ (C_{DS}) do CSCA cấp trên phát hành.

Tại điểm kiểm tra, đầu đọc hộ chiếu điện tử đọc C_{DS}, kiểm tra tính xác thực của nó bằng khóa công khai của CSCA tương ứng. Sau đó đầu đọc thẻ dung khóa công khai trong C_{DS} để xác thực nội dung thông tin lưu trong chip.

Danh sách chứng chỉ thi hồi – CRL: Mô hình PKI sử dụng trong xác thực hộ chiếu điện tử có điểm riêng đặc thù so với mô hình PKI nói chung vì đây là hình thức PKI offline. Do các khóa bí mật của các chính phủ dung để ký một số lượng lơn các HCĐT và sử dụng trong một khoảng thời gian dài nên nếu sảy ra trường hợp khóa bí mật này bị lộ, không thể hủy giá trị sử dụng của toàn bộ các HCĐT được ký bởi khóa này. Giá trị dùng để ký HCĐT ý muốn nói tới thời điểm cuối cùng của nó trong khoảng thời gian có giá trị. Một khi khóa bí mật của một chính phủ bị lộ, quốc gia này phải nhanh chóng cảnh báo cho tất cả các quốc gia khác (truyền song phương trực tiếp) và cập nhật vào ICAO PKD trong vòng 48 giờ.

Trong trường hợp khống khóa nào cần thu hồi thì các quốc gia cũng lên khẳng định lại danh sách thu hồi khóa CRL với các quốc gia khác và ICAO PKD ít nhất là trong vòng 90 ngày.

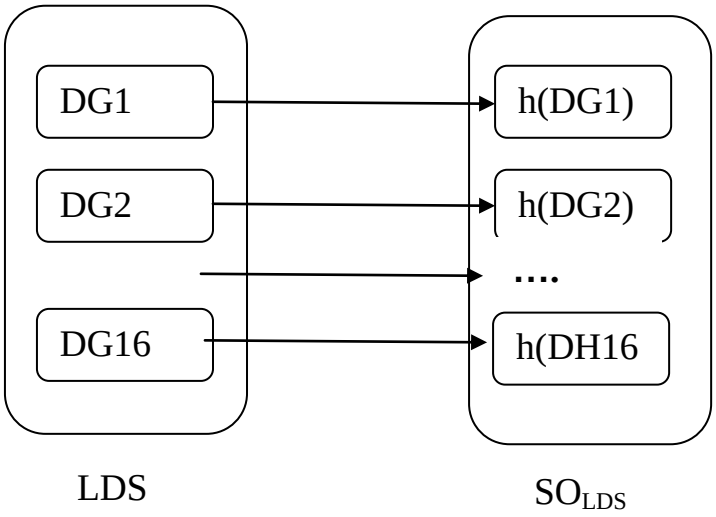
3.2.2.3 Mô hình cấp, xác thực hộ chiếu điện tử

1/. Quá trình cấp phát hộ chiếu điện tử

- **B1**: Đăng ký cấp hộ chiếu theo mẫu do cơ quan cấp phát, quản lý hộ chiếu phát hành. Quá trình này hiện nay đang được làm thủ công, em xin để xuất điện tử hóa quá trình đăng ký cấp hộ chiếu: Đăng ký, đặt lịch đến cơ quan cấp hộ chiếu để lấy thông tin sinh trắc học, nhận hộ chiếu thông qua mạng máy tính.
- **B2**: Kiểm tra nhân than, đây là quá trình nghiệp vụ của cục quản lý xuất nhập cảnh không nằm trong phạm vi luận văn em đề cập tới.
- **B3**: Thu nhập thông tin sinh trắc học. Trong luân văn em đề xuất sử dụng 03 thông tin sinh trắc học gồm ảnh khuôn mặt, ảnh hai vân tay ngón trỏ và ảnh mống mắt.
- **B4**: In hộ chiếu, ghi thông tin vào chip điện tử.
  - Ghi thông tin cơ bản như trên trang hộ chiếu giấy vào DG1 (Đây còn gọi là dòng ICAO).
  - Ghi ảnh khuôn mặt vào DG2.
  - Ghi ảnh hai vân tay vào DG3.

- Ghi ảnh hai hốc mắt vào DG4.
- Ghi SO_D: Tạo giá trị băm các nhóm thông tin theo SHA, tập tất cả các giá trị băm này gọi là SO_{LDS}; ký SO_{LDS} bằng khóa bí mật KPr_{DS} của cơ quan cấp hộ chiếu ta được chữ ký trên SO_{LDS} ký hiệu là SO_D.Signature. Cấu trúc của SO_D là (SO_{LDS}, SO_D.Signature,SO_D.cert), trong đó SO_D.cert là chứng chỉ C_{DS} – chứng chỉ số của cơ quan cấp hộ chiếu. Phần thông tin này phục vụ quá trình xác thực bị động .

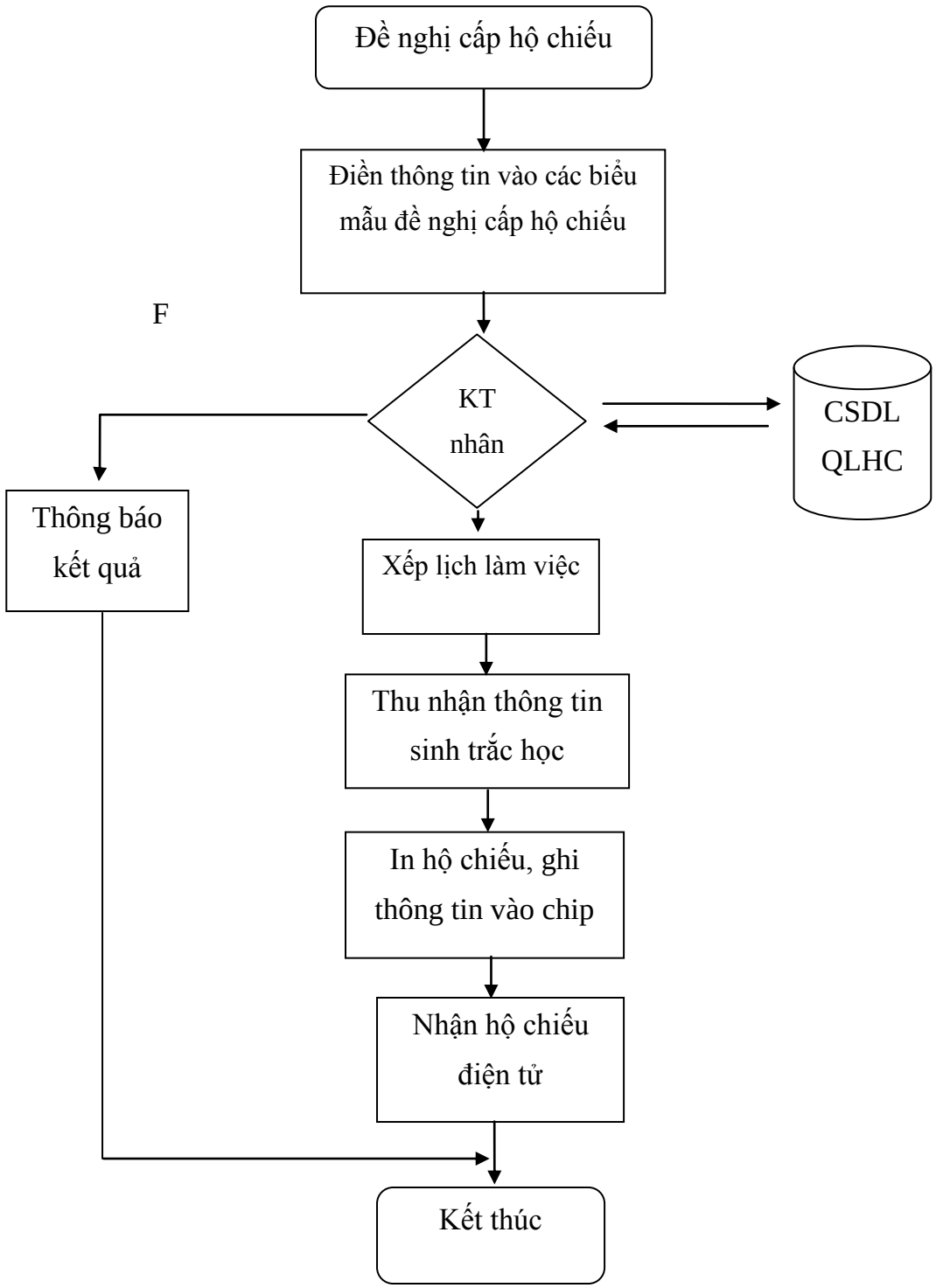
SO_D chứa C_{DS} nhằm mục đích tạo sự thuận lợi cho sự phê chuẩn sau này của cơ quan kiểm tra hộ chiếu đồng thời cũng hạn chế số lượng chứng chỉ. Thay vì cơ quan hộ chiếu phải lưu và quản lý tất cả các C_{DS} thì họ chỉ phải lưu và quản lý chứng chỉ của một quốc gia (C_{CSCA}) và danh sách CRL. C_{DS} được chứng thực thông qua C_{CSCA} này



{ | SO_{LDS}| } KPr_{DS}→ SO_D.Signature

C_{DS}→ SO_D.Cert

Hình 3.3: Mô tả quá trình tạo đối tượng SO_D

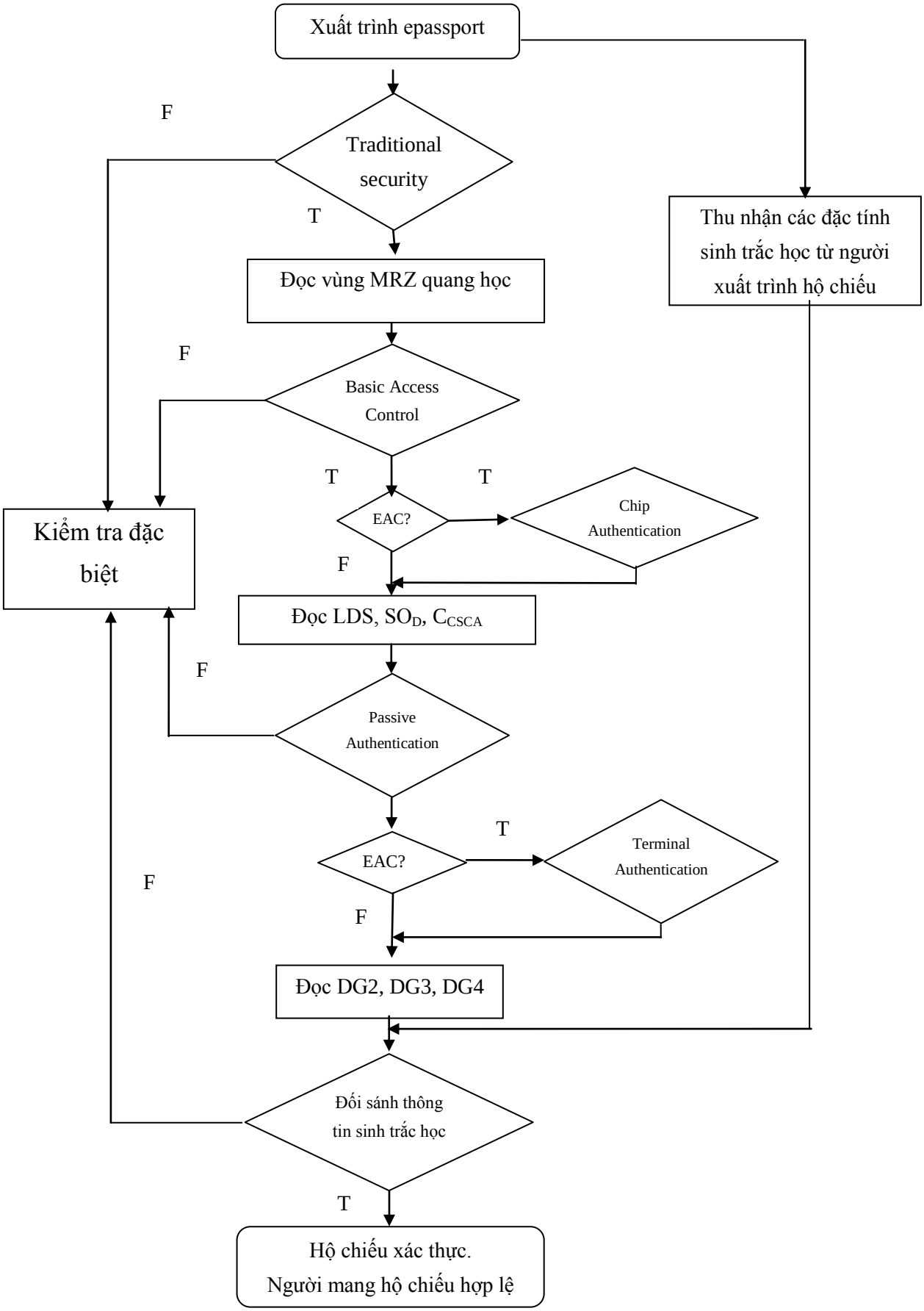


Hình 3.4: Quy trình cấp hộ chiếu điện tử đề xuất

2/. Quá trình kiểm tra kiểm soát tại các cửa khẩu quốc tế hộ chiếu điện tử

- **B1**: Người mang hộ chiếu suất trình hộ chiếu cho cơ quan kiểm tra, cơ quan tiến hành thu nhận các đặc tính sinh trắc học từ người xuất trình hộ chiếu.
- **B2**: Kiểm tra các đặc tính bảo mật trên trang hộ chiếu giấy thông qua các đặc điểm an ninh truyền thống đã biết: thủy ấn hoa văn chìm, mực phát quang, màng bảo vệ . . .

- **B3**: Hệ thống kiểm tra IS và chíp RFIC thực hiện quá trình BAC (kiểm soát truy cập căn bản). Sauk hi BAC thành công, IS có thẻ đọc các thông tin trong chip ngoại trừ DG3, DG4 (ảnh vân tay và mống mắt), mọi thông tin trao đổi giữa đầu đọc và chip được truyền thông báo bảo mật, mã hóa sau đó là xác thực theo cặp khóa (K_{ENC},K_{MAC}) có được từ khóa trình BAC.
- **B4**: Thực hiện quá trình xác thực bị động – Passive Authentication để kiểm tra tính xác thực và toàn vẹn của các thông tin lưu trong chip thông qua kiểm tra chữ ký trong SO_D bằng khóa công khai của cơ quan cấp hộ chiếu. Việc trao đổi khóa thông qua chứng chỉ số theo mô hình khuyến cáo của ICAO. Xác thực bị động kết hợp với xác thực chip (Chip Authentication) thì có thể khẳng định chip thực sự là nguồn gốc tức là không bị thay thế, không bị nhân bản (Đây là quá trình kiểm soát truy cập mở rộng).
- **B5**: Thực hiện quá trình xác thực chủ động – Active Authentication để đảm bảo rằng con chip điện tử trong hộ chiếu điện tử không bị thay thế, bằng cách trao đổi khóa xác thực giữa hệ thống kiểm soát khóa IS và con chip RFIC.
- **B6**: Quá trình xác thực đầu đọc Terminal Authentication (Thuộc phương pháp kiểm soát truy cập mở rộng) chứng minh quyền truy cập thông tin của hệ thống kiểm soát đến các nhóm thông tin nhậy cảm (DG3, DG4). Quá trình này chỉ thực hiện đối với những cơ quan kiểm tra hộ chiếu có triển khai kiểm soát truy cập mở rộng. Sauk hi xác thực đầu đọc thành công, đầu đọc chip có thể truy cập thông tin theo quyền thể hiện trong chứng chỉ C_{IS}.
- **B7**: Hệ thống kiểm soát đối sánh thông tin sinh trắc học thu nhận được trực tiếp từ người xuất trình hộ chiếu với thông tin sinh trắc học lưu trong chip. Nếu quá trình đối sánh thành công và kết hợp với các chứng thực trên, cơ quan kiểm tra hộ chiếu có đủ điều kiện để tin tưởng hộ chiếu là xác thực và người mang hộ chiếu đúng là con người mô tả trong hộ chiếu là xác thực và người mang hộ chiếu đúng là con người mô tả trong hộ chiếu. Nếu hệ thống kiểm tra tái cửa khẩu không được triển khai EAC (hoặc không có khóa mã để kiểm tra) thì sẽ không có quyền truy cập các thông tin trong DG3, DG4. Thông tin sinh trắc học duy nhất dùng để đối sánh chỉ là ảnh khuôn mặt.



Hình 3.5 Mô hình xác thực hộ chiếu điện tử

a. Basic Access Control

Mục đích: Chống đọc lén thông tin trong chip và nghe trộm thông tin truyền giữa RFIC và IS.

So sánh hộ chiếu điện tử có chứa con chip không tiếp xúc với hộ chiếu truyền thống, ta thấy có hai sự khác biệt cơ bản:

- Thông tin lưu trữ trong con chip có thể đọc được mà không cần mở cuốn hộ chiếu.

- Việc truyền thông giữa con chip và máy đọc nếu không được mã hóa, có thể bị thu nhận và đánh cắp từ khaongr cách xa vài mét.

Để chống đọc trộm thông tin bất hợp pháp , các quốc gia có thể lựa chọn kỹ thuật Kiểm soát truy cập cơ bản (BAC).

Kỹ thuật này là tùy chọn (OPTIONAL) sử dụng. Nó đảm bảo được rằng nội dung của chip điện tử chỉ có thể đọc được khi người mang hộ chiếu đồng ý xuất tình hộ chiếu của họ.

Một chip có hệ thống kiểm soát truy cập cơ bản phải chống được
các truy cập trái phép để đọc trộm thông tin. Để xác nhận truy cập là đáng tin cậy, ta phải thực hiện lần lượt các bước sau:

- Hệ thống liểm soát đọc các thông tin trong vùng dữ liệu đọc được bằng máy (dòng ICAO trong trang nhân than của hộ chiếu),trích ra các thông tin Số hộ chiếu, Ngày tháng năm sinh và Hạn hộ chiếu (bao gồm cả số kiểm tra của các thông tin này). Trong trường hợp không đọc được bằng máy, hệ thống phải cho phép nhập các thông tin trên bằng bàn phím. 16 bytes có trọng số lớn nhất của thông tin này sau khi áp dụng hàm băm SHA-1 được sử dụng làm đầu vào cho thuật toán sinh khóa truy cập cơ bản.

- Hệ thống kiểm soát và con chip kiểm tra tính tin cậy lẫn nhau và cùng sinh khóa.

- Sau khi xác nhận thành công tính đáng tin cậy, việc trao đổi thông tin giữa hệ thống kiểm soát và chip phải được bảo vệ bằng cơ chế trao đổi thông tin đảm bảo an toàn, trong đó các thông tin thay đổi đều được mã hóa.

Cơ chế này thực hiện bởi thực tế là các RFIC có thể kết nối đến bất kỳ một thiết bị đầu đọc theo chuẩn ISO/IEC 14443. Do đó, BAC nhằm mục đích giới hạn truy cập thông tin lưu trên RFIC của HCĐT cho những đối tượng có truy cập vật lý đến chính booklet của nó. Nghe trộm bị chặn bằng cách truyền thông báo bảo mật, tất cả dữ liệu truyền giữa RFIC và đầu đọc được mã hóa sử dụng khóa phiên có được từ BAC. Như vậy ta có thể ngăn chặn được hai hình thức tấn công là đọc lén và nghe trộm.

b. Xác thực bị động

Mục đích là để hệ thống kiểm tra thẩm định tính xác thực và toàn vẹn của thông tin lưu trong chip.

Trong các nhóm dữ liệu của cấu trúc logic LSD, con chip có chứa một đối tượng bảo vệ hộ chiếu (SO_D). Đối tượng này được mã hóa (ký) bởi cơ quan phát hành và chứa nội dung tóm lược của cấu dữ liệu logic LSD.

Các hệ thống kiểm tra kiểm soát cửa khẩu đều phải được cung cấp các khóa công khai bảo vệ hộ chiếu (KPu_{DS}) của các quốc gia khác hoặc có thể đọc trực tiếp Chứng chỉ số hộ chiếu (C_{DS}) từ hộ chiếu, nên có khả năng kiểm tra xác thực nội dung của SO_D. Bằng phương pháp này, thông qua nội dung của đối tượng bảo mật, nội dung của cấu trúc dữ liệu logic được xác thực.

Kỹ thuật kiểm tra này đòi hỏi khả năng xử lý của con chip điện tử trong hộ chiếu. Vì vậy nó được gọi là " xác thực bị động" nội dung của chip điện tử.

Các bước hoạt động

1. Đọc SO_D từ chip.
2. Lấy C_{DS} từ SO_D vừa đọc được ở trên.
3. Kiểm tra C_{DS} bằng KPu_{CSCA} có được từ PKD hoặc từ cơ sở dữ liệu cục bộ của hệ thống kiểm tra (trao đổi trực tiếp giữa hai quốc gia thông qua đường công hàm).
4. Kiểm tra chữ ký số SO_D.Signature sử dụng KPu_{DS}. Bước này nhằm khẳng định thông tin SO_{LDS} đúng là được tạo ra bởi cơ quan cấp hộ chiếu và SO_{LDS} không bị thay đổi.
5. Đọc các thông tin cần thiết từ LDS.
6. Tính hàm băm các thông tin ở bước 4 sau đó so sánh với SO_{LDS}. Bước này khẳng định được nhóm dữ liệu là xác thực và toàn vẹn.

Các thông tin sinh trắc bây giờ có thể được sử dụng để xác thực, đối chiếu với thông tin sinh trắc của người mang hộ chiếu.

Đánh giá về xác thực bị động

Xác thực bị động là cách đơn giản hiệu quả để phê chuẩn tính toàn vẹn và xác nhận những thông tin chứa trong epassport RFIC và một epassport nhân bản sẽ không được phát hiện bởi cơ chế này.

Mặt khác, cơ chế này quá đơn giản, vì PKI còn nhiều mặt hạn chế, liên quan đến chứng chỉ thu hồi. Đặc biệt, những điều này không đưa đến một hệ thống kiểm tra có

thể kết nối online đến PKD, đó có thể là một cơ hội cho phép epassport được ký bằng một DS trung hòa, có thể tiếp cận offline bởi hệt thống kiểm tra.

c. Xác thực chủ động

Các quốc gia phát hành hộ chiếu điện tử có thể lựa chọn phương pháp xác thực chủ động để bảo vệ con chip.

Phương pháp xác thực chủ động đảm bảo được rằng con chip điện tử trong hộ chiếu không bị thay thế, bằng cách trao đổi khóa xác thực giữa hệ thống kiểm soát và con chip.

Để làm được việc đó, con chip lưu trữ một cặp khóa xác thực chủ động (KPr_{AA} và KPu_{AA}). Một hàm băm của nhóm dữ liệu 15 (chứa thông tin về khóa công khai KPu_{AA}) được lưu trữ trong Đối tượng bảo mật hộ chiếu (SO_D) và được xác thực bởi chữ ký điện tử của cơ quan cấp phát.

Khóa bí mật tương ứng (KPr_{AA}) được lưu trữ trong vùng nhớ an toàn của con chip.

Bằng việc xác thực thông tin trong vùng đọc được bằng máy MRZ (dòng ICAO – thông qua nội dung của Đối tượng bảo mật SO_D) kết hợp với thông tin phản hồi trao đổi cặp khóa công khai và bí mật, hệ thống kiểm soát khẳng định được con chip không bị thay thế và sao chép nôi dung từ một hộ chiếu khác.

Phương pháp xac định chủ động yêu cầu khả năng xử lý thông tin của con chip điện tử trong hộ chiếu.

Khi hộ chiếu có sử dụng nhóm dữ liệu tùy chọn 15 thì hệ thống kiểm soát có thể cơ chế xác thực chủ động để đảm bảo rằng dữ liệu được đọc từ chip do chính cơ quan cấp phát phát hành và dữ liệu đọc từ trang nhân thân là trùng khớp.

Hệ thống kểm soát và chip thực hiện các bước sau:

- Đọc dòng ICAO trong trang nhân thân (nếu tronng quá trình kiểm soát truy cập cơ bản chưa đọc) và so sánh với dòng ICAO lưu trong chip tại nhóm dữ liệu thứ nhất đã được kiểm tra thông qua quá trình xác thực bị động nên tương tự ta cũng có thể đảm bảo rằng dòng ICAO trong trang nhân thân là đáng tin cậy và không bị thay đổi.

- Quá trình xác thực bị động cũng đảm bảo tính chính xác và toàn vẹn của nhóm dữ liệu thứ 15. Điều này thể hiện khóa công khai của quá trình xác thực chủ động cũng đáng tin cậy và không bị thay đổi.

- Để đảm bảo Đối tượng bảo mật không phải là bản sao chép hoặc thay thế, hệ thống kiểm soát sử dụng cặp khóa xác thực chủ động để kiểm tra chíp.

Sau khi đã qua bước kiểm tra trên thì có thể đảm bảo rằng Đối tượng bảo mật SO_D là thuộc về trang nhân thân, chip không bị thay thế và kết quả đối sáng thông tin trong trang nhân thân và trong chip là trùng khớp.

d. Kiểm soát truy cập mở rộng

Việc thực hiện bảo mật đối với các thông tin sinh trăc bổ sung phụ thuộc vào quy định của cơ quan cấp phát hoặc thỏa thuận song phương giữa các cơ quan cấp phát trong việc chia sẻ thông tin này để phục vụ công tác kiểm tra kiểm soát. Chỉ những cơ quan có thẩm quyền và có được khóa giải mã mới có thể đọc ghi thông tin trong vùng mở rộng. Vì vậy, vùng dữ liệu mở rộng này thường được các quốc gia sử dụng với mục đích quản lý nghiệp vụ, ví dụ như ghi các thông tin nhạy cảm về đặc điểm nhân dạng, quá trình hoạt động cũng như biện pháp đối sách để trợ giúp cho kiểm soát viên trong quá trình kiểm tra kiểm soát tại các cửa khẩu quốc tế.

Quá trình kiểm soát truy cập mở rộng gồm 2 quá trình:

- Xác thực chip (Chip Authentication)

Kết hợp với Passive Authentication sẽ chứng minh tính nguyên gốc của chip, ngoài ra chip Authentication còn khắc phục được nhược điểm ngữ cảnh thách đố của Active Authentication và cung cấp khóa phiên mạnh [Federal Office for Information Sercurity, Germany: *Advanced Sercurity Mechanisms for Machine Readable Ttravel Documents – Extended Access Control (EAC), September 2007]*.

- Xác thực đầu đọc (Terminal Authentication)

Terminal Authenticatiion là giáo thức thách đố - Trả lời tạo ra sự xac thực phía IS.

Nhận xét:

Với việc xác thực biện pháp xác thực bị động kết hợp với xác thực chủ động và kiểm soát truy cập cơ bản, kiểm soát truy cập mở rộng như em đã trình bày đã đảm bảo các mục tiêu, yêu cầu đặt ra đối với việc bảo mật hộ chiếu điện tử. Cụ thể:

Về tính chân thực: Mục tiêu này có thể đảm bảo nếu quá trình thu thập, in hộ chiếu và ghi thông tin vào chip tuân thủ đúng quy trình nghiệp vụ.

Tính không thể nhân bản: Mục tiêu này đạt được với sự kết hợp kết quả của chip Authentication và Passive Authentication. Hơn thế nữa nó còn khắc phục được nhược điểm ngữ cảnh thách đố so với sử dụng Active Authentication.

Tính nguyên vẹn và xác thực: Mục tiêu này luôn đạt được với Passive Authentication và sử dụng mô hình PKI.

Tính liên kết người - hộ chiếu: Sử dụng 3 đặc tính sinh trắc học có thể nâng cao hiệu quả của mục đích này thay vì chỉ "quan sát" một thông tin duy nhất là ảnh khuôn mặt.

Tính liên kết hộ chiếu – chip: Mục tiêu này đạt được do quá trình so sánh MRZ trong chip (đã được ký bởi cơ quan cấp hộ chiếu) với MRZ mà IS đọc được tại vùng quang học trên trang booklet.

Kiểm soát truy cập: Mục tiêu này đạt được thông qua 2 quá trình điều khiển truy cập BAC và EAC.

Chương 4:

LẬP TRÌNH ỨNG DỤNG THỬ NGHIỆM CHỮ KÍ SỐ ĐỂ MÃ HÓA BẢO VỆ THÔNG TIN

Trong chương này, em xin trình bày về chương trình thử nghiệm phát sinh chữ kí số để bảo vệ thông tin trong con chip của hộ chiếu điện tử và giải mã kiểm tra xác thực thông tin.

Chương trình thử nghiệm gồm 2 môđun chính, đó là phần chương trình mã hóa và giải mã thông tin sử dụng thuật toán khóa công khai RSA và phần chương trình mô tả thuật toán băm SHA để tóm lược bản tin. Chương trình được viết trên ngôn ngữ C++ và chạy trên môi trường windows. Do thời gian làm luận văn có hạn nên dự định viết chương trình bằng ngôn ngữ Java để có thể chạy trên các môi trường khác nhau của em đã không kịp hoàn thành.

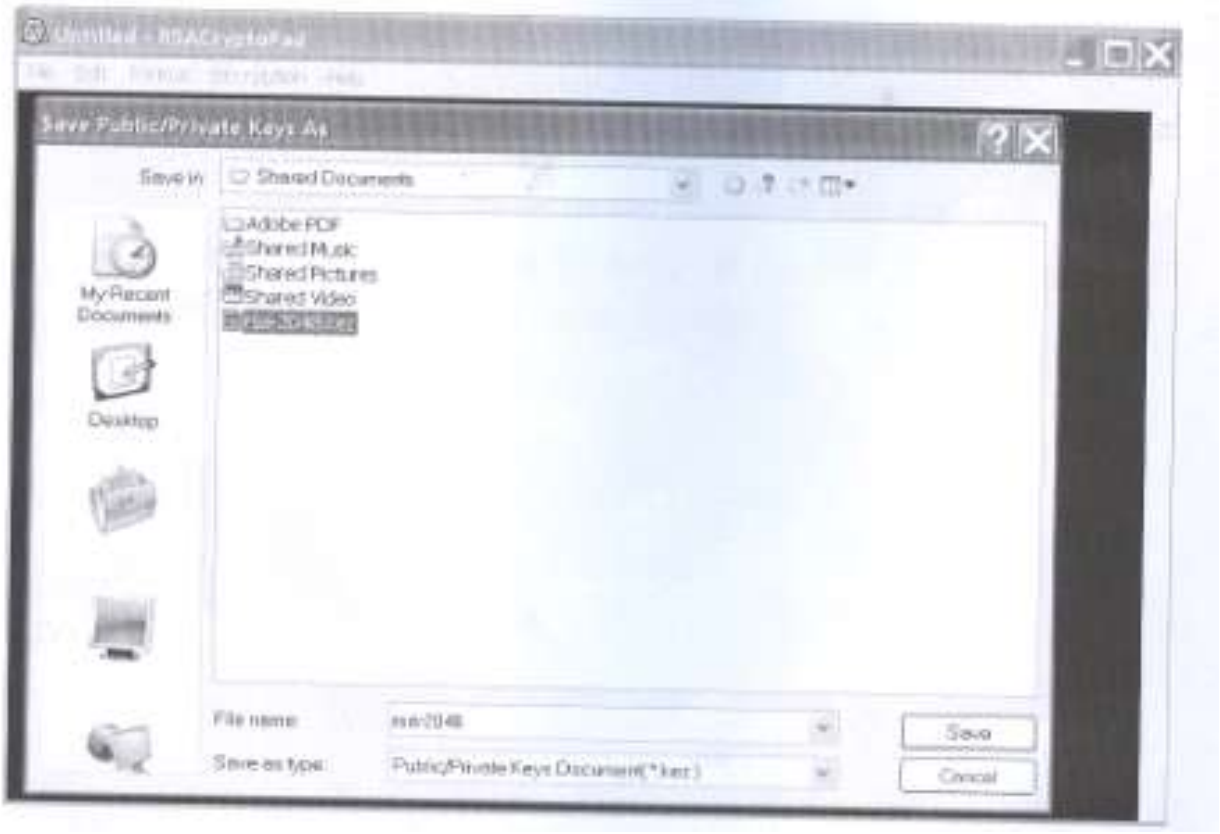
❖ **Chương trình mã hóa và giải mã thông tin sử dụng thuật toán RSA**

Chương trình gồm có 3 chức năng chính là:

- ***Phát sinh khóa*** (khóa công khai, khóa bí mật). Độ dài khóa có thể tùy chọn 1024, 2048 hoặc 3072 bit tùy thuộc vào độ bảo mật của thông tin cần mã hóa (khóa mã cấp quốc gia cần độ dài 3072 bit, khóa mã của cơ quan cấp phát cần độ dài 2048 bit theo quy định của Tổ chức hàng không dân dụng quốc tế ICAO).

Sau khi phát sinh khóa, cặp khóa sẽ được lưu trữ trong máy, tập tin chứa khóa bí mật được dùng để kí có đuôi .kez, tập tin chứa khóa công khai dùng để giải mã sẽ có đuôi .pke

Hình 4.1 Phát sinh cặp khóa RSA



Hình 4.2 Lưu trữ khóa bí mật có phần mở rộng .kez

- ***Mã hóa thông tin*** trước khi ghi vào con chip của hộ chiếu điện tử (sử dụng khóa công khai để mã hóa)

Để mã hóa thông tin trong các nhóm dữ liệu của con chip điện tử, chương trình sẽ lần lượt mở từng tập tin, thực hiện mã hóa trước khi ghi thông tin đó vào trong con chip.

Hình 4.3 Thông tin cần mã hóa trước khi ghi vào chip điện tử

Hình 4.4 Thông tin sau khi mã hóa

- ***Giải mã để xác thực và kiểm tra thông tin*** trong con chip của hộ chiếu điện tử.

Hình 4.5 Thông tin thu được sau khi giải mã

Thông tin thu được sau khi giả mã sẽ được so sánh với các thông tin lưu trữ trong cơ sở dữ liệu để kiểm tra tính xác thực.

❖ **Chương trình tóm lược bản tin một chiều sử dụng thuật toán băm SHA**

Như em đã giới thiệu ở phần chương 1 và chương 3, SHA là thuật toán tóm lược bản tin một chiều có độ an toàn cao và được sử dụng rất phổ biến hiện nay trên thế giới. SHA được phân chia thành SHA-1 và SHA-2 tùy thuộc vào độ dài của bản tin tóm lược. Trong khi SHA-1 có độ dài nhỏ hơn 160 bit thì SHA-2 có độ dài từ 224 bit trở lên (SHA-224, SHA-256, SHA-378, SHA-512).

Chương trình thử nghiệm cho phép tóm lược bản tin dưới cả dạng file và dạng chuỗi nhập trực tiếp bằng chương trình. Kết quả tóm lược có thể hiệm thị dưới dạng chuỗi kí tự hoặc dạng thập lục phân (haxa decimal), sau đó có thể lưu trữ dưới dạng tập tin để ghi vào trong chip điện tử.

KẾT LUẬN

Trong luận văn tốt nghiệm, em đã ứng dụng lý thuyết về hạ tầng mã hóa công khai và chữ kí số để phục vụ việc kí lên hộ chiếu điện tử (trực tiếp là con chip trong hộ chiếu điện tử) và xác thực thông tin trong hộ chiếu điên tử tại các cửa khẩu quốc tế. Việc áp dụng các biện pháp bảo mật này đã đáp ứng tốt các yêu cầu đối với vấn đề bảo mật hộ chiếu điện tử, chống lại các hình thức tấn công hiện nay. Đề xuất mà em đưa ra là sử dụng kết hợp RSA+SHA kế thừa được toàn bộ các kĩ thuật, công nghệ bảo mật hộ chiếu truyền thống đồng khai thác sử dụng các công nghệ bảo mật hiện đại nhất để bảo mật cho hộ chiếu điện tử. So sánh với các yêu cầu bảo mật bắt buộc quy định trong tài liệu ICAO Doc 9303 thì cách thức bảo mật em đưa ra đáp ứng đầy đủ quy định này.

Tuy nhiên trong quá trình thực hiện luận văn, do thời gian có hạn nên em không thể tránh được những thiếu sót và hạn chế nhất định. Em rất mong được sự đóng góp của thầy cô và các bạn để em tiếp tục nghiên cứu và phát triển đề tài đã thực hiện trong thời gian tới.

Em xin chân thành cảm ơn!

DANH MỤC TÀI LIỆU THAM KHẢO

[1] Nguyễn Ngọc Hoá, Phạm Tâm Long, Khoa CNTT, ĐHCN-ĐHQGHN: *Mô hình xác thực hộ chiếu điện tử,* Hội thảo Quốc gia lần thứ XI, 2008.

[2] GS.TS. Phan Đình Diệu, *Lý thuyết mật mã và An toàn thông tin*, 1999.

[3] Nguyễn Ngọc Bình Phương, Thái Thanh Phong, *Các giải pháp lập trình C#,* www.dvpub.com.vn.

[4] Doc 9303, Ningh Draft: *Machine Readable Travel Documents*, July 2005.

[5] Information *about the Australian e-Passport*, http:// www.dfat.gov.au/dept/passports/.

[6] Informtion *about the US e-Passport*, http://www.state.gov/r/pa/prs/ps/2006/61538.htm.

[7] ICAO, PKI for machine readable travel documents offering ICC read-only access, version 1.0. Technical Report, ICAO, Apr 2004/

[8] *Secure Hash Standard*, Federal Information Processing Standards Publication (FIPS PUBS) 180-2, 2002 August.

[9] Xiaoyun Wang, Dengguo Feng, Xuejja Lai, Hongbo Yu, *Conllisions for Hash Functions MD4, MD5, HAVAL* – 128 and RIPEMD, 2004 August.

[10] Bách khoa toàn thư mở Wikipedia, http://vi. wikipedia. org/wiki.

[11] Trang web http:// www.codeguru.com