ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

NGUYỄN THỊ HẰNG

NGHIÊN CỨU BÀI TOÁN AN TOÀN THÔNG TIN CHO DOANH NGHIỆP VỪA VÀ NHỎ

Ngành: Công nghệ thông tin
Chuyên ngành: Quản lý Hệ thống thông tin
Mã số: Chuyên ngành đào tạo thí điểm

TÓM TẮT LUẬN VĂN THẠC SĨ CÔNG NGHỆ THÔNG TIN

Hà Nội - 2017

LUẬN VĂN ĐÃ ĐƯỢC HOÀN THÀNH TẠI TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

Người hướng dẫn khoa học: **TS. Lê Phê Đô – TS. Phùng Văn Ổn**

Phản biện 1: TS. Nguyễn Ngọc Cương

Phản biện 2: TS. Nguyễn Long Giang

Luận văn được bảo vệ trước Hội đồng chấm luận văn thạc sĩ
tại trường Đại học Công Nghệ
Vào hồi: 8:00 ngày 11 tháng 8 năm 2017

Có thể tìm hiểu luận văn tại:

Trung tâm thông tin Thư viện Đại học Quốc gia Hà Nội

MỞ ĐẦU

1. Tính cấp thiết của đề tài

Trong nền kinh tế tri thức, thông tin đã trở thành một vấn đề sống còn đối với mọi lĩnh vực của đời sống kinh tế - xã hội đặc biệt là trong quản lý kinh tế, nó quyết định sự thành bại của các doanh nghiệp trên thương trường nếu họ biết sử dụng sao cho đạt hiệu quả nhất. Ứng dụng CNTT giúp các doanh nghiệp nắm bắt thông tin một cách chính xác kịp thời, đầy đủ, góp phần nâng cao hiệu quả kinh doanh, sức cạnh tranh với thị trường trong và ngoài nước.

Tuy nhiên, cùng với sự phát triển nhanh chóng của các lĩnh vực công nghệ thì nguy cơ mất an toàn thông tin cũng là một vấn đề bức thiết đối với các doanh nghiệp khi gần đây xảy ra rất nhiều cuộc tấn công mạng, tấn công bởi các hacker với mức độ và hậu quả nghiêm trọng.

Theo số liệu của phòng Công nghiệp và Thương mại Việt Nam, lực lượng doanh nghiệp vừa và nhỏ Việt Nam hiện chiếm gần 98% tổng số doanh nghiệp trên cả nước, phát triển đa dạng các ngành nghề, lĩnh vực. Mỗi ngành nghề, lĩnh vực đòi hỏi thông tin trong đó cần phải được bảo mật, xác thực và toàn vẹn. Bảo đảm an toàn thông tin vừa giúp doanh nghiệp phát triển, vừa giúp doanh nghiệp có được hình ảnh uy tín, được các bên đối tác đánh giá và tin tưởng khi hợp tác.

Xuất phát từ thực tế đó, học viên đã chọn đề tài **"Nghiên cứu bài toán an toàn thông tin cho doanh nghiệp vừa và nhỏ"** làm luận văn thạc sĩ của mình nhằm góp phần giúp các DNVVN có thêm một số giải pháp quản lý, bảo vệ thông tin an toàn, hiệu quả.

2. Mục tiêu nghiên cứu

Trên cơ sở làm rõ những vấn đề lý luận và thực tiễn về **an toàn thông tin số**; sau khi phân tích đặc điểm hệ thống thông tin của các DNVVN, thực trạng an toàn thông tin trên thế giới và tại Việt Nam, học viên tìm hiểu một số hệ mật mã đảm bảo an toàn thông tin hiện đang được sử dụng phổ biến, đề xuất một số giải pháp giúp các DNVVN đảm bảo an toàn thông tin; đáp ứng yêu cầu doanh nghiệp Việt Nam hội nhập ngày càng sâu rộng và thành công vào nền kinh tế khu vực và thế giới.

3. Nội dung nghiên cứu

Ngoài phần mở đầu và kết luận, nội dung luận văn bao gồm:

Chương 1: Bài toán an toàn thông tin cho DNVVN.

Chương 2: Các hệ mật mã đảm bảo an toàn thông tin được dùng phổ biến hiện nay.

Chương 3: Một số giải pháp đảm bảo an toàn thông tin cho DNVVN.

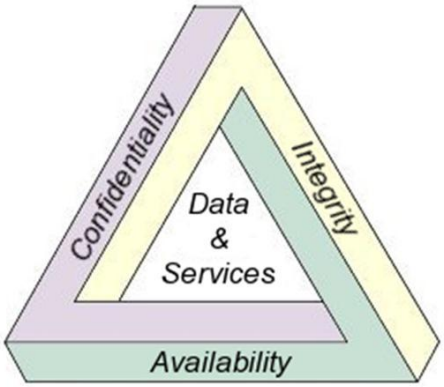
Chương 4: Cài đặt và thử nghiệm chữ ký số đảm bảo ATTT trong việc ký kết hợp đồng điện tử cho DNVVN.

CHƯƠNG 1: BÀI TOÁN AN TOÀN THÔNG TIN CHO DNVVN

1.1. Cơ sở lý luận về an toàn thông tin

1.1.1. An toàn thông tin

Các yếu tố đảm bảo an toàn thông tin



Hình 1. 1. Đặc tính cơ bản của an toàn thông tin

Tính bảo mật: Là tâm điểm chính của mọi giải pháp an toàn cho sản phẩm/hệ thống CNTT.

Tính toàn vẹn: Không bị sửa đổi là đặc tính phức hợp nhất và dễ bị hiểu lầm của thông tin.

Tính sẵn sàng: Đảm bảo độ sẵn sàng của thông tin, tức là thông tin có thể được truy xuất bởi những người được phép vào bất cứ khi nào họ muốn.

Các nguy cơ mất an toàn thông tin

- ***Mối đe doạ phá vỡ tính toàn vẹn*** là dữ liệu khi truyền đi từ nơi này đến nơi khác, hay đang lưu trữ có nguy cơ bị thay đổi, sửa chữa làm sai lệch nội dung thông tin.

- ***Mối đe doạ phá vỡ tính sẵn sàng*** là hệ thống mạng có nguy cơ rơi vào trạng thái từ chối phục vụ, khi mà hành động cố ý của kẻ xấu làm ngăn cản tiếp nhận tới tài nguyên của hệ thống;

1.1.2. Tấn công luồng thông tin trên mạng

Luồng thông tin được truyền từ nơi gửi (nguồn) đến nơi nhận (đích). Trên đường truyền công khai, thông tin bị tấn công bởi những người không được uỷ quyền nhận tin (gọi là kẻ tấn công).

1.1.3. Phân loại các kiểu tấn công luồng thông tin trên mạng

Các kiểu tấn công luồng thông tin trên được phân chia thành hai lớp cơ bản là tấn công bị động (passive attacks) và chủ động (active attacks)

Tấn công bị động

Là kiểu tấn công chặn bắt thông tin như nghe trộm và quan sát truyền tin. Mục đích của kẻ tấn công là biết được thông tin truyền trên mạng.

Tấn công chủ động

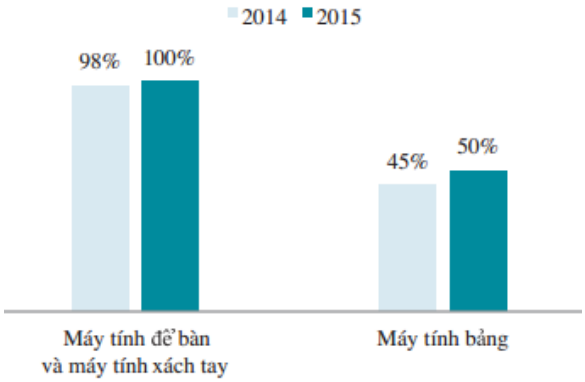
Là kiểu tấn công sửa đổi dòng dữ liệu hay tạo ra dòng dữ liệu giả. Tấn công chủ động được chia thành các loại nhỏ sau:

1.2. Thực trạng ATTT đối với các DNVVN

1.2.1. Đặc điểm hệ thống thông tin của các DNVVN

Về hạ tầng kỹ thuật

Hạ tầng kỹ thuật bao gồm các thiết bị CNTT như máy tính, máy in, các thiết bị trực tiếp xử lý thông tin và mạng máy tính.

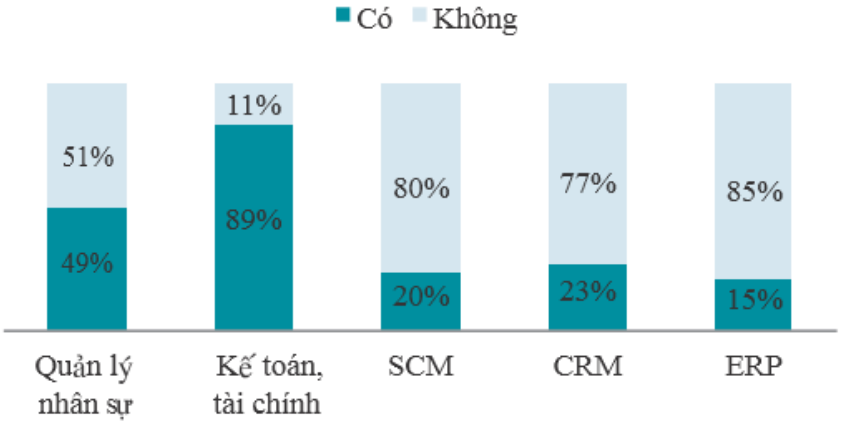


Hình 1. 2. Tỷ lệ máy tính trong doanh nghiệp [3]

Mạng và kết nối Internet là điều kiện kỹ thuật cơ sở để doanh nghiệp ứng dụng CNTT trên toàn bộ doanh nghiệp và tham gia thị trường thương mại điện tử, hiện đã có 98% số doanh nghiệp tham gia khảo sát đã kết nối Internet.

Về ứng dụng CNTT trong hoạt động quản lý điều hành [3]

Hầu hết các DNVVN mới chỉ sử dụng các phần mềm phục vụ tác nghiệp đơn giản như thư điện tử, phần mềm văn phòng, ngoài ra còn có hai phần mềm được sử dụng phổ biến là phần mềm kế toán, tài chính (89%) và quản lý nhân sự (49%).

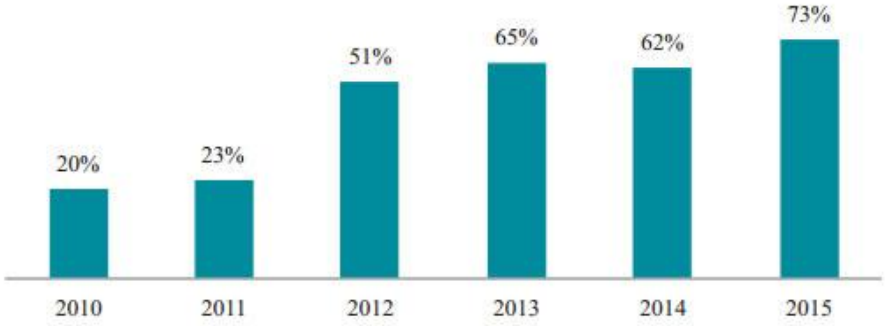


Hình 1. 3. Tỷ lệ ứng dụng phần mềm trong DNVVN

Bên cạnh việc ứng dụng các phần mềm phục vụ tác nghiệp kể trên, các DNVVN cũng đã thiết lập website vào trong hoạt động sản xuất kinh doanh phổ biến hơn.

Về nguồn nhân lực phụ trách CNTT

Tỷ lệ doanh nghiệp có cán bộ chuyên trách về CNTT và TMĐT tăng qua các năm, từ 20% năm 2010 lên 73% năm 2015.

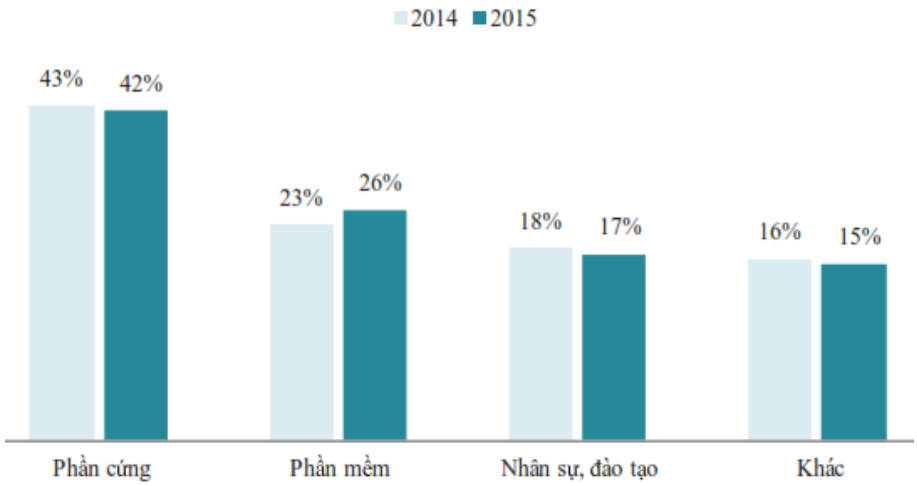


Hình 1. 4. Tỷ lệ DNVVN có cán bộ chuyên trách về CNTT qua các năm [3]

Tuy nhiên việc tuyển dụng ***nhân sự có kỹ năng về CNTT thì lại gặp khó khăn***, kết quả khảo sát trong 3 năm gần đây cho thấy tỷ lệ này có chiều hướng giảm, từ 29% năm 2013 xuống còn 24% năm 2015.

Về cơ cấu chi phí cho hạ tầng CNTT trong doanh nghiệp

Chi phí cho hạ tầng công nghệ thông tin trong doanh nghiệp tương tự nhau qua các năm. Năm 2015, phần cứng vẫn chiếm tỷ trọng đầu tư cao nhất (42%), tiếp đến là phần mềm (26%), nhân sự và đào tạo (17%).



Hình 1. 5. Cơ cấu chi phí cho hạ tầng công nghệ thông tin [3]

Số liệu tổng hợp cho thấy, do quy mô về nguồn nhân lực và vốn, **hệ thống thông tin của các DNVVN so với các doanh nghiệp lớn còn nhiều hạn chế**:

Các DNVVN không thể đầu tư có chiều sâu vào các ứng dụng CNTT cũng như hệ thống mạng an toàn. Các phần mềm mang tính đồng bộ, an toàn, hiệu quả như ERP là "bài toán khó" đối với các doanh nghiệp.

Về mặt nhân sự CNTT, các DNVVN chưa đầu tư một cách lâu dài, chưa có các cán bộ chuyên trách đảm nhiệm vai trò an toàn thông tin, việc đào tạo ý thức ATTT cho toàn bộ người dùng của các DNVVN gần như chưa được triển khai.

Bên cạnh đó, nhiều doanh nghiệp không biết cách thiết lập một quy trình chuẩn và các biện pháp bảo vệ hệ thống của mình.

Do đó, việc nghiên cứu các giải pháp đảm bảo ATTT cho các doanh nghiệp vừa và nhỏ là vấn đề cấp thiết

1.2.2. Thực trạng ATTT thế giới

Năm 2016 tình hình tấn công mạng trên thế giới gia tăng đáng kể, có diễn biến rất phức tạp và khó đoán trước, hàng loạt công ty bị đánh cắp tài khoản người dùng, trong đó nổi bật là vụ đánh cắp người dùng tại Yahoo tháng 12/2016.

Năm 2016 cũng là năm mã độc tống tiền - Ransomware trở thành vấn nạn

Ngoài ra tấn công mạng bằng mã độc lây nhiễm trên thiết bị IoT cũng xảy ra tràn lan

1.2.3. Thực trạng ATTT đối với các doanh nghiệp Việt Nam

Theo khảo sát của Hiệp hội An toàn thông tin Việt Nam, chỉ số ATTT của Việt Nam trong năm 2016 là 59,9%. Đây là bước tiến đáng kể trong những năm qua, bởi năm 2015, con số này là 47,4%.

1.3. Bài toán an toàn thông tin cho DNVVN

1.3.1. Các nguy cơ mất ATTT đối với DNVVN

Nguy cơ mất an toàn thông tin về khía cạnh vật lý

Nguy cơ mất an toàn thông tin về khía cạnh vật lý là nguy cơ do mất điện, nhiệt độ, độ ẩm không đảm bảo, hỏa hoạn, thiên tai, thiết bị phần cứng bị hư hỏng, các phần tử phá hoại như nhân viên xấu bên trong và kẻ trộm bên ngoài.

Nguy cơ bị mất, hỏng, sửa đổi nội dung thông tin:

Người dùng có thể vô tình để lộ mật khẩu hoặc không thao tác đúng quy trình tạo cơ hội cho kẻ xấu lợi dụng để lấy cắp hoặc làm hỏng thông tin.

Nguy cơ bị tấn công bởi các phần mềm độc hại

Các phần mềm độc hại tấn công bằng nhiều phương pháp khác nhau để xâm nhập vào hệ thống với các mục đích khác nhau như: virus, sâu máy tính (Worm), phần mềm gián điệp (Spyware),...

Nguy cơ xâm nhập từ lỗ hổng bảo mật

Lỗ hổng bảo mật thường là do lỗi lập trình, lỗi hoặc sự cố phần mềm, nằm trong một hoặc nhiều thành phần tạo nên hệ điều hành hoặc trong chương trình cài đặt trên máy tính.

Nguy cơ xâm nhập do bị tấn công bằng cách phá mật khẩu

Quá trình truy cập vào một hệ điều hành có thể được bảo vệ bằng một khoản mục người dùng và một mật khẩu.

Nguy cơ mất ATTT do sử dụng e-mail

Tấn công có chủ đích bằng thư điện tử là tấn công bằng email giả mạo giống như email được gửi từ người quen, có thể gắn tập tin đính kèm nhằm làm cho thiết bị bị nhiễm virus

Nguy cơ mất ATTT với website

Về mặt kỹ thuật, các website của các DNVVN tồn tại những lỗ hổng nghiêm trọng cho phép xâm nhập và chiếm quyền điều khiển. Các lỗ hổng thường gặp như: SQL Injection, Cross-site Scripting, Upload....

Nguy cơ mất ATTT do kỹ nghệ xã hội

Các nghiên cứu trong lĩnh vực kỹ nghệ xã hội đã chỉ ra rất nhiều điểm yếu của con người mà giới đạo chích có thể tận dụng để thực hiện các hành vi lừa đảo. Nhưng ngay

cả những phẩm chất tốt như lòng nhân ái, sự hào hiệp, sự chân thực cũng là kẽ hở để đạo chích lợi dụng. Vì vậy, ngoài việc nắm kiến thức chung về phẩm chất của con người, giới kỹ sư xã hội rất chú trọng phân biệt đặc tính của từng kiểu người được hình thành do nghề nghiệp.

1.3.2. Những tổn thất của DNVVN trước những nguy cơ mất ATTT

Có rất nhiều tổn thất có thể xảy ra, có thể được phân thành các loại sau:

1. DNVVN có thể bị phá sản;
2. Doanh nghiệp có thể bị ngừng kinh doanh;
3. Tổn thất về tài chính;
4. Trách nhiệm pháp lý;

…..

1.3.3. Danh mục các tài sản thông tin của DNVVN cần được bảo vệ [10]

Tài sản thông tin của doanh nghiệp là những thứ mà doanh nghiệp cần bảo vệ về mặt ATTT bao gồm 02 dạng tài sản dữ liệu và tài sản dịch vụ.

Tài sản dữ liệu

Dưới đây là danh sách các tài sản dữ liệu phổ biến tại các DNVVN

Tài sản dịch vụ

Tài sản dịch vụ bao gồm các dịch vụ cung cấp trực tiếp cho khách hàng

Tài sản dữ liệu và tài sản dịch vụ có mối liên hệ chặt chẽ với nhau, ví dụ như dịch vụ **lương** phụ thuộc vào dữ liệu **hồ sơ nhân sự, mức lương, thời gian làm việc**, vv.

CHƯƠNG 2: CÁC HỆ MẬT MÃ ĐẢM BẢO ATTT ĐƯỢC DÙNG PHỔ BIẾN HIỆN NAY

2.1. Tổng quan về hệ mật mã

2.1.1. Định nghĩa

Hệ mật mã [7] được định nghĩa bởi bộ năm (P, C, K, E, D), trong đó:

P: là tập hữu hạn các bản rõ có thể

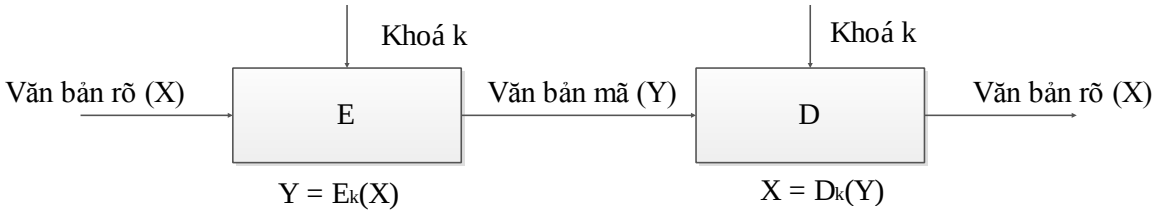
C: là tập hữu hạn các bản mã có thể

K: là tập hữu hạn các khoá có thể

E: là tập hữu hạn các hàm lập mã

D: là tập các hàm giải mã.

Với mỗi k ∈ K có một hàm lập mã $e_k \in E, e_k : \mathrm{P} \rightarrow \mathrm{C}$ và một hàm giải mã $d_k \in D, d_k: C \rightarrow P$ sao cho $d_k(e_k(x)) = x$ với $\forall x \in P$



Hình 2. 1. Quá trình mã hoá và giải mã

2.1.2. Phân loại các hệ mật mã

Hệ mật mã có nhiều loại nhưng chia làm hai loại chính: Hệ mật mã khoá đối xứng và Hệ mật mã khoá công khai.

2.1.3. Một số khái niệm cơ bản về sử dụng mật mã [6].

1. **Bản rõ** X được gọi là là bản tin gốc. Bản rõ có thể được chia nhỏ có kích thước phù hợp.
2. **Bản mã** Y là bản tin gốc đã được mã hoá. Ở đây ta thường xét phương pháp mã hóa mà không làm thay đổi kích thước của bản rõ, tức là chúng có cùng độ dài.
3. **Khoá** K là thông tin tham số dùng để mã hoá, chỉ có người gửi và người nhận biết. Khóa là độc lập với bản rõ và có độ dài phù hợp với yêu cầu bảo mật.
4. **Mã hoá** là quá trình chuyển bản rõ thành bản mã, thông thường bao gồm việc áp dụng thuật toán mã hóa và một số quá trình xử lý thông tin kèm theo.
5. **Giải mã** chuyển bản mã thành bản rõ, đây là quá trình ngược lại của mã hóa.

2.2. Hệ mật AES [9]

2.2.1. Giới thiệu

AES (Advanced Encryption Standard - Tiêu chuẩn mã hóa nâng cao) được thiết kế bởi Joan Daemen và Vincent Rijmen, hai nhà khoa học người Bỉ.

2.2.2. Thuật toán

2.2.2.1 Cơ sở toán học của AES

Trong AES các phép toán cộng và nhân được thực hiện trên các byte trong trường hữu hạn GF(2^8)

2.2.2.2. Mở rộng khóa

AES thực hiện việc mở rộng khóa dựa trên khóa gốc K, tạo thành chu trình tạo

khóa để sinh ra 10, 12 hoặc 14 khóa con, tương ứng với 10, 12 hoặc 14 chu kỳ lặp của giải thuật AES.

2.2.2.3. Quá trình mã hóa

Quá trình mã hóa của giải thuật AES trải qua 10, 12 hoặc 14 chu kỳ, tương ứng với độ dài của khóa là 128, 192 hoặc 256 bit. Mỗi chu kỳ bao gồm 4 bước được thự hiện tuần tự:

Bước 1: AddRoundKey - mỗi byte của khối trạng thái được kết hợp với khóa con. Các khóa con này được tạo ra từ quá trình tạo khóa con

Bước 2: SubBytes - mỗi byte trong khối trạng thái được thay thế bằng một byte khác trong bảng tra S-box.

Bước 3: ShiftRows - Các hàng trong khối được dịch vòng, số lượng vòng dịch phụ thuộc vào thứ tự của hàng.

Bước 4: MixColumns - các cột trong khối được trộn theo một phép biến đổi tuyến tính

Các bước của quá trình mã hóa được thực hiện trên trạng thái hiện hành S. Kết quả S' của mỗi bước sẽ trở thành đầu vào của bước tiếp theo.

2.2.2.4. Quá trình giải mã

Là quá trình ngược của quá trình mã hóa AES.

2.2.3. Đánh giá

Ưu điểm: AES là giải thuật mã hóa có tốc độ xử lý nhanh, đã được chính phủ Hoa Kỳ tuyên bố là có độ an toàn cao, được sử dụng làm tiêu chuẩn mã hóa mới thay thế cho tiêu chuẩn DES đã lỗi thời. AES được sử dụng để mã hóa các thông tin mật đến tuyệt mật, kháng lại rất nhiều tấn công.

Nhược điểm của AES:

- Mặc dù AES được đánh giá là an toàn nhưng với phương pháp "*tấn công kênh biên*" thì nó chưa thực sự an toàn.
- Cấu trúc toán học của AES được mô tả khá đơn giản. Điều này có thể dẫn tới một số mối nguy hiểm trong tương lai.
- Ngoài ra, AES rất cồng kềnh và cần nhiều tài nguyên cho việc cài đặt [1].

2.3. Hệ mật RC4

2.3.1. Giới thiệu

RC4 là hệ mã dòng với chiều dài khóa biến đổi được nêu ra năm 1987, tác giả của RC4 là Ronald Rivest,.

Trong RC4, để sinh chuỗi Gama thì mỗi khi xuất hiện một xung cần thực hiện các thao tác sau đây:

1. Tăng Q_1 lên 1:	$Q_1 = (Q_1 + 1) \bmod 256$
2. Thay đổi giá trị của Q_2:	$Q_2 = (Q_2 + S[Q_1]) \bmod 256$
3. Hoán đổi giá trị của 2 phần tử:	$S[Q_1] \leftrightarrow S[Q_2]$
4. Tính trổng T của 2 phần tử này:	$T = (S[Q_1] + S[Q_2]) \bmod 256$
5. Gán giá trị cho γ:	$\gamma = S[T]$

Trong quá trình sử dụng, bộ đếm Q_1 sẽ làm cho nội dung của khối S thay đổi chậm, còn bộ đếm Q_2 sẽ đảm bảo sự thay đổi này là ngẫu nhiên.

2.3.2. Thuật toán

2.3.2.1. Khởi tạo khối S

Giá trị của khối S là một hoán vị nào đó của 256 số từ 0…255. Sau đây là thuật toán để xác định hoán vị đó.

1. Gán cho mỗi phần tử giá trị bằng chỉ số của nó: S[i] = i; i=0…255
2. Tạo một mảng k gồm 256 phần tử, mỗi phần tử có kích thước 1 byte. Điền đầy bảng k bằng các byte của khóa K: k[0]=K[0], k[1]=K[1], ... Trong trường hợp cần thiết, khóa K được dùng lặp lại.
3. Khởi tạo biến đếm j: j=0;
4. Xáo trộn khối S:
    a. i = 0…255
    b. j = (j + S[i] + k[i]) mod 256

   Hoán đổi giá trị: S[i] ↔ S[j]

2.3.2.2. Mã hóa và Giải mã

Khi đã có được Gama rồi thì việc mã hóa và giải mã của RC4 diễn ra đơn giản. Nhận xét rằng Gama được tạo ra theo từng khối 8 bit nên kích thước của mỗi ký tự trong alphabet mà chúng ta sẽ sử dụng là 8.

2.3.3. Đánh giá

Ưu điểm của RC4 là thuật toán đơn giản, ý nghĩa của từng bước rõ ràng, logic.

- RC4 an toàn đối với cả 2 phương pháp thám cơ bản là thám tuyến tính và thám vi phân (chưa có công trình nào về thám RC4 được công bố). Số trạng thái mà RC4 có thể có là $256!\times256\times256 \approx 2^{1700}$.

- Tốc độ mã đạt rất cao, so với DES thì RC4 nhanh gấp 10 lần.

2.4. Hệ mã hóa RC5 [9]

2.4.1. Giới thiệu

Thuật toán mã hóa RC5 do giáo sư Ronald Rivest của đại học MIT công bố vào tháng 12 năm 1984

2.4.2. Thuật toán

2.4.2.1. Định nghĩa các giá trị

+ w: kích thước khối cần được mã hóa (giá trị chuẩn là 32 bit, ngoài ra ta có thể chọn 16 hay 64 bit).

+ r: số vòng lặp (giá trị từ 0,1,...,255)

+ b: chiều dài khóa theo byte (0 đến 255)

Các giá trị thường dùng là: w = 32, r = 20, còn chiều dài khóa có thể 16, 24, hay 32 byte.

2.4.2.2. Mở rộng khóa

Thuật toán mở rộng cho khóa K của người sử dụng thành một tập gồm 2(r+1) các khóa trung gian. Các khóa trung gian này được điền vào một bảng khóa mở rộng S. Do

vậy, S là một bảng của t = 2(r+1) các giá trị nhị phân ngẫu nhiên được quyết định bởi khóa K.

Quá trình mở rộng khóa bao gồm các bước sau:

+ *Bước 1:*

Chép khóa bí mật K[0,...,b-1] vào mảng L[0,...,c-1].

+ Bước 2:

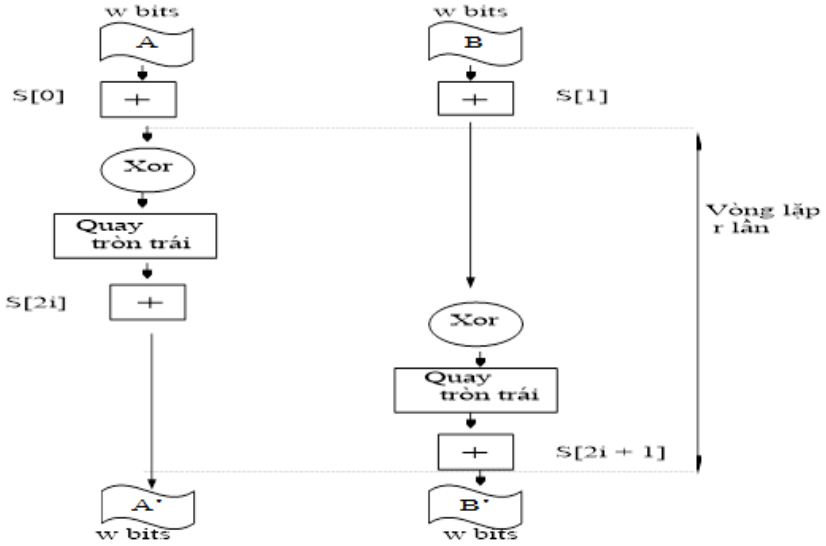
Khởi tạo mảng S với một mẫu bit ngẫu nhiên đặc biệt, bằng cách dùng một phép tính số học module 2^w được quyết định bởi hằng số lý tưởng P_W và Q_w.

+ Bước 3 :

Trộn khóa bí mật của người sử dụng vào mảng L và S.

2.4.2.3. Quá trình mã hóa

Quá trình mã hóa và giải mã có thể được minh họa như sau:



Hình 2. 2. Sơ đồ khối quá trình mã hóa và giải mã RC5

2.4.2.4. Quá trình giải mã :

Quá trình giải mã của RC5 đi ngược lại quá trình mã hóa để có được giá trị gốc.

Thuật toán giải mã như sau :

```
For i = r downto 1 do {
            B' = ((B' - S[2i + 1]) >>> A') XOR A'
            A' = ((A' - S[2i]) >>> B' XOR B'
}
B = B' - S[1]
A = A' - S[0]
```

2.4.3. Đánh giá

+ Theo kết quả đánh giá độ an toàn của các thuật toán, RC5 với 12 vòng lặp và mã hóa khối 64-bit cung cấp độ an toàn tương đương với thuật toán DES khi thử với phương pháp giả mã, 2^{44} cho RC5 và 2^{43} DES.

2.5. Hệ mã hóa RC6 [19]

2.5.1. Giới thiệu

RC6 là một cải tiến của RC5, được thiết kế để giải quyết các yêu cầu về một chuẩn mã hóa cao cấp AES (Advanced Encryption Standard). Giống như RC5, RC6 sử dụng những vòng lặp.

2.5.2. Thuật toán

2.5.2.1. Định nghĩa các giá trị

w: kích thước khối cần được mã hóa (giá trị chuẩn là 32 bit, ngoài ra ta có thể chọn 16 hay 64 bit).

r: số vòng lặp (giá trị từ 0,1,...,255)

b: chiều dài khóa theo byte (0 đến 255)

2.5.2.2. Mở rộng khóa

Quá trình mở rộng khóa bao gồm các bước sau:

Bước 1 :

- Chép khóa bí mật K[0,...,b-1] vào mảng L[0,...,c-1].
- Thao tác này sử dụng u byte liên tục nhau của khóa K để điền vào cho L, theo thứ tự từ byte thấp đến byte cao. Các byte còn lại trong L được điền vào giá trị 0.
- Trong trường hợp b = c = 0, chúng ta sẽ đặt c về 1 và L[0] về 0.

Bước 2 :

- Khởi tạo mảng S với một toán tử ngẫu nhiên đặc biệt, bằng cách dùng một phép tính số học module 2^w được quyết định bởi hằng số lý tưởng P_W và Q_w.

Bước 3:

- Trộn khóa bí mật của người sử dụng vào mảng L và S.

Lưu ý rằng hàm mở rộng khóa là một chiều do vậy không dễ dàng tìm ra khóa K từ S.

2.5.2.3. Thuật toán mã hóa:

```
B = B + S[0]
D = D + S[1]
For i = 1 to r do {
        t = (B x (2B + 1)) <<< lgw
        u = (D x (2D +1)) <<< lgw
```

2.5.2.4. Thuật toán giải mã:

Quá trình giải mã của RC6 là quá trình đi ngược lại quá trình mã hóa để có được giá trị gốc.

Thuật toán giải mã như sau :

Input: giá trị mã được lưu trữ trong bốn khối *w-bit* A', B', C', D'

Số vòng lặp r

w-bit khóa vòng lặp S[0,...,2r + 3]

Output: giá trị giải mã được lưu trong bốn khối *w-bit* A, B, C, D

2.5.3 Đánh giá

RC6 được phát triển từ RC5 nên sẽ có tất cả những ưu điểm của RC5. Bên cạnh đó, RC6 còn có một số đặc tính sau :

+ RC6 tăng thêm sự phức tạp của quá trình mã hóa và giải mã bằng cách sử dụng các phép toán: cộng, trừ, nhân, exclusive-or, quay trái và quay phải.

+ Một số đặc điểm nổi bật khác của RC6 so với RC5 là thao tác quay sử dụng chặt chẽ các dữ liệu phụ thuộc và được thao tác trên tất cả các bit.

2.6. Hệ mật RSA [9]

2.6.1. Giới thiệu

Khái niệm hệ mật mã RSA đã được ra đời năm 1977 bởi các tác giả R.Rivets, A.Shamir, và L.Adleman. Hệ mật này dựa trên cơ sở của hai bài toán:

+ Bài toán Logarithm rời rạc (Discrete logarith)

+ Bài toán phân tích thành thừa số.

2.6.2. Thuật toán

Bước 1. ***Tạo cặp khóa*** **(*bí mật, công khai*) (a, b)**

Input: 2 số nguyên tố lớn phân biệt p và q.

Output: Cặp (n,b) là khóa công khai.

Bước 2. ***Ký số***:

Chữ ký trên $x \in P$ là $y = Sig\ k(x) = x^a \pmod n$, $y \in A$.

Bước 3. ***Kiểm tra chữ ký***:

Verk (x,y) = đúng $\Leftrightarrow x \equiv y^b \pmod n$.

2.5.3. Đánh giá

Độ an toàn của hệ RSA

Sau đây ta sẽ xem xét một số các tấn công phương pháp RSA.

1) Vét cạn khóa: cách tấn công này thử tất cả các khóa *d* có thể có để tìm ra bản giải mã có ý nghĩa, tương tự như cách thử khóa *K* của mã hóa đối xứng, với *N* lớn, việc tấn công là bất khả thi.

2) Phân tích N thành thừa số nguyên tố N = pq: việc phân tích phải là bất khả thi thì mới là hàm một chiều, đây cũng là nguyên tắc hoạt động của RSA. Tuy nhiên, nhiều thuật toán phân tích mới đã được đề xuất, cùng với tốc độ xử lý của máy tính ngày càng nhanh, đã làm cho việc phân tích *N* không còn quá khó khăn như trước đây. Năm 1977, các tác giả của RSA đã treo giải thưởng cho ai phá được RSA có kích thước của *N* vào khoảng 428 bit, tức 129 chữ số. Các tác giả này ước đoán phải mất 40 nghìn triệu triệu năm mới có thể giải được.

Tuy nhiên vào năm 1994, câu đố này đã được giải chỉ trong vòng 8 tháng.

3) Đo thời gian: Đây là một phương pháp phá mã không dựa vào mặt toán học của thuật toán RSA, mà dựa vào một "hiệu ứng lề" sinh ra bởi quá trình giải mã RSA. Hiệu ứng lề là thời gian thực hiện giải mã. Giả sử người phá mã có thể đo được thời giải mã dùng thuật toán bình phương liên tiếp.

CHƯƠNG 3: MỘT SỐ GIẢI PHÁP ĐẢM BẢO ATTT CHO CÁC DNVVN

3.1. Nhóm giải pháp về Quản lý ATTT

3.1.1. Thiết lập hệ thống quản lý ATTT cho DNVVN theo tiêu chuẩn ISO 27001:2013

Hệ thống quản lý ATTT (ISMS) là nhu cầu thiết yếu của một doanh nghiệp, khi cần đảm bảo ATTT một cách toàn diện. Xây dựng hệ thống ISMS theo tiêu chuẩn ISO 27001: 2013 sẽ giúp hoạt động đảm bảo ATTT của doanh nghiệp được quản lý chặt chẽ.

Theo tiêu chuẩn ISO/IEC 27001: 2013, thông tin và các hệ thống, quy trình, cán bộ liên quan đều là tài sản của tổ chức. Tất cả các tài sản đều có giá trị quan trọng trong hoạt động của tổ chức và cần được bảo vệ thích hợp. Do thông tin tồn tại và được lưu trữ dưới nhiều hình thức khác nhau, nên tổ chức phải có các biện pháp bảo vệ phù hợp để hạn chế rủi ro.

Tại Việt Nam, một số tiêu chuẩn quốc gia (TCVN) về ATTT đã được xây dựng, công bố trên cơ sở chấp nhận nguyên vẹn các tiêu chuẩn ISO/IEC.

Bộ tiêu chuẩn về hệ thông quản lý an toàn thông tin ISMS:

Công nghệ thông tin - Hệ thống quản lý an toàn thông tin - Các yêu cầu (TCVN ISO/IEC 27001:2009 ISO/IEC 27001:2005).

Công nghệ thông tin - Các kỹ thuật an toàn - Quy tắc thực hành Quản lý an toàn thông tin (TCVN ISO/IEC 27002:2011).

Công nghệ thông tin - Các kỹ thuật an toàn - Quản lý rủi ro an toàn thông tin (TCVN 10295:2014 ISO/IEC 27005:2011)

Bộ tiêu chuẩn về đánh giá ATTT:

Công nghệ thông tin - Các kỹ thuật an toàn - Các tiêu chí đánh giá an toàn CNTT - Phần 1: Giới thiệu và mô hình tổng quát (TCVN 8709-1:2011 ISO/IEC 15408-1:2009).

- Công nghệ thông tin - Các kỹ thuật an toàn - Các tiêu chí đánh giá an toàn CNTT - Phần 2: Các thành phần chức năng an toàn (TCVN 8709-2:2011 ISO/IEC 15408-2:2008).

Công nghệ thông tin - Các kỹ thuật an toàn - Các tiêu chí đánh giá an toàn CNTT - Phần 3: Các thành phần đảm bảo an toàn (TCVN 8709-3:2011 ISO/IEC 15408-3:2008).

Bộ tiêu chuẩn về an toàn mạng

TCVN 9801-1:2013 (ISO/IEC 27033-1:2009) Công nghệ thông tin - Kỹ thuật an ninh - An ninh mạng - Phần 1: Tổng quan và khái niệm

3.1.1.1. Chính sách về ATTT [10]

Chính sách ATTT là tài liệu cấp cao đặc thù, tập hợp các luật đặc biệt của Doanh nghiệp như những yêu cầu, quy định mà những người trong doanh nghiệp đó phải thực hiện để đạt được các mục tiêu về ATTT. Chính sách ATTT sẽ được người đứng đầu tổ chức, doanh nghiệp phê chuẩn và ban hành thực hiện. Nó được ví như bộ luật của tổ chức, doanh nghiệp mà mọi thành viên trong tổ chức, các đối tác, khách hàng quan hệ đều phải tuân thủ

3.1.1.2 Thực hiện chính sách ATTT theo các tiêu chuẩn, quy trình và hướng dẫn

Tất cả các tiêu chuẩn, hướng dẫn và quy trình liên quan đến ATTT đều có nguồn gốc từ chính sách ATTT.

3.1.1.3. Chính sách về an toàn đối với nhân sự trong doanh nghiệp

Chính sách này được ban hành bởi phòng quản lý nhân sự, bao gồm một số nội dung chính như sau:

- Quá trình tuyển dụng: Tài liệu tham khảo hỗ trợ cho ứng viên phải được xác nhận trước khi chấp nhận tuyển dụng;
- Không nên sắp xếp những nhân viên làm việc có tính chất thời vụ vào những công việc nhạy cảm.
- Cần đưa ra những cách tuyên truyền hiệu quả về chính sách ATTT tới toàn thể nhân viên trong công ty.
- Cần tổ chức các khóa đào tạo nâng cao nhận thức về ATTT cho nhân viên

3.1.1.5. Chính sách quản lý truy cập

Chính sách này được ban hành bởi bộ phận kỹ thuật nhằm đảm bảo sự nhất quán trong việc quản lý truy cập mạng internet, hệ thống và các ứng dụng cho những người truy cập ở văn phòng cũng như từ xa.

3.1.2. Đánh giá rủi ro về ATTT

Đánh giá rủi ro về ATTT là một quá trình xác định những nguồn lực thông tin tồn tại cần được bảo vệ, và để hiểu cũng như lưu tài liệu các rủi ro tiềm ẩn từ mối nguy CNTT có thể gây ra mất thông tin bí mật, tính toàn vẹn, hoặc tính sẵn có.

3.1.3. Chính sách phòng chống virus

Virus là một mối đe dọa cho các doanh nghiệp nếu như các máy tính bị nhiễm virus có thể truyền tải thông tin bí mật đến các bên thứ ba một cách trái phép, cung cấp một nền tảng cho việc truy cập hoặc sử dụng mạng nội bộ trái phép, lây nhiễm các thiết bị kết nối mạng khác, hoặc gây trở ngại với việc sử dụng các dịch vụ CNTT của Doanh nghiệp.

3.1.4. Chính sách sao lưu và phục hồi

Tất cả thông tin điện tử phải được sao lưu vào các phương tiện lưu trữ an toàn một cách thường xuyên (ví dụ: sao lưu dữ liệu), với mục đích khôi phục sau sự cố có thể xảy ra và hoạt động trở lại. Kế hoạch sao lưu và phục hồi dữ liệu đưa ra các yêu cầu tối thiểu cho việc tạo ra và duy trì các bản sao lưu.

3.2. Nhóm giải pháp về công nghệ

3.2.1. Mã hóa dữ liệu trong lưu trữ

Yếu tố quan trọng đầu tiên cần xét đến trong quy trình mã hoá dữ liệu trong lưu trữ là quản lý khoá, nếu hệ thống quản lý khoá không đảm bảo thì tác dụng của mã hoá cũng giảm rất nhiều.

3.2.1.1. Quản lý khóa

Theo xu thế phát triển, quản lý khóa dần được tiêu chuẩn hóa nhằm đưa đến các cơ chế sử dụng thống nhất đáp ứng vấn đề tương thích giữa các hệ thống sử dụng kỹ thuật mật mã, tại Việt Nam là tiêu chuẩn TCVN 7817: 2007, trong đó có phần 3: TCVN

7817- 3: 2007 Công nghệ thông tin - Kỹ thuật mật mã - Quản lý khoá - Phần 3: Các cơ chế sử dụng kỹ thuật phi đối xứng - khuyến cáo 7 cơ chế thỏa thuận khóa bí mật, 6 cơ chế vận chuyển khóa bí mật và 3 cơ chế vận chuyển khóa công khai. Các cơ chế này đều dựa trên kỹ thuật mật mã phi đối xứng.

3.2.1.2. Mã hóa dữ liệu theo tiêu chuẩn mã hóa tiên tiến – AES

Thuật toán mã dữ liệu AES được NIST ban hành thành FIPS PUB 197: ADVANCED ENCRYPTION STANDARD - AES (Tiêu chuẩn mã hóa dữ liệu tiên tiến - AES) ngày 26/11/2001 và ISO ban hành trong ISO/IEC 18033-3 Information technology- Security techniques- Encryption algorithms - Part 3: Block ciphers (Công nghệ thông tin - Kỹ thuật an toàn - Thuật toán mã hóa - Phần 3: Các hệ mã khối). Việc biên soạn Tiêu chuẩn mã hóa dữ liệu này tại Việt Nam được dựa trên việc tham khảo, kết hợp cả hai tài liệu trên nhưng chủ yếu dựa vào FIPS PUB 197.

3.2.2. Phòng chống tấn công website

Để chống xâm nhập vào website, các DNVVN nên thực hiện một số giải pháp sau:

Không dùng share hosting

Kiểm tra mã nguồn website thường xuyên

Không cài thêm các plugin "lạ" vào website

Sao lưu dữ liệu thường xuyên

3.2.3. Sử dụng chữ ký số trong các giao dịch điện tử

Chữ ký số giải quyết vấn đề đảm bảo độ an toàn thông tin, toàn vẹn dữ liệu và là bằng chứng chống chối bỏ trách nhiệm trên nội dung đã ký, giúp cho các DNVVN không phải gặp trực tiếp nhau mà vẫn có thể yên tâm mua bán, trao đổi, ký hợp đồng,… thông qua môi trường Internet".

3.2.3.1. Khái niệm:

Chữ ký số khóa công khai (hay hạ tầng khóa công khai) là mô hình sử dụng các kỹ thuật 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.

3.2.3.2. Chức năng chữ ký số

- Xác minh tác giả và thời điểm ký thông tin được gửi
- Xác thực nội dung thông tin gửi
- Là căn cứ để giải quyết tranh chấp – không thể từ chối trách nhiệm

Giao thức của chữ ký số bao gồm thuật toán tạo chữ ký số và thuật toán để kiểm tra chữ ký số

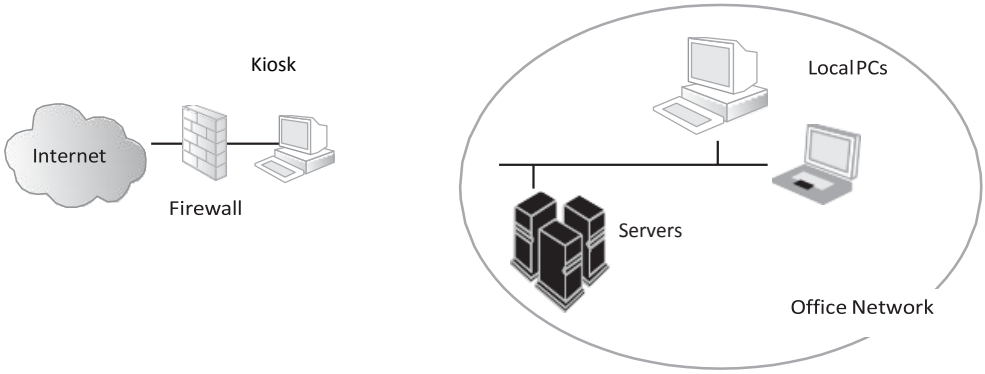
3.2.3.3. Mô hình chữ ký số RSA trong các hệ thống quản lý

Quá trình gửi và nhận các tệp văn bản phục vụ quản lý dựa vào thuật toán băm và thuật toán mã hóa RSA.

3.2.4 Xây dựng hệ thống mạng an toàn

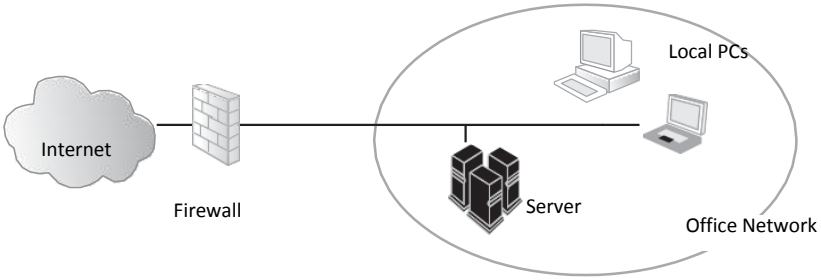
- Các DNVVN có thể chọn từ một trong mô hình truy cập Internet sau[10]:

(1) Mô hình Kiosk



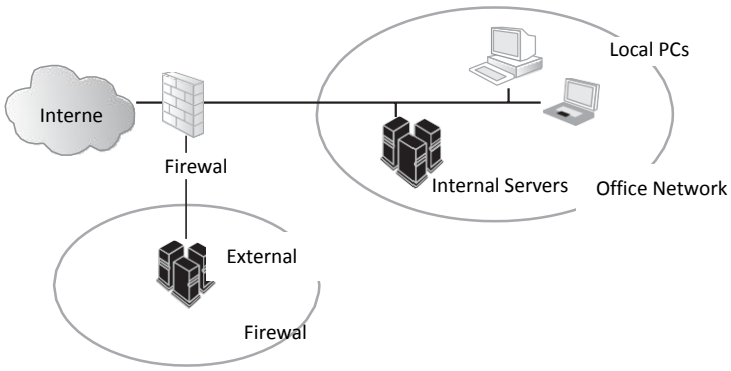
Hình 3. 1. Mô hình Kiosk

(2) Mô hình Office-Internet



Hình 3. 2. Mô hình Office-Internet

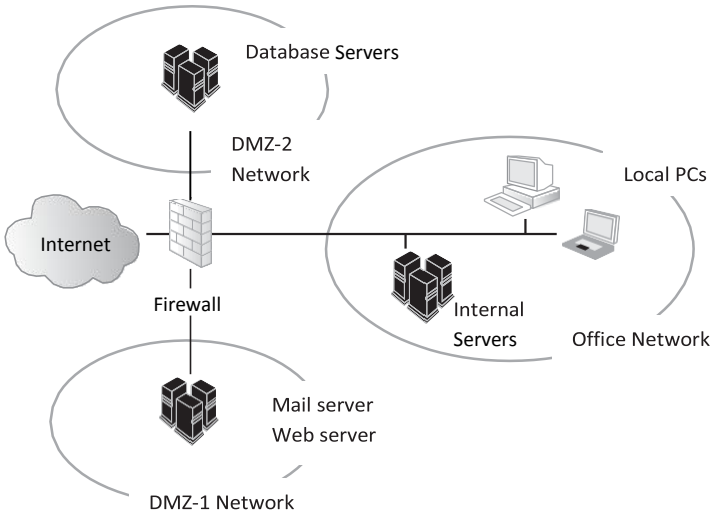
(3) Mô hình Office-DMZ-Internet



Hình 3. 3. Mô hình Office-DMZ-Internet

(4) Mô hình Office-MultiDMZ-Internet

- Mô hình này là một phần mở rộng của mô hình Office-DMZ-Internet, với nhiều hơn một mạng DMZ. Các máy chủ công cộng được chia thành 2 nhóm, mỗi nhóm được đặt trong một mạng DMZ riêng biệt.



Hình 3. 4. Mô hình Office-MultiDMZ-Internet

3.3. Các biện pháp giảm nhẹ rủi ro về ATTT cho các DNVVN [10]

3.3.1. Vai trò của giảm nhẹ rủi ro về ATTT

Giảm nhẹ rủi ro về ATTT giúp cho doanh nghiệp giảm thiểu thiệt hại về kinh doanh và mức độ bồi thường cho khách hàng;

3.3.2. Kiểm soát và kiểm định [10]

Kiểm soát ATTT

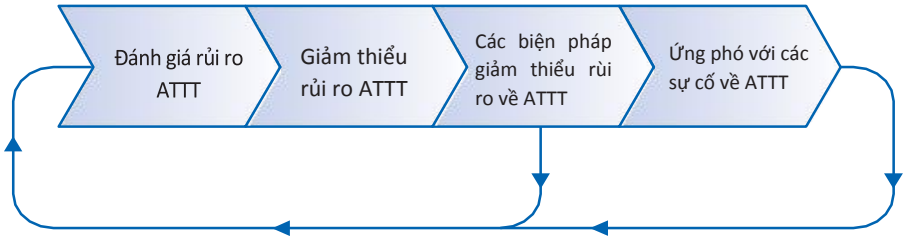
Kiểm soát ATTT bao gồm việc giám sát và thực hiện các hành động khắc phục cần thiết đối với các khu vực ATTT trọng yếu

Kiểm định

Kiểm định ATTT là một phần quan trọng của chương trình đảm bảo rủi ro, mục tiêu của việc kiểm định ATTT bao gồm:

3.3.3. Đánh giá quy trình ATTT [10]

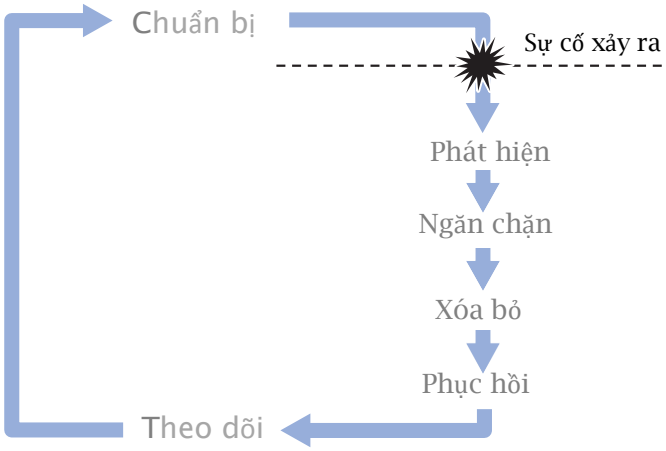
Đánh giá quy trình ATTT của doanh nghiệp nên được tiến hành tuần tự theo các giai đoạn: đánh giá rủi ro, giảm thiểu rủi ro, các biện pháp giảm thiểu rủi ro, giải quyết các sự cố về ATTT.



Hình 3. 5. Đánh giá quy trình ATTT theo các giai đoạn

3.4. Ứng phó sự cố về ATTT

Có 6 bước ứng phó các sự cố về ATTT cho doanh nghiệp như sau[10]:



Hình 3. 6. Các bước ứng phó với sự cố về ATTT

3.4.1. Chuẩn bị

Ở bước này doanh nghiệp cần lập kế hoạch giải quyết sự cố một cách tối ưu nhằm đảm bảo chất lượng và thời gian giải quyết.

3.4.2. Phát hiện

Khi phát hiện sự cố ATTT, doanh nghiệp nên dành thời gian để đánh giá sự cố, tìm hiểu trước khi đưa ra kết luận, đồng thời theo dõi những biểu hiện bất thường như: các thông báo lỗi, bản ghi đáng ngờ,…

3.4.3. Ngăn chặn

Một trong những quyết định quan trọng cần thực hiện là có nên tiếp tục hay đình chỉ các hoạt động và dịch vụ của hệ thống bị xâm nhập hay không. Điều này phụ thuộc vào loại và mức độ nghiêm trọng của sự cố bởi nó tác động đến hình ảnh của công ty.

3.4.4. Xóa bỏ

Mục đích của giai đoạn này là loại bỏ hoặc giảm nhẹ nguyên nhân của sự cố ATTT. Trong giai đoạn này, các hành động sau có thể cần được thực hiện tùy thuộc vào mức độ, tính chất của sự cố cũng như yêu cầu của hệ thống.

3.4.5. Phục hồi

Mục đích của giai đoạn này là khôi phục hệ thống hoạt động bình thường.

3.4.6. Theo dõi

Mục tiêu của giai đoạn này là rút ra bài học từ sự cố, việc theo dõi nên bắt đầu càng sớm càng tốt.

CHƯƠNG 4: CÀI ĐẶT VÀ THỬ NGHIỆM CHỮ KÝ SỐ ĐẢM BẢO ATTT TRONG VIỆC KÝ KẾT HỢP ĐỒNG ĐIỆN TỬ CỦA DNVVN

4.1. Tổng quan về hợp đồng điện tử

4.1.1. Khái niệm

Theo Điều 11, mục 1, Luật mẫu về Thương mại điện tử UNCITRAL 1996: *"Hợp đồng điện tử được hiểu là hợp đồng được hình thành thông qua việc sử dụng thông điệp dữ liệu"*

Theo Luật giao dịch điện tử của Việt Nam 2005: *"Hợp đồng điện tử là hợp đồng được thiết lập dưới dạng thông điệp dữ liệu theo quy định của Luật này"*

Thông điệp dữ liệu: "Thông tin được tạo ra, được gửi đi, được nhận và lưu trữ bằng phương tiện điện tử"

4.1.2. Một số hợp đồng điện tử

Hợp đồng truyền thống được đưa lên web

Một số hợp đồng truyền thống đã được sử dụng thường xuyên và chuẩn hóa về nội dung, do một bên soạn thảo và đưa lên website để các bên tham gia ký kết

Hợp đồng điện tử hình thành qua giao dịch tự động

Ở hình thức này nội dung hợp đồng không được soạn sẵn mà được hình thành trong giao dịch tự động.

Hợp đồng hình thành qua nhiều giao dịch bằng email

Đây là hình thức hợp đồng điện tử được sử dụng phổ biến trong các giao dịch điện tử giữa các doanh nghiệp với doanh nghiệp (B2B), đặc biệt là trong các giao dịch thương mại điện tử quốc tế.

Hợp đồng điện tử sử dụng chữ ký số

Đặc điểm nổi bật là các bên phải có chữ ký số để ký vào các thông điệp dữ liệu trong quá trình giao dịch. Chính vì có sử dụng chữ ký số nên loại hợp đồng điện tử này có **độ bảo mật và ràng buộc trách nhiệm các bên cao hơn các hình thức trên.**

4.1.3. Lợi ích của hợp đồng điện tử

Thứ nhất, hợp đồng điện tử giúp các bên tiết kiệm thời gian, chi phí giao dịch, đàm phán và ký kết hợp đồng.

Thứ hai, sử dụng hợp đồng điện tử giúp các doanh nghiệp giảm chi phí bán hàng.

Thứ ba, sử dụng hợp đồng điện tử giúp quá trình giao dịch, mua bán nhanh và chính xác hơn.

Thứ tư, sử dụng hợp đồng điện tử giúp các doanh nghiệp nâng cao năng lực cạnh tranh và khả năng hội nhập kinh tế quốc tế. Hợp đồng điện tử không chỉ đem lại lợi ích cho các nhà sản xuất mà còn đem lại nhiều lợi ích cho các công ty thương mại..

4.1.4. Một số điểm cần lưu ý khi ký kết và thực hiện hợp đồng điện tử

Những hợp đồng nào có thể ký dưới dạng dữ liệu điện tử ?

- Điều 24 Luật thương mại 2005: quy định HĐ mua bán hàng hóa được thể hiện bằng văn bản, lời nói, hành vi

- Điều 27: Quy định HĐ mua bán hàng hóa quốc tế phải được thực hiện trên cơ sở hợp đồng bằng văn bản hoặc hình thức khác có giá trị tương đương

- Điều12 Luật giao dịch điện tử: Trường hợp pháp luật yêu cầu thông tin phải được thể hiện bằng văn bản thì thông điệp dữ liệu được xem là đáp ứng yêu cầu này nếu thông tin chứa trong thông điệp dữ liệu đó có thể truy cập và sử dụng được để tham chiếu khi cần thiết.

4.2. Quy trình cơ bản để ký kết hợp đồng điện tử có sử dụng chữ ký số

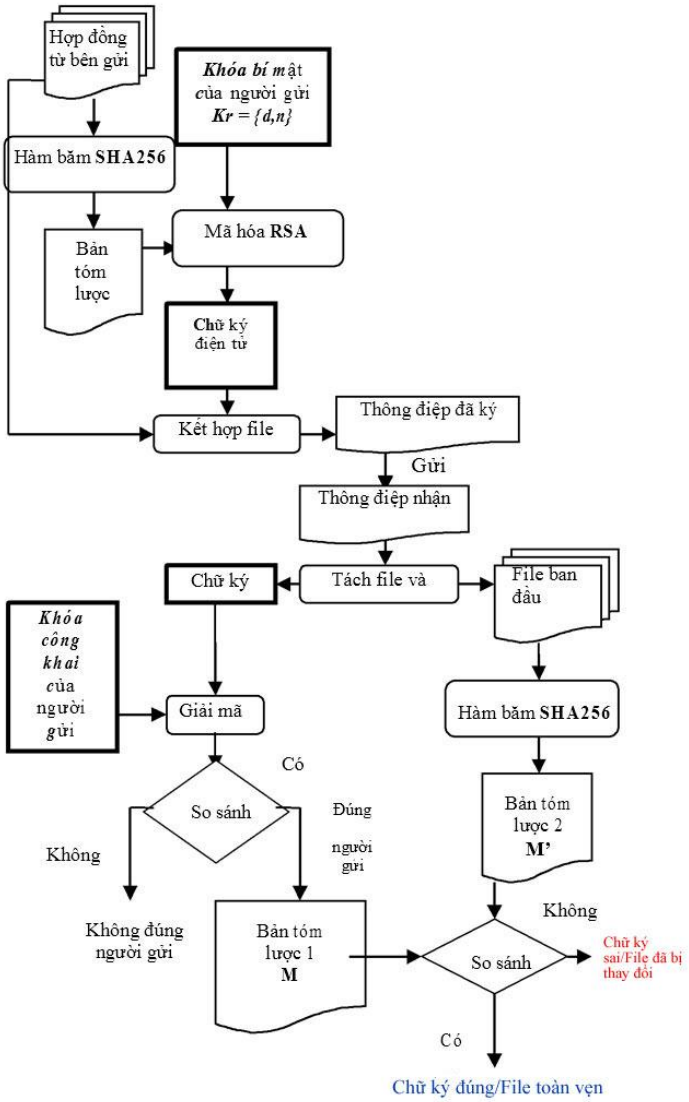
4.2.1. Những khía cạnh cần thiết về an toàn thông tin

Các yêu cầu trong giao dịch thương mại điện tử nói chung và hợp đồng điện tử nói riêng gồm:

• **Đảm bảo tính bí mật**: tính bí mật nội dung thông điệp truyền đi được thực hiện bằng mã hóa trước khi gửi đi.

• **Đảm bảo tính toàn vẹn và nguồn gốc người gửi thông điệp**: thực hiện nhờ chữ ký số dựa trên mã hóa khóa công khai.

Trong quá trình ký kết hợp đồng điện tử, việc truyền thông điệp được đảm bảo an toàn qua việc mô tả quá trình ký và kiểm tra chữ ký trong chương trình như sau:



Hình 4. 1. Sơ đồ quá trình ký số hợp đồng điện tử

4.2.1.1. Quá trình ký và gửi hợp đồng

- Bên gửi soạn thảo hợp đồng, sau đó chương trình sử dụng hàm băm SHA256 để mã hóa thành chuỗi ký tự dài 256 bit gọi là bản tóm lược. Quy trình này còn được gọi là quy trình rút gọn hợp đồng (Hash-Value).
- Sử dụng thuật toán RSA để mã hóa khóa mật (private key) và bản tóm lược được chữ ký điện tử.
- Kết hợp bản hợp đồng với chữ ký điện tử thành một thông điệp đã ký và gửi đi cho người nhận.

4.2.1.2. Quá trình nhận hợp đồng

Sau khi bên nhận đăng nhập vào hệ thống và thực hiện việc nhận các tệp văn bản, hệ thống sẽ tách thông điệp đã ký thành ra file và chữ ký điện tử. Đến giai đoạn này sẽ có 2 quá trình kiểm tra :

a. Kiểm tra file có đúng người gửi hay không?

- Chương trình sử dụng thuật toán RSA để giải mã chữ ký điện tử bằng khóa công khai của người gửi.
- Nếu giải mã không được thì file nhận được không đúng người gửi.
- Nếu giải mã thành công thì file nhận được đúng người gửi và có được Bản tóm lược 1.

b. Kiểm tra file có bị thay đổi hay không?

- Từ file được tách ra, chương trình sử dụng hàm băm SHA256 mã hóa thành Bản tóm lược 2.
- Kiểm tra Bản tóm lược 1 và Bản tóm lược 2 có giống nhau hay không? Nếu giống nhau thì file nhận được là vẹn toàn (không bị thay đổi hay tác động), ngược lại là file đã bị thay đổi.

4.2.2 Cài đặt thử nghiệm

4.2.2.1. Xây dựng chương trình

Chương trình được xây dựng bằng ngôn ngữ lập trình C#, sử dụng hàm băm SHA256 và hệ mật RSA.

4.2.2.2. Các bước thử nghiệm chương trình:

Bước1: Bên gửi soạn thảo hợp đồng.

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

Độc lập – Tự do – Hạnh phúc

HỢP ĐỒNG HỢP TÁC

V/v: Ươm tạo doanh nghiệp Công nghệ

Số:……/2017/ RISME

- Căn cứ Luật Khoa học và Công nghệ;
- Chức năng, nhiệm vụ của các bên;
- Căn cứ kết quả tiền ươm tạo và đơn đăng ký tham gia ươm tạo của doanh nghiệp.

Hôm nay, ngày 06 tháng 3 năm 2017, tại Văn phòng Viện Nghiên cứu doanh vừa và nhỏ, chúng tôi gồm:

BÊN A: VIỆN NGHIÊN CỨU DOANH NGHIỆP VỪA VÀ NHỎ (Cơ sở ươm tạo)

Đại diện: TS Phạm Thế Hưng - Chức vụ: Viện trưởng

Địa chỉ: Phòng 415-416E1, Khu ngoại giao đoàn Trung Tự, số 6 Đặng Văn Ngữ, Đống Đa, Hà Nội

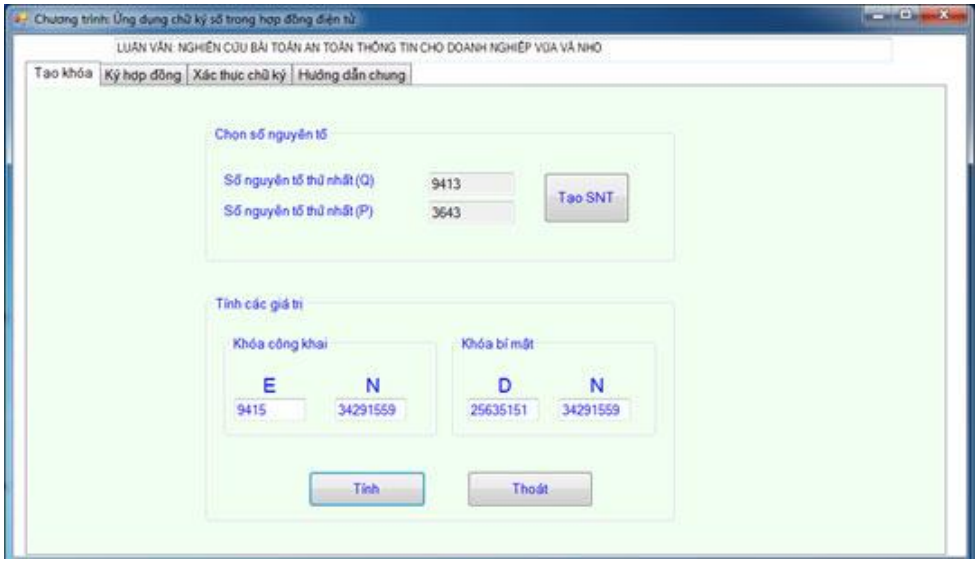
Hình 4. 2. Mẫu hợp đồng

Bước 2*: *Quy trình ký số và gửi hợp đồng

Tạo khóa

- Nhấn nút "Tính" để tạo ra cặp khóa bí mật (Pravite key) - (D,N), khóa công khai (Public key) - (E,N).

- Cất giữ khóa bí mật (D,N) để ký văn bản, công bố khóa công khai (E,N) để xác nhận chữ ký.



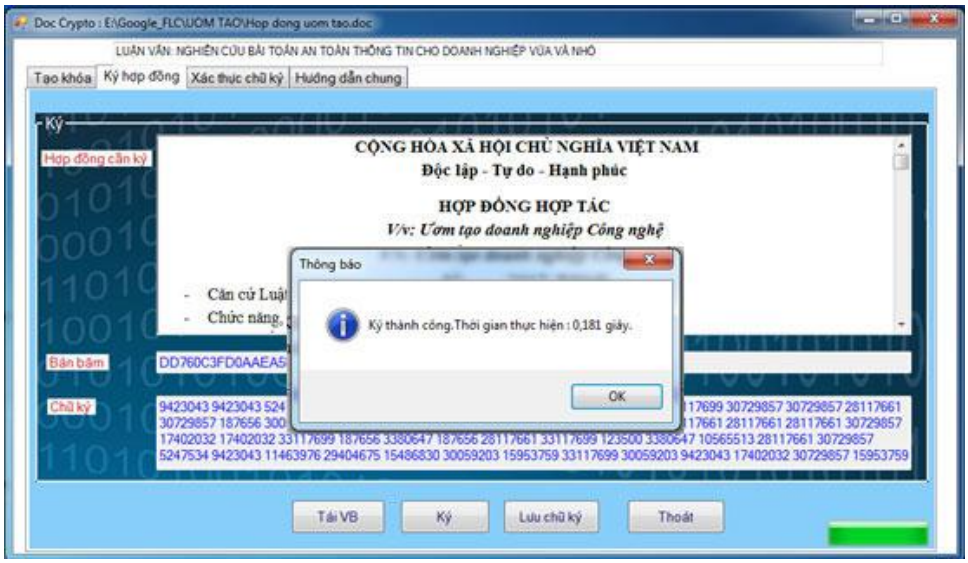
Hình 4. 3. Tạo cặp khóa RSA cho người dùng

Ký hợp đồng

- Tải hợp đồng cần ký bằng cách chọn nút “Tải VB”

- Nhấn nút "Ký" để ký văn bản, hàm băm SHA256 tóm lược hợp đồng chuỗi 256 bit (bản băm hay bản tóm lược).

- Thuật toán RSA mã hóa khóa mật (private key) và bản tóm lược được chữ ký điện tử



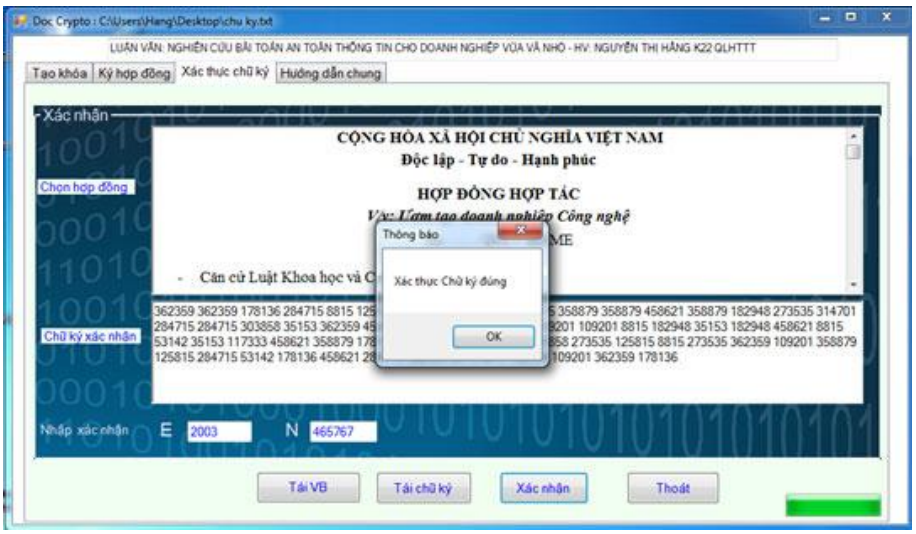
Hình 4. 4. ký hợp đồng bằng chữ ký điện tử

- Nhấn nút "Lưu chữ ký" để lưu giữ chữ ký điện tử dưới dạng file .txt.

Bên gửi gửi cho bên nhận bao gồm: Chữ ký điện tử và văn bản gốc cần ký

Bước 3: Quá trình nhận hợp đồng và xác thực chữ ký

- Bên nhận sử dụng chương trình, chọn cửa sổ "Xác thực chữ ký"
- Tải hợp đồng nhận được để xác nhận.
- Tải chữ ký điện tử của người gửi để xác nhận.
- Nhập khóa công khai (E,N) của người gửi để xác nhận.
- Nhấn nút "Xác nhận" để xác thực chữ ký của văn bản điện tử.



Hình 4. 5. Quá trình kiểm tra chữ ký

KẾT LUẬN

1. Các kết quả đạt được

a. Về lý thuyết

Để nghiên cứu bài toán an toàn thông tin cho doanh nghiệp vừa và nhỏ, học viên đã tập trung nghiên cứu cơ sở lý luận về an toàn thông tin, tìm hiểu đặc điểm hệ thống thông tin, thực trạng ATTT của các DNVVN, những tổn thất của DNVVN trước những nguy cơ mất ATTT để có thể đưa ra một số giải pháp đảm bảo ATTT phù hợp.

Bên cạnh đó, học viên cũng nghiên cứu, tìm hiểu một số hệ mật mã đảm bảo ATTT được dùng phổ biến hiện nay như: AES, RC5, RC6, RSA, đề xuất một số giải pháp đảm bảo ATTT cho DNVVN về mặt công nghệ ứng dụng một số hệ mật mã này như: Mã hóa dữ liệu cho DNVVN, ứng dụng chữ ký số trong các giao dịch điện tử đang phổ biến tại các DNVVN hiện nay.

Cùng với nhóm giải pháp về công nghệ, học viên cũng đề xuất nhóm giải pháp về quản lý ATTT đối với các DNVVN trong đó tập trung vào việc hướng dẫn các DNVVN thiết lập các Chính sách ATTT một cách bài bản, xây dựng kế hoạch đánh giá rủi ro, các biện pháp giảm thiểu rủi ro, cách ứng phó khi xuất hiện các mối de dọa ATTT.

b. Về thực nghiệm

Xuất phát từ yêu cầu thực tế cần phải đảm bảo tính bí mật, toàn vẹn nội dung thông điệp và xác định được nguồn gốc dữ liệu trong việc ký kết hợp đồng điện tử, học viên đã xây dựng ứng dụng chữ ký số trong việc ký kết hợp đồng điện tử dựa trên sơ đồ chữ ký số RSA và hàm băm SHA256.

1. Hướng nghiên cứu tiếp theo

Học viên sẽ tiếp tục tìm hiểu và thực nghiệm với một số phương pháp mã hoá khoá đối xứng như IDEA, một số hệ mật mã dòng, mật mã khối; các phương pháp mã hoá khoá công khai như Elgamal, Rabin, Knapsack, Eliptic Curve,…

Về phần thực nghiệm, học viên sẽ tìm hiểu, phát triển thêm phần chứng thực số và ứng dụng chữ ký số dùng trên các thiết bị thông minh như điện thoại, máy tính bảng,… giúp các DNVVN ký kết hợp đồng điện tử một cách thuận lợi nhất.

Hoàn thiện luận văn này, học viên mong muốn đóng góp một phần kiến thức của mình vào vấn đề ATTT cho các DNVVN hiện nay. Tuy nhiên, do hạn chế về nguồn số liệu và kiến thức, luận văn không tránh khỏi những thiếu sót nhất định. Hơn nữa, do tình hình ATTT còn nhiều bất ổn và khó dự đoán nên trong tương lai học viên sẽ tiếp tục nghiên cứu để tìm ra những giải pháp phù hợp nhất, đảm bảo an toàn thông tin cho các DNVVN.