ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

VƯƠNG THỊ HẠNH

NGHIÊN CỨU CÁC PHƯƠNG PHÁP MẬT MÃ ĐẢM BẢO TÍNH TOÀN VẸN DỮ LIỆU TRONG TRƯỜNG HỌC THÔNG MINH

Ngành**:** Hệ thống thông tin
Chuyên ngành: Hệ thống thông tin
Mã số: 60.48.01.04

TÓM TẮT LUẬN VĂN THẠC SĨ NGÀNH HỆ THỐNG THÔNG TIN

NGƯỜI HƯỚNG DẪN KHOA HỌC: TS. LÊ PHÊ ĐÔ
TS. PHÙNG VĂN ỔN

HÀ NỘI 2017

LỜI CẢM ƠN

Trước tiên tôi xin gửi lời cảm ơn sâu sắc nhất đến thầy Lê Phê Đô và thầy Phùng văn Ổn. Các thầy đã tận tâm, tận lực hướng dẫn, định hướng phương pháp nghiên cứu khoa học cho tôi, đồng thời cũng đã cung cấp nhiều tài liệu và tạo điều kiện thuận lợi trong suốt quá trình học tập và nghiên cứu để tôi có thể hoàn thành luận văn này.

Tôi xin được gửi lời cảm ơn đến các thầy, cô trong bộ môn Hệ thống thông tin và khoa công nghệ thông tin, Trường Đại học Công nghệ - Đại học Quốc gia Hà Nội đã nhiệt tình giảng dạy và truyền đạt những kiến thức, kinh nghiệm quý giá trong suốt thời gian tôi học tập tại trường.

Tôi xin gửi lời cảm ơn đến các bạn học viên lớp K22-HTTT, những người đồng hành trong suốt khóa học và có nhiều góp ý bổ ích cho tôi. Cảm ơn gia đình, bạn bè đã quan tâm và động viên giúp tôi có nghị lực phấn đấu để hoàn thành tốt luận văn này.

Do kiến thức và thời gian có hạn nên luận văn chắc chắn không tránh khỏi những thiếu sót nhất định.

Một lần nữa xin gửi lời cảm ơn chân thành và sâu sắc.

Hà Nội, tháng 8 năm 2017

Học viên thực hiện

Vương Thị Hạnh

LỜI CAM ĐOAN

Luận văn thạc sĩ đánh dấu cho những thành quả, kiến thức tôi đã tiếp thu được trong suốt quá trình rèn luyện, học tập tại trường. Tôi xin cam đoan luận văn "***Nghiên cứu các phương pháp mật mã đảm bảo tính toàn vẹn dữ liệu trong trường học thông minh".*** được hoàn thành bằng quá trình học tập và nghiên cứu của tôi dưới sự hướng dẫn của TS. Lê Phê Đô và TS. Phùng văn Ổn.

Trong toàn bộ nội dung nghiên cứu của luận văn, các vấn đề được trình bày là những tìm hiểu và nghiên cứu của cá nhân tôi hoặc là trích dẫn các nguồn tài liệu và một số trang web đều được đưa ra ở phần Tài liệu tham khảo.

Tôi xin cam đoan những lời trên là sự thật và chịu mọi trách nhiệm trước thầy cô và hội đồng bảo vệ luận văn thạc sĩ.

Hà Nội, tháng 8 năm 2017

Vương Thị Hạnh

MỞ ĐẦU

1. Tính cấp thiết của đề tài luận văn

Mô hình trường học thông minh nhằm tối ưu hóa các thiết bị dạy học. Các thiết bị hiện đại bao gồm: Máy chủ kết nối màn hình tương tác hoặc máy chiếu Projector, màn hình LCD, camera ghi hình, máy tính, máy in cùng với hệ thống internet được kết nối đồng bộ. Sử dụng các phần mềm hỗ trợ học tập, phần mềm mô phỏng, phần mềm quản lý học tập với nội dung đa phương tiện có thể giao tiếp hai chiều giữa giáo viên, học sinh và gia đình. Đồng thời khuyến khích học sinh tham gia chủ động hơn vào nội dung học tập. Giải pháp trường học thông minh đã được triển khai thành công tại nhiều trường học ở Mỹ, Trung Đông và một số nước Châu Âu, Châu Á. Trường học thông minh tạo môi trường tốt cho giáo viên và học sinh học tập; nâng cao chất lượng dạy và học.

Tuy nhiên, cùng với lợi ích của việc sử dụng phần mềm quản lý học sinh thông qua mạng internet là vấn đề mất an toàn thông tin như: mất mát dữ liệu, rò rỉ thông tin làm ảnh hưởng nghiêm trọng đến nhà trường, thầy cô và học sinh. Các phương thức tấn công thông qua mạng ngày càng tinh vi phức tạp có thể dẫn đến mất mát thông tin, thay đổi thông tin…. Vì vậy đảm bảo an toàn thông tin trường học thông minh là nhiệm vụ rất quan trọng mà tôi đề cập trong luận văn này. Trường học Việt Nam tuy có quan tâm nhiều nhưng chưa được toàn diện, nên mục tiêu và đối tượng mà tôi hướng đến là *"**Nghiên cứu các phương pháp mật mã đảm bảo tính toàn vẹn dữ liệu trong trường học thông minh".***

2. Mục đích nghiên cứu:

❖ Mục tiêu của đề tài.

- Nghiên cứu mô hình trường học thông minh.
- Nhận diện những thách thức và biện pháp giải quyết đảm bảo toàn vẹn dữ liệu nói chung và toàn vẹn dữ liệu trường học nói riêng.
- Xây dựng chương trình mô phỏng

❖ Đối tượng và phạm vi nghiên cứu.

- Các trường học và lớp học thông minh.

❖ Phương pháp nghiên cứu.

- Tìm hiểu các mô hình lớp học thông minh trên thế giới và Việt Nam cũng như các nguy cơ của công nghệ ảnh hưởng đến trường học.
- Tìm hiểu các phương pháp mật mã để đảm bảo toàn vẹn dữ liệu trường học.
  - Phương pháp sử dụng hàm băm SHA
  - Phương pháp dùng mã xác thực dữ liệu MAC

- Phương pháp dùng chữ ký số

3. Nội dung của đề tài, các vấn đề cần giải quyết.

a. Hướng nghiên cứu:

- Mô hình trường học thông minh
- Các nguy cơ và các công nghệ đảm bảo an toàn dữ liệu.

b. Nội dung:

Chương 1: An toàn thông tin ở trường học thông minh

Chương 2: Các phương pháp mật mã đảm bảo toàn vẹn dữ liệu

Chương 3: Ứng dụng chữ ký điện tử đảm bảo tính toàn vẹn dữ liệu trong trường học

Chương trình demo.

CHƯƠNG 1: VẤN ĐỀ AN TOÀN THÔNG TIN Ở TRƯỜNG HỌC THÔNG MINH

1.1 TỔNG QUAN VỀ TRƯỜNG HỌC THÔNG MINH

Bước sang thế kỷ 21, công nghệ thông tin được ứng dụng mạnh trong quá trình tổ chức đào tạo, thay đổi nội dung, phương pháp giảng dạy hiện đại và bám sát yêu cầu thực tiễn theo xu thế chung thế giới là phát triển giáo dục điện tử, hình thành trường học nền tảng số hóa

Lớp học thông minh – trường học thông minh chú trọng vào giờ dạy tương tác và quản lý học tập.

- Giảng dạy tương tác: hỗ trợ bằng cách sử dụng các chức năng chia sẻ màn hình, màn hình giám sát các hoạt động nhóm, bài kiểm tra và thăm dò ý kiến,…
- Quản lý học tập: hỗ trợ giáo viên lập kế hoạch quản lý khóa học, bài học.

Hầu hết các phòng học được kết nối internet thông qua wifi hoặc băng thông rộng không dây và có trang thiết bị máy tính để bàn, máy tính xách tay, máy tính bảng,..

Hình 1.1 Mô hình lớp học thông minh

1.2 XÂY DỰNG TRƯỜNG HỌC THÔNG MINH Ở VIỆT NAM

1.3 CÁC NGUY CƠ MẤT AN TOÀN THÔNG TIN TRONG TRƯỜNG HỌC

1.3.1 Những mối đe dọa về an toàn thông tin trong trường học

- Dữ liệu thuộc về tài sản trí tuệ của trường cần được lưu trữ, truy cập và sử dụng thích hợp để phục vụ công tác học tập, nghiên cứu.
- Dữ liệu có được do liên kết với các tổ chức bên ngoài như tổ chức y tế, chính trị, các viện nghiên cứu hoặc doanh nghiệp, cơ quan thương mại ngoài nước.
- Dữ liệu phát sinh do hoạt động nhà trường gồm các thông tin giáo viên, sinh viên, nhân viên, số liệu tài chính.

Bất kỳ dữ liệu riêng tư nào bị truy cập trái phép hoặc sử dụng sai mục đích cũng sẽ dẫn đến hậu quả không thể lường trước, một số ảnh hưởng có thể kể đến như:

- Danh tiếng:

- Pháp lý:
- Kinh tế:
- Hoạt động

1.3.2 Những loại hình tấn công dữ liệu

- *Xem trộm thông tin*
- *Thay đổi thông điệp*
- *Mạo danh*
- *Phát lại thông điệp*

1.3 GIẢI PHÁP ĐẢM BẢO AN TOÀN THÔNG TIN TRONG TRƯỜNG

Để dữ liệu trong trường được an toàn, mạng internet được ổn định lâu dài thì cán bộ quản lý hệ thống công nghệ thông tin trường học cần thực hiện tốt các nhiệm vụ sau:

- *Đánh giá rủi ro*
- *Xây dựng và thực hiện nghiêm túc*
- *Giám sát và báo cáo định kỳ*

1.3.1 Đánh giá rủi ro

Đánh giá rủi ro những dữ liệu quan trọng có thể chia thành ba nhóm giá trị sau:

- Dữ liệu sử dụng nội bộ:
- Dữ liệu liên quan đến pháp luật, các hợp đồng có hiệu lực
- Dữ liệu có giá trị kinh tế hoặc chính trị:

1.3.2 Xây dựng và thực hiện nghiêm túc các giải pháp quản trị dữ liệu, thiết lập các lớp an toàn mạng.

- Đánh giá, lường trước những rủi ro khi mất ATTT, có phương án phản ứng kịp thời.
- Đảm bảo không có kênh thông tin liên lạc không rõ ràng giữa các bộ phận nắm giữ, điều khiển dữ liệu quan trọng khác.
- Xem xét vai trò của kiểm toán nội bộ và bên ngoài để đánh giá hiệu quả công tác quản trị dữ liệu và quản lý an ninh mạng.
- Xem xét việc thành lập một ban quản trị chuyên duy trì giám sát, quản lý dữ liệu về thể chế và rủi ro an ninh mạng.

1.3.3 Giám sát và báo cáo định kỳ

- Phối hợp chặt chẽ giữa hiệu trưởng, chuyên gia nghiên cứu và nhân viên quản lý dữ liệu, an ninh mạng để hiểu rõ các mối đe dọa, kịp thời đưa ra giải pháp.

- Khuyến khích trao đổi giữa các phòng ban, xây dựng diễn đàn trường học, học hỏi kinh nghiệm để tăng cường hiểu biết các mối đe dọa đã từng gặp phải và cùng nhau phòng tránh hoặc tìm cách giải quyết.
- Đưa ra các chương trình đào tạo, liên kết giữa giáo viên và học sinh trong trường, tích hợp thực hành quản lý an toàn thông tin vào chương trình đào tạo.

1.3.4 Kiểm soát truy cập internet

Cán bộ quản lý CNTT của nhà trường cần đảm bảo hệ thống mạng được an toàn. Dưới đây là một số vấn đề cho máy chủ ứng dụng và dịch vụ:

- Đặt các máy chủ trong vùng DMZ
- Loại bỏ toàn bộ các dịch vụ không cần thiết khỏi máy chủ.
- Không cho phép quản trị hệ thống từ xa
- Giới hạn số người có quyền quản trị hay truy cập mức tối đa
- Tạo các log file theo dõi hoạt động của người sử dụng và duy trì các log file này trong môi trường được mã hóa.
- Hệ thống điều khiển log file thông thường được sử dụng cho bất kỳ hoạt đông nào.

1.3.5 Đảm bảo an toàn thông tin bằng phương pháp mật mã

- *Theo đường truyền*
- *Từ nút đến nút*

Vai trò của hệ mật mã.

- Dùng để che giấu nội dung của văn bản rõ
- Tạo các yếu tố xác thực thông tin.

CHƯƠNG 2. CÁC PHƯƠNG PHÁP MẬT MÃ ĐẢM BẢO TOÀN VẸN DỮ LIỆU

2.1 HỆ MẬT MÃ

2.1.1 Định nghĩa hệ mật mã

Một hệ mật mã là một bộ gồm 5 (P,C,K,E,D) thảo mãn các điều kiện sau:

- P (Plaintext) là một tập hợp hữu hạn các bản rõ và được gọi là không
- gian bản rõ.
- C (Ciphertext) là tập hữu hạn các bản mã được gọi là không gian các bản mã.
- K (Key) là tập hữu hạn các khóa hay còn gọi là không gian khóa. Đối với mỗi phần tử k của K được gọi là một khóa. Số lượng của không gian khóa phải lớn để không có đủ thời gian thử mọi khóa.
- E (Encrytion) là tập hợp các qui tắc mã hóa có thể.
- D (Decrytion) là tập hợp các qui tắc giải mã có thể.

2.1.2 Những yêu cầu đối với một hệ mật mã.

- *Độ tin cậy*:
- *Tính toàn vẹn*:
- *Không bị chối bỏ*:
- *Tính xác thực*:

2.2. HỆ MÃ KHÓA ĐỐI XỨNG

Phương pháp Ceasar là phương pháp mã hóa đơn giản nhất của mã hóa đối xứng. phương pháp mã hóa đối xứng được biểu diễn bằng mô hình sau:

Mô hình gồm 5 yếu tố:

- Bản rõ P (plaitext)
- Thuật toán mã hóa E (encrypt alorithm)
- Khóa bí mật K (secret key)
- Bản mã C (cipheetext)
- Thuật toán giải mã D (decrypt algorithm)

Trong đó: C = E (P,K)

P = D (C,K)

Mã hóa đối xứng có thể được phân thành hai loại:

- Loại thứ nhất tác động trên bản rõ theo từng nhóm bits.
- Loại thứ hai tác động lên bản rõ theo từng bits một.

Ưu nhược điểm mã hóa khóa đối xứng

- Ưu điểm

  Giải mã và mã hóa nhanh hơn hệ mã hóa khóa công khai.

- Nhược điểm

Vấn đề thỏa thuận khóa và quản lý khóa chung là khó khăn và phức tạp. Người gửi và người nhận phải luôn thống nhất với nhau về khóa. Việc thay đổi khóa là rất khó và dễ bị lộ. Khóa chung phải được gửi nhau trên kênh an toàn.

2.3 HỆ MÃ KHÓA BẤT ĐỐI XỨNG

2.3.1 Giới thiệu chung

Ý tưởng của hệ mật công khai được Diffie và Hellman đưa ra năm 1976. Còn việc thực hiện hệ mật công khai thì do Rivest, Shamir và Adleman đưa ra đầu tiên năm 1977, họ đề xuất hệ mật RSA[8]. Một số hệ mật khác được công bố sau đó, độ mật của chúng dựa trên bài tính toán khác nhau, như dựa trên độ khó của bài toán phân tích thành nhân tử như hệ mật RSA, dựa trên độ khó logarithm rời rạc như hệ mật Elgamal. Hay dựa trên đường cong Elliptic.

Ưu điểm và nhược điểm của hệ mã hóa khóa công khai

- Ưu điểm:

Đơn giản trong việc lưu chuyển khóa:

Mỗi người có một cặp khóa công khai – khóa bí mật

- Nhược điểm:

Mã hóa và giải mã chậm hơn hệ mã hóa khóa đối xứng.

2.3.2 Hệ mật RSA

Thuật toán được Ron Rivest, Adi Shamir và Len Adleman mô tả lần đầu tiên vào năm 1977 tại học viện công nghệ Masachusetts (MIT) [9]. Đây là thuật toán đầu tiên phù hợp với việc tạo ra chữ ký điện tử.

2.3.2.1 Nguyên tắc thực hiện của RSA

2.3.2.2 Sơ đồ

2.3.2.3 Ví dụ RSA

2.3.3 Hệ mật Elgama

Hệ mật Elgama hình thành trên cơ sở bài toán logarith rời rạc. Được đề xuất năm 1984, sau đó chuẩn chữ ký điện tử của Mỹ và Nga hình thành trên cơ sở hệ mật này.

2.3.3.1 Nguyên tắc hoạt động của khóa Elgama

2.3.3.2 Quá trình mã hóa bản tin

2.3.3.3 Quá trình giải mã

2.3.3.3 Ví dụ Elgama

2.4 CÁC PHƯƠNG PHÁP ĐẢM BẢO TÍNH TOÀN VẸN DỮ LIỆU BẰNG HÀM BĂM

2.4.1 Giới thiệu hàm băm mật mã

Khái niệm

Hàm băm mật mã là hàm toán học chuyển đổi một thông điệp có độ dài bất kỳ thành một dãy bits có độ dài cố định (tùy thuộc vào thuật toán băm). Dãy bits này được gọi là thông điệp rút gọn (message digest) hay giá trị băm (hash value), đại diện cho thông điệp ban đầu[6].

Tính chất cơ bản của hàm băm mật mã

- Giá trị băm của bất kỳ thông điệp nào có thể được tính toán một cách dễ dàng.
- Không thể suy ra thông điệp gốc của giá trị băm. Với thông điệp x thì dễ dàng tính được z = h(x), nhưng lại không thể suy ngược lại được x nếu chỉ có giá trị hàm băm h.
- Với thông điệp đầu vào x thu được bản băm z = H(x) là duy nhất.
- Không thể thay đổi một thông điệp nếu không thay đổi giá trị băm. Nếu dữ liệu trong thông điệp x thay đổi hay bị xóa để thành thông điệp x′ thì h(x´) ≠ h(x).
- Không tồn tại hai thông điệp khác nhau có giá trị băm như nhau (tính chất không xung đột).

Phân loại hàm băm mật mã

- *Hàm băm mật mã có khóa*
- *Hàm băm mật mã không khóa (có hàm băm dựa trên mật mã khối)*

Ý nghĩa của việc dùng thông điệp và hàm băm

2.4.2 Cấu trúc của hàm băm mật mã.

- *Tiền xử lý*
- *Thuật toán băm*

2.4.3 Hàm băm SHA (secure hash algorithm)

SHA hay thuật toán băm bảo mật là một họ những thuật toán băm mật mã do viện tiêu chuẩn và công nghệ Quốc gia (NIST) công bố thuộc tiêu chuẩn xử lý thông tin Liên Bang Hoa Kỳ (FIPS)[6,8,9]. Hiện tại có ba thuật toán SHA1, SHA2, SHA3 được định nghĩa.

Dưới đây các thuật toán băm SHA

- SHA 1
- SHA 2 (SHA - 224; SHA - 256; SHA - 384; SHA - 512)
- SHA 3 (SHA3 – 224; SHA3 – 256; SHA3 – 384; SHA3 – 512)

2.4.3.1. SHA1 & SHA2

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

Đối với SHA 384, SHA – 512 thông điệp mở rộng được phân tích thành N khối 1024 bits $M^{(1)}$, $M^{(2)}$,.., $M^{(N)}$. Do đó 1024 bits của khối dữ liệu ban đầu vào có thể được thể hiện bằng 16 từ 64 bits, $M_0^{(i)}$ chứa 64 bit đầu của khối thông điệp i, $M_1^{(i)}$ chứa 64 bits kế tiếp… $M_{16}^{(i)}$ chứa 64 bits cuối cùng.

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

2.4.3.2. Hàm băm SHA3

Trong tháng 11 năm 2007 Viện Tiêu Chuẩn và Công nghệ Quốc gia Mỹ (NIST) đã mở một cuộc thi để phát triển thuật toán hàm "băm" mới thay cho SHA2. Các thuật toán băm mới sẽ được gọi là Secure Hash Alorithm – 3 (SHA3) [10,11,12,13]. Có 56 trong đó 64 mẫu thiết kế đã tham gia cuộc thi SHA3, 51 mẫu đệ trình đã lọt qua vòng 1 và vào ngày 01 tháng 11 năm 2008, 14 mẫu đã lọt vào vòng 2. Chung kết thiết kế SHA -3 đã được công bố vào ngày 09 tháng 12 năm 2010. Các thuật toán cuối cùng được coi như một ứng cử viên thay thế cho SHA -3 lad BLAKE, Grostl, JH, Keccak và Skein. Các tiêu chí lựa chọn bao gồm việc thực thi trong cả phần mềm và phần cứng, dung lượng thực hiện phần cứng, phản ứng với những nguy cơ tấn công đã biết tốt nhất và đủ khác biệt với các ứng viên khác.

Trong tháng 10 năm 2012, Viện Tiêu Chuẩn và công nghệ (NIST) đã chọn các thuật toán Keccack như là tiêu chuẩn mới SHA – 3. Hàm băm được thiết kế bởi Guido Bertoni, Joan Daemen, Michael Peeters và Gilles van Assche. Các hoán vị cơ bản Keccak tạo điều kiện cho việc mở rộng các chức năng mã hóa hoán vị dựa trên hoán vị bổ sung.

Thuật toán SHA -3 bao gồm:

- Bốn dạng hàm băm mật mã là: SHA 3 -224, SHA3 – 256, SHA3 – 384, SHA3 – 512.
- Hai dạng hàm băm mở rộng là: SHAKE-128, SHAKE- 256.

1. Trạng thái Keccak

Trong phần này, các hoán vị Keccak – p được xác định với hai tham số:

- Độ dài cố định của chuỗi hoán vị được gọi là chiều rộng của hoán vị
- Số lần lặp lại của một chuyển đổi được gọi là một vòng.

SHA3 là tổ hợp các hàm sponge được đặc trưng bởi hai tham số, tốc độ r bits và cường độ an toàn c. Tổng, r+c xác định độ rộng của hàm băm SHA3. Phép hoán vị được sử dụng trong việc xây dựng Sponge và giới hạn giá tị cực đại là 1600.

Chiều rộng được biểu thị bởi b và số vòng được biểu thị bởi n_r. Các Keccak – p hoán vị với số vòng là n_r và chiều rộng b được ký hiệu Keccak – p[b n_r].

Mỗi hàm nén Keccak là duy nhất bao gồm 24 dạng viên đạn và mỗi vòng được chia thành năm bước là: $\boldsymbol{\theta(A)}$**, Rho (ρ) và Pi (π), Chi(X), Iota(i) (***sẽ tương ứng với 5 thuật toán sẽ trình bày bên dưới*)

a. Thành phần của mảng trạng thái hàm băm SHA3
b. Chuyển dạng chuỗi thành dạng mảng các trạng thái
c. Chuyển mảng trạng thái thành dạng chuỗi

2. Đặc tả thuật toán chuyển trạng thái của Keccak –p[b,n_r]

a) Đặc tả thuật toán theta $\theta(A)$
b) Đặc tả thuật toán 2 Rho ρ(A)
c) Đặc tả thuật toán pi (π)
d) Thuật toán 4 Chi(X);
e) Thuật toán 5 (Iota): j(A,i_r)

3. Xây dựng Sponge.

Xây dựng sponge là một khuân khổ để xác định các hàm dạng nhị phân với độ dài đầu ra tùy ý. Việc xây dựng sử dụng ba thành phần sau:

- Hàm cơ bản về chuỗi có chiều dài cố định, kí hiệu là *f*.
- Một tham biến tốc độ, kí hiệu là *r*.
- Một quy tắc chêm/thêm, kí hiệu là *pad*.

Xây dựng sponge

2.5. CÁC PHƯƠNG PHÁP ĐẢM BẢO TÍNH TOÀN VẸN BẰNG MÃ XÁC THỰC

2.5.1 Xác thực thông điệp

2.5.2 Phân loại mã xác thực

- *Tiêu chuẩn thứ nhất là mã xác thực thông điệp sử dụng hàm một chiều có khóa HMAC* (Keyd-Hash Messasge Authentication Code).

- *Chuẩn thứ hai NIST đưa ra là mã xác thực thông điệp mã hóa* (Cipher Message Authentication Code- CMAC).

2.5.3 Mã xác thực thông điệp mã hóa (CMAC – CBC MAC)

2.5.3.1 An toàn CMAC

2.5.3.2 Khởi tạo, mô tả cài đặt CMAC

2.5.4 Mã xác thực thông điệp sử dụng hàm một chiều

2.5.4.1 Thiết kế HMAC

2.5.4.2.Thuật toán

2.5.5 Ứng dụng hàm MAC trên thực tế

2.5.5.1 Chống tấn công lặp

- Sử sụng Tem thời gian
- Sử dụng con đếm

2.5.5.2 **Sử dụng MAC**

- CMAC dựa trên mã khối nhưng với đầu vào nhỏ (so với hash) và đầu ra ngắn gọn, thời gian trễ cho tính toán nhỏ.
- HMAC thắng thế khi áp dụng cho thông điệp kích thước lớn

2.5.5.3 Thứ tự thực hiện mã hóa và MAC

- Mã hoá trước, MAC sau
- MAC trước, mã hoá sau

2.6 CHỮ KÝ SỐ

2.6.1 Chữ ký điện tử

Chữ ký số là một cơ chế xác thực cho phép người tạo thông tin dùng khóa riêng của mình để xử lý khối thông tin theo một thuật toán nào đó giúp người nhận thông tin kiểm chứng được tính toàn vẹn về nội dung và nguồn gốc thông tin.

2.6.2 Chữ ký số

Chữ ký số "digital signature" là một dạng chữ ký điện tử được tạo ra bằng sự biến đổi một thông điệp có sử dụng hệ mật mã khóa công khai, theo đó người có thông điệp ban đầu và khóa công khai của người ký có thể xác thực được chữ ký số vừa ký

Định nghĩa: [5]Sơ đồ chữ ký bao gồm các thành phần sau

1. Không gian bản rõ M.

2. Không gian chữ ký S.

3. Không gian khóa K để tạo nên chữ ký, không gian khóa K' để kiểm tra chữ ký.

4. Thuật toán hiệu quả để tạo nên khóa Gen: $N \rightarrow K \times K'$, ở đây K và K' tương ứng với không gian khóa mật và khóa công khai

5. Thuật toán tạo chữ ký Sing: $M \times K \rightarrow S$.

6. Thuật toán kiểm tra chữ ký Verfy: $M \times K \times K' \rightarrow \{True, False\}$.

Đối với bất kỳ khóa tọa chữ ký $sk \in K$ và bất kỳ bản tin $m \in M$ lệnh ký bức điện được ký hiệu:

$$s \leftarrow Sign_{sk}(m).$$

Đối với bất kỳ khóa mật của chữ ký $k \in K$, tương ứng với khóa công khai để kiểm tra chữ ký $sk \in K'$, bất kỳ bản tin $m \in M$ và chữ ký $s \in S$ cần thõa mãn điều kiện sau:

Chức năng của chữ ký điện tử:

Xác thực được nguồn gốc tài liệu

Tính toán vẹn dữ liệu

Chống từ chối bức điện

Các chức năng tấn công đối với chữ ký điện tử:

1. Tội phạm có thể giả mạo chữ ký tương ứng với văn bản đã chọn.
2. Tội phạm thử chọn bức điện tương ứng với chữ ký đã cho.
3. Tội phạm có thể ăn trộm khóa mật và có thể ký bất kỳ một bức điện nào nó muốn giống như chủ của khóa mật.
4. Tội phạm có thể dã mạo ông chủ ký một bức điện nào đó.
5. Tội phạm có thể đổi khóa công khai bởi khóa của mình.

2.6.3 Cách tạo chữ ký số

2.6.3.1 Quy trình tạo chữ ký số

Dùng giải thuật băm để thay đổi thông điệp cần truyền đi, kết quả ta được một message digest (MD), sử dụng khóa bí mật người gửi để mã hóa thông điệp thu được.

2.6.3.2 Quy trình kiểm tra chữ ký

Dùng public key của người gửi để giải mã chữ ký số của thông điệp.

Dùng giải thuật SHA băm thông điệp đính kèm.

So sánh kết quả thu được ở trên, nếu thấy trùng nhau ta kết luận thông điệp này không bị thay đổi trong quá trình truyền và thông điệp này là của người gửi.

Chữ ký số (digital signature) được tạo ra bằng sự biến đổi một thông điệp sử dụng hệ thống mật mã công khai, theo đó người có thông điệp dữ liệu ban đầu và khóa công khai của người ký có thể xác định được.

2.6.3.3 Thuật toán chữ ký số

Yêu cầu chữ ký số:

- Chữ ký phải dựa vào thông điệp được ký.
- Chứa thông tin duy nhất của người gửi để tránh giả mạo.
- Dễ nhận diện và xác nhận chữ ký số.
- Khó khăn giả mạo chữ ký.

Đặc điểm của chữ ký số:

- Tính xác thực: bảo đảm người ký là người tạo ra nó.
- Tính an toàn: Không thể giả chữ ký số nếu như không biết thông tin bí mật tạo chữ ký.
- Không thể dùng lại: một chữ ký số không thể dùng cho một tài liệu khác.
- Tính hiệu quả: ký và xác minh nhanh chóng dễ dàng.

2.6.4 Sơ đồ chữ ký số RSA

Tạo khóa:

Tạo chữ ký

Để tạo ra chữ ký số của bức điện $m \in Z_N^*$ người gửi tạo ra số

$$S = Sign_d\ (m) \leftarrow m^d\ (mod\ N).$$

Thẩm tra chữ ký:

Để thẩm tra chữ ký S, người nhận kiểm chứng bằng thủ tục

$$Verify_{(N,b)}(m, s) = true, nếu\ như\ m \equiv s^b \text{ (mod N)}$$

2.6.4.1 Độ an toàn của sơ đồ chữ ký số RSA

- *Ký trước, Mã hóa sau:*
- *Mã hóa trước, Ký sau:*

CHƯƠNG 3: ỨNG DỤNG CHỮ KÝ ĐIỆN TỬ ĐẢM BẢO TÍNH TOÀN VẸN DỮ LIỆU TRONG TRƯỜNG HỌC

3.1. Thực trạng quy trình ra đề thi và bảo mật thông tin đề thi các trường ĐH - CĐ.

a) Quy trình biên soạn, duyệt, quản lý, sao in và sử dụng đề thi

b) Biên soạn đề thi và đáp án

c) Duyệt đề thi và bàn giao cho phòng KT&KĐCLGD

d) Sao in đề thi và quản lý đề thi

e) Bàn giao đề thi cho Ban coi thi

f) Sử dụng đề thi

g) Điều khoản thi hành

3.2. Yêu cầu giải pháp quản lý đề thi theo phương pháp hiện đại.

3.3. Quá trình ký và xác thực ký số

3.3.1. Tạo và trao đổi khóa

Các thành phần của chương trình:

1. Thông điệp ban đầu: P

2. Khóa bí mật K_R dùng trong quá trình giải hóa

3. Khóa công khai K_u dùng trong quá trình mã hóa.

4. Bản mã C và được trao đổi thông qua ường truyền tin

3.3.2. Quá trình tạo chữ ký số

Bước 1: Dữ liệu ban đầu sử dụng hàm băm để nén dữ liệu thành "giá trị băm" để truyền đi.

Sử dụng khóa private key (khóa bí mật) của người gửi để mã hóa "giá trị băm" thu được ở bước 1. Kết quả thu được gọi là chữ ký điện tử của thông điệp ban đầu.

Bước 2: Dữ liệu ban đầu cùng với khóa công khai của người gửi để mã hóa thu được "giá trị mã hóa".

Bước 3: Gộp "chữ ký điện tử" thu được bước 1 vào "giá trị mã hóa" thu được bước 2. Công việc này gọi là "ký nhận" vào dữ liệu. Mọi sự phát hiện trong giai đoạn kiểm tra.

3.3.3. Quá trình xác thực chữ ký

Bước 1: Sử dụng khóa công khai của A giải mã "chữ ký điện tử" thu được "giá trị băm".

Bước 2: Sử dụng khóa bí mật B để giải mã "giá trị mã hóa", sau đó sử dụng hàm băm để tính toán chuỗi đại diện thu được "giá trị băm".

Bước 3: So sánh hai "giá trị băm" của bước 1 và bước 2 trên xem thông điệp có toàn vẹn hay không.

- Nếu toàn vẹn, người nhận B chấp nhận thông điệp. Chữ ký thành công
- Nếu không toàn vẹn, người nhận B có thể bỏ qua thông điệp

3.4. Chương trình demo

3.4.1. Giới thiệu chương trình

Chương trình xây dựng gồm 2 modul chính:

Demo thuật toán băm SHA3 (SHA3- 224; SHA3 – 256; SHA3 -384; SHA3-512)

Demo chữ ký số lên đề thi

3.4.3. Hình ảnh Demo chữ ký số áp dụng trong quản lý đề thi

A. Tạo khóa K

- Chọn 2 số nguyên tố đủ lớn
- tính được khóa công khai và khóa bí mật

B. Thủ tục ký văn bản:

1. Tải văn bản
2. Ký
3. Lưu chữ ký.

C. Xác thực chữ ký

1. Tải văn bản
2. Tải chữ ký
3. Xác nhận chữ ký
4. Báo lỗi khi chữ ký không đúng/ hoặc văn bản sai.

KẾT LUẬN

1. Các kết quả đạt được:

Để đảm bảo tính toàn vẹn dữ liệu là bài toán lớn trong trường học nói chung và trường học thông minh nói riêng. Việc sử dụng rộng rãi văn bản, tài liệu điện tử cùng với các đặc điểm của nó như: dễ dàng thay đổi nội dung thông tin trong tài liệu mà không để lại dấu vết, vấn đề xác định người gửi văn bản điện tử v.v... đã dẫn đến sự cần thiết phải tìm giải pháp cho các vấn đề trên. Luận văn nêu ra một số biện pháp để đảm bảo tính toàn vẹn của văn bản điện tử như: *Thứ nhất,* đảm bảo toàn vẹn dữ liệu bằng thuật toán băm SHA; *thứ hai,* đảm bảo toàn vẹn dữ liệu bằng một số phương pháp mã xác thực; *Thứ ba,* đảm bảo toàn vẹn dữ liệu bằng chữ ký số. Việc ứng dụng chữ ký số vào cơ quan trường học sẽ giúp quá trình luân chuyển văn bản được nhanh chóng, chính xác, kịp thời, không chối bỏ, quá trình xử lý và triển khai công việc không bị gián đoạn, giảm thiểu thời gian giải quyết công việc.

a. Lý thuyết:

- Để đảm bảo toàn vẹn dữ liệu cho các cơ quan nhà nước, trường học, các doanh nghiệp,... luận văn đã nghiên cứu các phương pháp toàn vẹn dữ liệu như:
  - Nghiên cứu các họ hàm băm mật mã SHA (SHA1,SHA2,SHA3). Trong đó nghiên cứu hàm băm SHA3 – Keccak do nhóm các nhà mật mã người Bỉ đứng đầu là Daemen (người đồng tác giả của thuật toán AES) thiết kế. Keccak có số vòng lặp là 18 vòng và kích thước trạng thái thay đổi lần lượt là 25, 50, 100, 200, 400, 800, 1600.

Nhóm thiết kế Keccak đã đưa vào cấu trúc Sponge, bên cạnh cấu trúc Sponge nhóm tác giả còn thực hiện các biện pháp như bổ sung khóa mật vào đầu vào của keccak biến nó thành mã xác thực thông báo.

SHA3 bao gồm bốn hàm băm SHA3 – 224, SHA3-256, SHA3-384, SHA3-512 và hai hàm mở rộng SHAKE128 và SHAKE256.

- Nghiên cứu các phương pháp đảm bảo tính toàn vẹn bằng mã xác thực. Có hai dạng chuẩn mà NIST đưa ra "mã xác thực thông điệp sử dụng hàm một chiều có khóa HMAC" và " mã xác thực thông điệp mã hóa". Ứng dụng MAC là đảm bảo tính xác thực giữa các bên trong kênh liên lạc có thể gửi và nhận thông điệp được xác thực với nhau và khả năng bị kẻ tấn công giả mạo là rất thấp.

- Nghiên cứu về chữ ký số có nhiều loại sơ đồ chữ ký số khác nhau, trong luận văn này tôi sử dụng sơ đồ chữ ký thông dụng là RSA. Chữ ký số chức năng là xác thực được nguồn gốc tài liệu, tính toàn vẹn dữ liệu và tính chống từ chối bức thông điệp.

b. Thực nghiệm:

- Chương trình xây dựng gồm 2 modul chính: "demo thuật toán SHA3 và demo chữ ký số".
  - Demo các thuật toán băm SHA3 (SHA3-224, SHA3-256, SHA3-384, SHA3-512)
  - Demo chữ ký số lên đề thi.

2. Hướng nghiên cứu tiếp theo

Học viên sẽ phát triển ứng dụng các phương pháp mật mã vào các thuật toán mới và đảm bảo an toàn dữ liệu nói chung toàn vẹn dữ liệu nói riêng.

Tài liệu tham khảo

Tài liệu tiếng Việt

[1]. Phan Đình Diệu, "Lý thuyết mật mã và an toàn thông tin", Đại Học Quốc Gia Hà Nội, năm 2002.

[2]. Phạm Huy Điển, Hà Huy Khoái (2004), Mã hóa thông tin cơ sở toán học và ứng dụng, Viện toán học.

[3]. Trịnh Nhật Tiến (2009), "Bài giảng về mật mã và An toàn dữ liệu", Trường Đại học Công nghệ, Đại học Quốc gia Hà Nội.

[4]. TCVN 7635:2007, *Chữ ký số, kỹ thuật Mật mã*, 2007

[5]. Hàm băm an toàn và ứng dụng, *Luận văn ths Nguyễn Thanh Hưng, Đại học Quốc gia Hà Nội*

[6]. Giáo trình mã hóa và ứng dụng của nhóm tác giả TS. Dương Anh Đức – Ths Trần Minh Triết cùng cới nhóm SV, trường Đại học Khoa học Tự nhiên, Đại học Quốc gia TP Hồ Chí Minh.

Tài liệu tiếng Anh

[7] Design of SHA-3 Algorithm using Compression Box (3200 bit) for Digital Signature Applications

[8]. Secure Hash Algorithm-3(SHA-3) implementation on Xilinx FPGAs, Suitable for IoT Applications. Group of author Muzaffar Rao, Thomas Newe and Ian Grout University of Limerick, Ireland muhammad.rao @ ul.ie, thomas.newe @ ul.ie, Ian.grout @ ul.ie

[9] R.L. Rivest, A. Shamir, and L. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM, 21 (2), trang 120-126, Feb 1978.

[10]. Keccak-reference-3.0. Guido Bertoni[1],Joan Daemen[1], Michael Peters[2], Gilles Van Assche[1].

[11]. Introduction to SHA-3 and Keccak, Joan Daemen STMicroelectronics and Radboud University **,**Crypto summer school 2015, Šibenik, Croatia, May 31 - June 5, 2015

[12]. N. F. Pub, "FIPS PUB 202. SHA-3 Standard: Permutation Based Hash and Extendable-Output Functions," *Federal Information Processing Standards Publication*, 2015.

[13] Introduction to Network Security Missouri S&T University CPE 5420 Data Integrity Algorithms.

[14]Design of SHA-3 Algorithm using Compression Box (3200 bit) for Digital Signature Applications

[15] Cryptography and Network Security, Fourth Edition – William Stallings