

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

NGUYỄN HẢI NINH

HỆ MÃ CÔNG KHAI RSA VÀ ỨNG DỤNG BẢO MẬT
TRONG TRAO ĐỔI TÀI LIỆU LÂM SÀNG CDA

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

THÁI NGUYÊN - 2016

LỜI CẢM ƠN

Trên thực tế không có sự thành công nào mà không gắn liền với những sự hỗ trợ, giúp đỡ dù ít hay nhiều của người khác. Trong suốt thời gian từ khi bắt đầu học tập tại trường đến nay, em đã nhận được rất nhiều sự quan tâm, giúp đỡ của quý Thầy Cô, gia đình và bạn bè. Với lòng biết ơn sâu sắc nhất, em xin gửi lời cảm ơn chân thành và sự tri ân đến quý Thầy Cô - Trường Đại Học Công Nghệ Thông Tin và Truyền Thông Thái Nguyên.

Em xin gửi lời cảm ơn tới TS. Nguyễn Văn Tảo, thầy đã dạy cho em những kiến thức quý báu về bảo mật, về hệ mã công khai cũng như về hệ mã RSA mà em đã sử dụng trong luận văn này. Em xin gửi lời cảm ơn tới TS. Nguyễn Hải Minh – Khoa Công Nghệ Thông Tin - Trường Đại Học Công Nghệ Thông Tin và Truyền Thông Thái đã tận tình hướng dẫn em trong thời gian thực hiện đề tài.

Tôi xin gửi lời cảm ơn đến các anh chị em lớp CK13C Quảng Ninh, cảm ơn gia đình, bạn bè đồng nghiệp tại trường THPT Hoàng Hoa Thám nơi tôi công tác đã luôn ủng hộ động viên và tạo điều kiện cho tôi trong suốt thời gian học tập.

Do thời gian có hạn nên trong phần trình bày bản luận văn không tránh khỏi những thiếu sót. Em rất mong nhận được những ý kiến đóng góp quý báu của quý Thầy Cô và các bạn đọc.

Em xin chân thành cảm ơn!

Thái Nguyên, ngày 10 tháng 05 năm 2016

Học viên thực hiện

Nguyễn Hải Ninh

LỜI CAM ĐOAN

Tôi tên là: **Nguyễn Hải Ninh**

Sinh ngày: 24/03/1985

Là học viên lớp Cao học K13C – Trường Công Nghệ Thông Tin & Truyền Thông – Đại Học Thái Nguyên, hiện đang công tác tại trường THPT Hoàng Hoa Thám – Đông Triều – Quảng Ninh.

Trong thời gian làm luận văn tốt nghiệp tôi nghiên cứu và triển khai đề tài: “Hệ mã công khai RSA và ứng dụng bảo mật trong trao đổi tài liệu lâm sàng CDA”, dưới sự hướng dẫn khoa học của TS. Nguyễn Hải Minh. Tôi xin cam đoan, nội dung được trình bày trong bản luận văn là do tôi tìm hiểu, nghiên cứu và trình bày. Các nội dung tham khảo đều có trích dẫn đầy đủ và đúng quy định.

Tôi xin chịu hoàn toàn trách nhiệm trước lời cam đoan của mình.

Thái Nguyên, ngày 10 tháng 05 năm 2016

Học viên thực hiện

Nguyễn Hải Ninh

MỤC LỤC

	Trang
LỜI CẢM ƠN	i
LỜI CAM ĐOAN	iii
MỤC LỤC.....	iv
DANH MỤC CÁC BẢNG.....	vi
DANH MỤC CÁC HÌNH ẢNH	vii
MỞ ĐẦU.....	1
CHƯƠNG 1 CHUẨN TÀI LIỆU LÂM SÀNG	2
CLINICAL DOCUMENT ARCHITECTURE	2
1.1. Giới thiệu chung.....	2
1.1.1. Mục đích thiết kế chuẩn tài liệu CDA [3]	2
1.1.2. Các tính chất của một tài liệu CDA	3
1.2. Cấu trúc chuẩn tài liệu CDA	4
1.2.1. Cấu trúc Header của tài liệu CDA.	4
1.2.2. Cấu trúc Body của tài liệu CDA	7
1.2.3. Cấu trúc của một Entry.	14
1.3. Mô hình tham chiếu dữ liệu - HL7 Reference Information Model(RIM)	19
1.3.1. Một số khái niệm quan trọng trong mô hình.	19
1.3.2. HL7 V3 Data Types.....	20
1.3.3. Nhóm từ vựng – HL7 Vocabulary Domains	20
1.4. Mô hình để sinh một tài liệu CDA.....	21
1.5. Một số Entry chính được sử dụng trong việc gắn ảnh vào tài liệu.	22
1.6. Ví dụ tài liệu CDA khi duyệt trên trình duyệt IE.....	26
CHƯƠNG 2 CÁC KIẾN THỨC CƠ BẢN VỀ HỆ MÀ CÔNG KHAI.....	27
2.1. Giới thiệu chung.....	27
2.1.1. Khái niệm hệ mật mã	27
2.1.2. Hệ mật mã khóa công khai [2].....	29
2.2. Hệ mã RSA	30

2.2.1. Cơ sở xây dựng RSA	30
2.2.2. Quá trình xây dựng tạo khóa cho hệ mật RSA.	31
2.2.3. Một số chú ý quan trọng về RSA.....	37
2.2.4. Ưu và nhược điểm của hệ mật mã khoá công khai.....	39
CHƯƠNG 3 KẾT QUẢ CÀI ĐẶT CÁC THUẬT TOÁN.....	41
3.1. Các tài liệu lâm sàng được sử dụng trong bệnh viện.	41
3.1.1. Nội dung hồ sơ bệnh án hiện đang áp dụng.....	41
3.1.2. Các thông tin có trong tờ bệnh án.....	45
3.2. Mô hình ứng dụng Hệ mã RSA trong bài toán mã hóa tài liệu lâm sàng CDA. 53	
3.2.1. Ứng dụng thuật toán mã hóa RSA cho tài liệu lâm sàng CDA	53
3.2.2. Mô hình ứng dụng Hệ mã RSA trong bài toán mã hóa tài liệu lâm sàng CDA	54
3.3. Module Mã hóa tài liệu CDA.....	56
3.3.1. Dữ liệu vào.....	56
3.3.2. Quy trình mã hóa	57
3.3.3. Tài liệu CDA dạng XML sau khi mã hóa.....	58
3.3.4. Module giải mã tài liệu	59
3.3.5. Giao diện chương trình	60
3.4. Module mã hóa thông tin phần Header hoặc Body.....	61
3.4.1. Thuật toán mã hóa thông tin phần Header hoặc Body	61
3.4.2. Thuật toán giải mã thông tin phần Header hoặc Body	62
3.4.3. Demo module mã hóa Header hoặc Body.	63
3.5. Một số Modules cốt lõi trong chương trình.	63
3.5.1. Module RSA	63
3.5.2. Module ReadDOM	63
3.5.3. Một số vấn đề quản lý khóa RSA.	64
KẾT LUẬN VÀ KIẾN NGHỊ.....	65
TÀI LIỆU THAM KHẢO.....	66

DANH MỤC CÁC BẢNG

Bảng 1.1: Các thuộc tính của Header.....	6
Bảng 1.2: Quan hệ các lớp trong Header	7
Bảng 1.3: Cấu trúc Body của tài liệu CDA.....	8
Bảng 1.4: Các thuộc tính của Section	8
Bảng 1.5: Các đối tượng của Section.....	9
Bảng 1.6: Các quan hệ của Section.....	9
Bảng 1.7: Các thuộc tính hỗ trợ cho định dạng.....	13
Bảng 1.8: Các đối tượng tham gia một Entry	15
Bảng 1.9: Quan hệ trong một Entry	17
Bảng 1.10: Quan hệ entry-Entry Relationships	18
Bảng 1.11: Ví dụ đoạn mã Entry.....	22
Bảng 1.12: Diễn giải đoạn mã Entry.....	24
Bảng 2.1: Tóm tắt các bước tạo khoá, mã hoá, giải mã của Hệ RSA.....	34
Bảng 3.1: Cấu trúc thông tin tờ bệnh án	47

DANH MỤC CÁC HÌNH ẢNH

Hình 1.1: Cấu trúc tài liệu CDA [3].....	5
Hình 1.2: Sơ đồ sinh tài liệu CDA	21
Hình 1.3: Quan hệ giữa các module trong tài liệu CDA.....	22
Hình 2.1: Quá trình mã hoá và giải mã	28
Hình 2.2: Mã hoá thông điệp sử dụng khoá công khai P	29
Hình 2.3: Giải mã thông điệp sử dụng khoá riêng của người nhận	30
Hình 2.4: Mã hoá thông điệp sử dụng khoá bí mật S để mã thông điệp và khoá công khai P để mã khoá bí mật S.....	39
Hình 2.5: Giải mã thông điệp sử dụng khoá bí mật S để giải mã thông điệp và khoá riêng P để giải mã khoá bí mật S.....	39
Hình 3.1: Sơ đồ thuật toán RSA.....	54
Hình 3.2: Sơ đồ mã hóa tài liệu CDA	55
Hình 3.3: Tài liệu CDA dạng XML	56
Hình 3.4: Sơ đồ quy trình mã hóa toàn bộ tài liệu CDA.....	57
Hình 3.5: Tài liệu CDA sau khi mã hóa.....	58
Hình 3.6: Sơ đồ quy trình giải mã toàn bộ tài liệu CDA	59
Hình 3.7: Giao diện chương trình	60
Hình 3.8: Sơ đồ quy trình mã hóaphần Header hoặc Body	61
Hình 3.9: Sơ đồ quy trình giải mã phần Header hoặc Body	62
Hình 3.10: Demo mã hóa vàgiải mã Header Body tài liệu CDA.....	63

MỞ ĐẦU

Khi mà các ứng dụng CNTT đã và đang ngày càng phổ biến rộng rãi đã ảnh hưởng rất lớn đến diện mạo của đời sống xã hội, kinh tế. Mọi công việc của chúng ta đều có thể thực hiện được từ xa với sự hỗ trợ của máy tính và mạng Internet. Tất cả các thông tin liên quan đều được máy tính quản lý và truyền đi trên hệ thống mạng. Trong y tế, việc ứng dụng công nghệ thông tin để nâng cao chất lượng chăm sóc sức khỏe cho người dân cũng đã được chú trọng, rất nhiều chương trình ứng dụng trên máy tính đã được xây dựng để hỗ trợ việc quản lý thông tin bệnh nhân, quản lý viện phí, thanh toán bảo hiểm và khám chữa bệnh từ xa và các hệ thống hỗ trợ quản lý và trao đổi thông tin tài liệu lâm sàng cũng đang được xây dựng và phát triển. Do đó, vấn đề bảo mật các thông tin cá nhân trong tài liệu lâm sàng là một việc cần thiết vì nó sẽ bảo đảm tính riêng tư cho mỗi bệnh nhân.

Trong phạm vi nghiên cứu của đề tài, chúng tôi tập chung nghiên cứu cấu trúc chuẩn tài liệu lâm sàng HL7 Clinical Document Architecture (CDA), hệ mã công khai RSA và ứng dụng trong việc mã hóa phần thông tin riêng tư của bệnh nhân được lưu trong tài liệu CDA ở hai mức: Phần Header của tài liệu và mức section nằm trong component thuộc phần Body.

Kết quả của nghiên cứu sẽ là cơ sở khoa học để hướng tới việc khi gửi thông tin khám chữa bệnh đến người nhận thì đúng người nhận mới có thể xem và tra cứu thông tin trong tài liệu. Hơn nữa, kết quả đầu ra của tài liệu sau khi mã hóa phải đảm bảo được 6 tích chất cơ bản của tài liệu lâm sàng được quy định bởi tổ chức chuẩn quốc tế Health Level 7. Bên cạnh đó chúng tôi cũng đề xuất mô hình và giải pháp sử dụng hệ mã vào quá trình mã hóa dùng trong trao đổi thông tin giữa cơ sở y tế và bác sỹ, giữa bác sỹ với bác sỹ thông qua môi trường Internet.

CHƯƠNG 1

CHUẨN TÀI LIỆU LÂM SÀNG

CLINICAL DOCUMENT ARCHITECTURE

1.1. Giới thiệu chung.

Chuẩn tài liệu lâm sàng – HL7 Clinical Document Architecture (CDA) là chuẩn tài liệu có cấu trúc. Thông qua chuẩn tài liệu này, sẽ chi rõ cho cơ quan quản lý, các cơ sở y tế, các nhà thiết kế phần mềm, phần cứng về cấu trúc “Structure” và tính ngữ nghĩa “Semantic” của một tài liệu lâm sàng. Với mục đích hỗ trợ việc trao đổi thông tin giữa các cơ sở y tế, các tổ chức cơ quan liên quan được thuận tiện và chính xác trên môi trường truyền thông rất đa dạng và phong phú hiện nay. Phiên bản CDA Release 1 hay còn gọi (ANSI/HL7 CDA R1.0), được thông qua và công nhận là chuẩn Quốc tế vào tháng 11 năm 2000. Phiên bản CDA Release 2 (CDA R2) được thông qua tháng 5 năm 2005 bởi American National Standards Institute/ Health Level Seven International (ANSI/HL7). Với sự tân tiến về thiết kế của phiên bản CDA R2, cùng với việc cập nhật các dữ liệu (Data type), loại bỏ, bổ sung một số thuộc tính (Header Attribute và Section Attribute), sự gắn kết chặt chẽ với mô hình HL7 Reference Information Model (RIM) trong quá trình phát sinh và hình thành tài liệu, cho phép tham chiếu và sử dụng các bộ máy tương thích với chuẩn của HL7 (như: chuẩn LOINC, chuẩn SMOMED-CT và ICD 10), sự thay đổi các từ vựng trong nhóm CNE (Code No Extended) và việc bổ sung nhóm từ vựng trong CNE từ nhóm CWE (Code With Extended) đã làm cho CDA R2 có những tính năng mạnh hơn rất nhiều so với phiên bản trước và đồng thời tính ngữ nghĩa trong tài liệu lâm sàng đã được thể hiện một cách rõ nét hơn.

1.1.1. Mục đích thiết kế chuẩn tài liệu CDA [3]

- Đưa ra quy định trong việc trao đổi thông tin chăm sóc sức khỏe.
- Mang lại hiệu quả trong việc triển khai các hệ thống mang tính liên thông, có sự trao đổi và chia sẻ thông tin giữa các hệ thống khác nhau trên phạm vi lớn.
- Việc mở và hiển thị nội dung tài liệu CDA không bị giới hạn bởi sự khác nhau về công nghệ và phần mềm hiện đang sử dụng giữa nơi gửi và nơi nhận.

Số hóa bởi Trung tâm Học liệu – ĐHTN <http://www.lrc.tnu.edu.vn>

- Các thông tin được mã hóa theo chuẩn CDA được toàn vẹn, an toàn và dễ dàng lưu trữ lâu dài theo thời gian.
- Cho phép trao đổi thông tin qua các hệ thống trao đổi thông tin điện tử và hệ thống thư tín điện tử.
- Tương thích với các chuẩn tài liệu được tạo ra bởi các chương trình ứng dụng khác.
- Việc trao đổi thông tin không phụ thuộc vào cơ sở hạ tầng hoặc hệ thống lưu trữ.
- Cung cấp một thiết kế hợp lý cho mọi ứng dụng.
- Cho phép ghi lại những thông tin nhằm đáp ứng nhu cầu và các quy định trong việc giám sát và quản lý thông tin trong tài liệu.

1.1.2. Các tính chất của một tài liệu CDA

Một tài liệu lâm sàng được thiết kế dựa trên chuẩn tài liệu CDA sẽ có 6 tính chất sau:

- Tính bền - Persistence: Một tài liệu CDA tiếp tục lưu trữ và được bảo tồn trong trạng thái nguyên vẹn về cấu trúc và ngữ nghĩa, trong khoảng thời gian đáp ứng các yêu cầu truy vấn thông tin từ phía người sử dụng và khai thác tài liệu.
- Tính quản lý - Stewardship: Một tài liệu lâm sàng cần phải được duy trì, cập nhật, bảo đảm tính an toàn, an ninh và toàn vẹn bởi một tổ chức cơ quan có thẩm quyền.
- Tính xác thực - Potential for authentication: Một tài liệu lâm sàng là sự tập hợp các thông tin mà có thể dùng để chứng thực tính pháp lý.
- Tính bối cảnh - Context: Một tài liệu lâm sàng cần phải chứng minh được bối cảnh với nội dung của nó.
- Tính đủ- Wholeness: Tính toàn vẹn và đầy đủ của tài liệu được áp dụng cho toàn bộ tài liệu CDA, không phải chỉ áp dụng cho riêng từng phần của tài liệu.