



ỦY BAN NHÂN DÂN THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG CAO ĐẲNG KỸ THUẬT LÝ TỰ TRỌNG
KHOA CÔNG NGHỆ THÔNG TIN

Hội thảo khoa học

**CẬP NHẬT VÀ ÁP DỤNG CÁC
CÔNG NGHỆ TRONG THỰC TIỄN
VÀO GIẢNG DẠY CHUYÊN NGÀNH
MẠNG MÁY TÍNH NHẪM ĐÁP ỨNG
NHU CẦU CỦA DOANH NGHIỆP**



TP.HCM - Tháng 11 năm 2015

MỤC LỤC

DẪN NHẬP	1
SỰ TÍCH HỢP GIỮA PHẦN CỨNG VÀ PHẦN MỀM TRONG HỆ THỐNG NHÚNG ĐỀ TỰ TRỊ CÁC THIẾT BỊ MÁY MÓC CHUYÊN DỤNG HIỆN ĐẠI	2
1. ĐẶT VẤN ĐỀ	2
2. NỘI DUNG	2
2.1. Giới thiệu	2
2.2. Phần cứng và phần mềm trong hệ thống nhúng	3
2.3. Mô phỏng sự tích hợp giữa phần cứng và phần mềm và sản phẩm Hệ thống nhúng 4	
3. PHẦN KẾT	9
TÀI LIỆU THAM KHẢO	11
CHỮ KÝ SỐ RSA ÁP DỤNG GIẢNG DẠY HỌC PHẦN AN NINH MẠNG NÂNG CAO VÀ ỨNG DỤNG TRONG THỰC TIỄN	12
4. ĐẶT VẤN ĐỀ	12
5. NỘI DUNG	12
5.1. Tổng quan về chữ ký số	12
5.2. Thuật toán SHA-1	15
5.3. Ứng dụng thực tiễn	19
5.4. Các hạn chế của chữ ký số	25
6. PHẦN KẾT	26
TÀI LIỆU THAM KHẢO	26
ĐỊNH TUYẾN BẰNG GIAO THỨC LINK-STATE (OSPF) THÔNG QUA THIẾT BỊ ROUTER CỦA CISCO ỨNG DỤNG GIẢNG DẠY HỌC PHẦN THIẾT LẬP HỆ THỐNG MẠNG	27
1. ĐẶT VẤN ĐỀ	27
2. NỘI DUNG	28
2.1. Giao thức OSPF (Open Shortest Path First)	28
2.2. Mô hình mạng	29
2.3. Phần mềm	29
2.4. Cấu hình hệ thống	30

3. PHỤ LỤC	37
TÀI LIỆU THAM KHẢO	40

DẪN NHẬP

Đào tạo nguồn nhân lực đáp ứng nhu cầu của xã hội đang là mối quan tâm lớn của ngành giáo dục và cả xã hội. Trong giai đoạn nước ta hội nhập quốc tế tự do thương mại, vấn đề quan tâm nhất vẫn là việc làm. Theo thống kê, chúng ta có đến 82,16% lao động phổ thông giản đơn dẫn đến tình trạng vừa thừa vừa thiếu lao động. Từ đó cho thấy nhu cầu cấp bách để đáp ứng nhu cầu phát triển đất nước, phải đào tạo cái xã hội đang cần. Có phải chưa có tiếng nói chung giữa doanh nghiệp và nhà trường khi mà công ty nào cũng “Yêu cầu 3 năm kinh nghiệm”

Hội thảo lần này đề cập đến các kiến thức, ứng dụng đang ứng dụng trong thực tế, tập trung vào các nội dung mới nhằm mục đích từng bước thực hiện chủ trương, chính sách của nhà trường. Với ba nội dung tham luận về lập trình nhúng thiết bị, an toàn mạng và thiết lập định tuyến trên thiết bị Cisco.

Tham luận 1 đề cập đến một số ứng dụng trong thực tế của hệ thống nhúng. Các mô hình này đã được thực thi và vận hành bởi sinh viên thực tập tại công ty như: Hộp nhạc quà tặng, máy ấp trứng, điều khiển motor bước, điều khiển thiết bị thông qua bluetooth, điều khiển GPRS. Sinh viên đã thật sự hiểu và thực hiện thành công các mô hình đang ứng dụng hiệu quả ở các doanh nghiệp.

Tham luận 2 đề cập đến vấn đề an toàn hệ thống thông tin mạng máy tính. Tìm hiểu các ứng dụng của chữ ký số sử dụng cho doanh nghiệp. Viết chương trình demo để làm tiền đề cho một ứng dụng thực tế quản lý hệ thống văn bản sau này. Trong thời đại công nghệ, bảo mật là vấn đề sống còn đối với doanh nghiệp, sinh viên phải thật sự ý thức và am hiểu về điều đó.

Tham luận 3 đề cập đến kỹ thuật định tuyến mạng Link-state, áp dụng trong giao thức định tuyến OSPF. OSPF là một giao thức định tuyến được áp dụng rộng rãi trong mô hình doanh nghiệp vừa và lớn và tương thích với hầu hết thiết bị trên thị trường. Mô hình cũng như tuần tự các bước thiết lập sẽ được trình bày chi tiết thông qua mô hình ảo hóa.

Ba nội dung trên đều rất cần trong doanh nghiệp hiện nay đồng thời phù hợp với mục tiêu cũng như chuẩn đầu ra của nhà trường.

SỰ TÍCH HỢP GIỮA PHẦN CỨNG VÀ PHẦN MỀM TRONG HỆ THỐNG NHÚNG ĐỂ TỰ TRỊ CÁC THIẾT BỊ MÁY MÓC CHUYÊN DỤNG HIỆN ĐẠI

Tác giả: ThS. NcS VÕ HOA SƠN

Giám đốc công ty Đăng Dũng

1. ĐẶT VẤN ĐỀ

Hiện nay, chúng ta biết máy tính cá nhân là một thiết bị không thể thiếu trong hằng ngày. Tuy nhiên, ở một mảng khác, hệ thống nhúng mới là mối quan tâm lớn cho nhiều quốc gia trên thế giới và nó thực sự là mối quan tâm hàng đầu vì những đặc điểm vượt trội và khả năng phát triển phục vụ đời sống cực cao. Ở Việt Nam, chính phủ và các viện nghiên cứu, các trường đại học đã bắt đầu nhận thấy tầm quan trọng của hệ thống nhúng và đã có những chiến lược phát triển cho phù hợp với lộ trình phát triển của thế giới và khu vực.

Hệ thống nhúng xuất hiện đầu thập niên 1960 và dần dần trở thành một ngành có nhiều ứng dụng rộng rãi trong công nghiệp và đời sống nhờ sự phát triển mạnh mẽ của ngành công nghệ thông tin. Thêm vào đó, dựa vào sức đẩy công nghệ vi điện tử, công nghệ sinh học, công nghệ Nano làm nền tảng cho những sự thay đổi cơ bản trong việc đưa những thiết bị công nghệ vào thị trường với những chức năng thân thiện người dùng có mức độ thông minh ngày càng cao, từ đó khẳng định vai trò của “hệ thống nhúng” trong đời sống.

SmartPhone và SmartHome là những ví dụ điển hình. Nó đã mở ra một triển vọng mà các “đại gia công nghệ” đặt biệt quan tâm và đã lĩnh vực mang lại lợi nhuận khổng lồ mà các quốc gia đều mong muốn đạt được.

Thêm vào đó, các sản phẩm của những doanh nghiệp vừa và nhỏ; họ đã có những đóng góp muôn vàn sản phẩm thiết thực phục vụ cho nhu cầu thực tế sinh động hàng ngày, từ đó đã khẳng định vai trò hết sức to lớn của “Hệ thống nhúng” trong nền kinh tế quốc dân.

2. NỘI DUNG

2.1. Giới thiệu

Hệ thống nhúng (embedded system) được định nghĩa là một hệ thống chuyên dụng, thường có khả năng tự hành và được thiết kế tích hợp vào một hệ thống lớn hơn để thực hiện một chức năng chuyên biệt nào đó.

Hệ thống nhúng bao gồm cả thiết bị phần cứng và phần mềm và các thiết bị hỗ trợ để cùng hoạt động trong môi trường nhúng nhằm phục vụ cho một dự án cụ thể và chúng phải thỏa mãn yêu cầu hoạt động theo thời gian thực (real-time).

Hệ thống nhúng là một phần hệ thống xử lý thông tin nhúng trong hệ thống lớn, phức hợp và độc lập. Đây một hệ thống có khả năng tự trị được nhúng vào trong một môi trường hay một hệ thống mẹ. Chúng là các hệ thống tích hợp cả phần cứng và phần mềm

để thực hiện một hoặc một nhóm chức năng chuyên biệt trong nhiều lĩnh vực công nghiệp, tự động hoá điều khiển, quan trắc và truyền tin. Đặc điểm của các hệ thống nhúng là hoạt động ổn định và có tính năng tự động hoá cao.

Do tính chất chuyên biệt của Hệ thống và chúng được sản xuất hàng loạt với số lượng lớn nên các nhà sản xuất thường yêu cầu phải tối ưu hóa chúng nhằm giảm thiểu kích thước và chi phí sản xuất. những yêu cầu đó đưa đến những khác biệt cơ bản trong lĩnh vực viết phần mềm cho hệ thống nhúng so với phần mềm thông thường.

2.2. Phần cứng và phần mềm trong hệ thống nhúng

Với sự phát triển ngành kỹ thuật, các bộ vi xử lý ngày càng đa dạng: Phong phú về nhà sản xuất, đa dạng về dòng sản phẩm, chủng loại và nhiều giá thành. Ngoài các công ty sản xuất phần cứng như: Texas Instrument, ARM, Intel, Motorola, Atmel, Freescale, AVR...còn có các nhà sản xuất của các quốc gia khác trong đó có Việt Nam đã cho ra những chip xử lý mới phục vụ cho sự phát triển công nghệ.

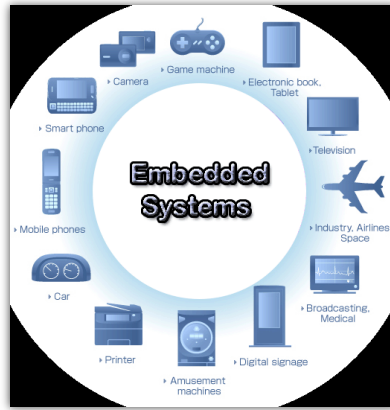
Những Hệ điều hành cho hệ thống nhúng khác nhau như: QNX, VxWorks, Window CE/Xp Embedded, Embedded Linux.....

Ngôn ngữ lập trình : C/C++, Keil C, Assembly, PMC, LabView, PLC....

Ngoài ra, để phục vụ cho cộng đồng công nghệ, các nhà sản xuất còn cho ra những kit xử lý và mã nguồn mở rất tiện ích. Các Modul, Shield....ngày càng hỗ trợ đặc lực cho cộng đồng.

Ngành Hệ thống nhúng có những yêu cầu rất cao cho những người hoạt động trong lĩnh vực này. Ngoài việc rành rẽ về ngôn ngữ lập trình, còn có sự hiểu biết đa dạng về sản phẩm đầu ra như: tự động hóa, y tế, ô-tô, viễn thông, nông nghiệp, công nghiệp... Do đó, những người làm việc ở ngành này phải có khả năng thích ứng cao với nhiều dự án và nhiều lĩnh vực[2].

Thêm vào đó, người lập trình viên cần phải có những kiến thức nhất định về trình biên dịch (compiler), xử lý tín hiệu số, schematic, điện tử...để có thể làm việc hiệu quả. Trong hơn 9 tỷ bộ vi xử lý được sản xuất hằng năm, chỉ có khoảng 150 triệu bộ (1,5%) được sử dụng cho máy vi tính cá nhân, phần còn lại (98,5%) là dành cho hệ thống nhúng[2]. Theo một thống kê khác của BCC Research Group[4] thì đến năm 2009, tổng doanh số của thị trường hệ thống nhúng trên toàn cầu sẽ đạt khoảng 88 tỷ đô-la Mỹ, với phần cứng chiếm 78 tỷ đô-la Mỹ và phần mềm chiếm 3,5 tỷ đô-la Mỹ, phần còn lại là các bo mạch nhúng. Tốc độ tăng trưởng trung bình hằng năm (AAGR) của phần mềm nhúng hiện đang đạt mức 16%.

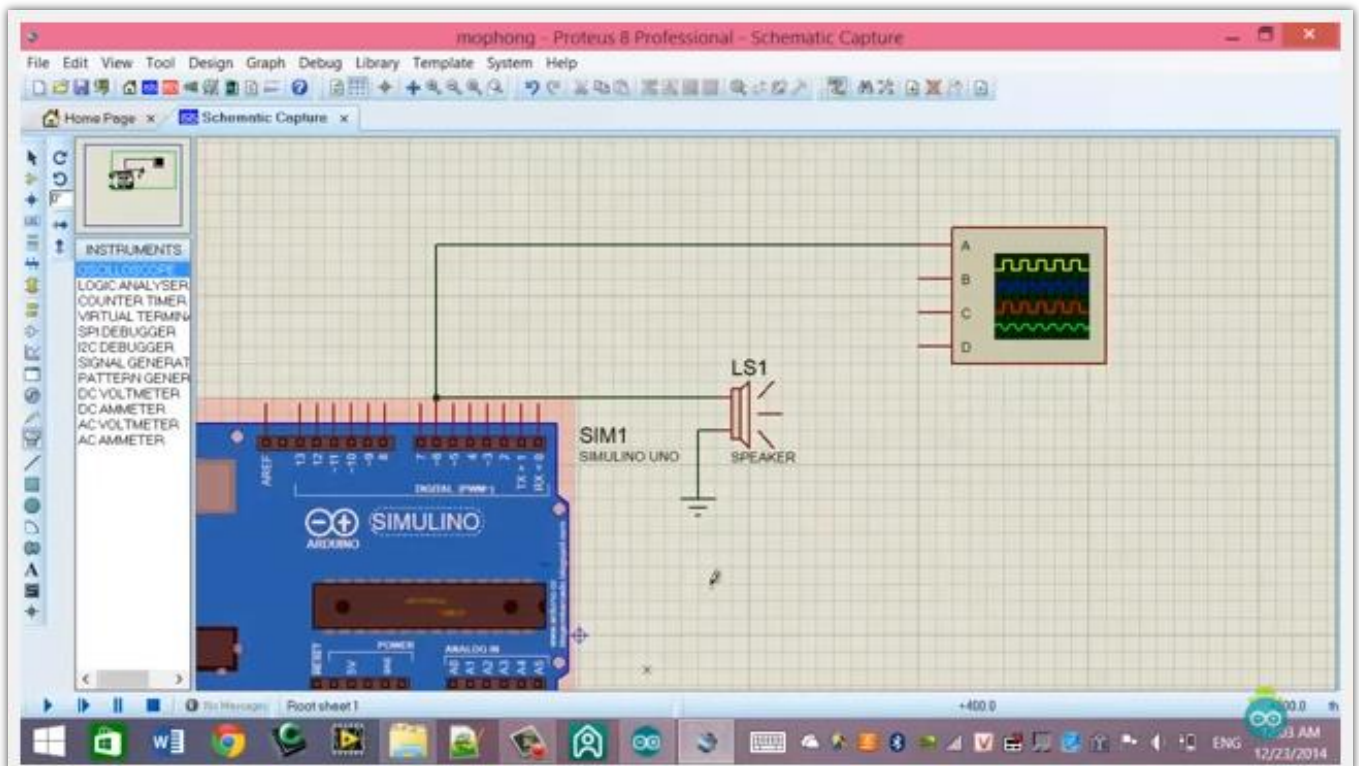


Hình 1. 1 - Ứng dụng của hệ thống nhúng

2.3. Mô phỏng sự tích hợp giữa phần cứng và phần mềm và sản phẩm Hệ thống nhúng

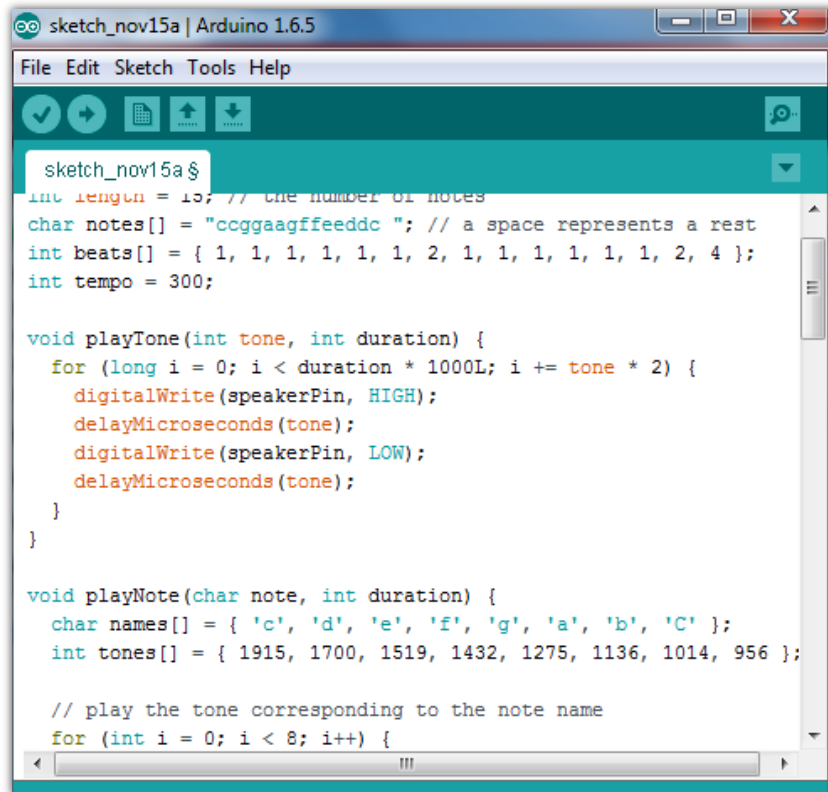
2.3.1. Hộp nhạc quà tặng

- + Phần cứng:Arduino uno R3
- + Phần mềm : Arduino Ide
- + Mô phỏng Proteus
- + Mô phỏng:



Hình 1. 2 - Lược đồ thiết kế hộp nhạc quà tặng

+ Lập trình (Code)



```
sketch_nov15a $
int length = 15; // the number of notes
char notes[] = "ccggaagffeeddc "; // a space represents a rest
int beats[] = { 1, 1, 1, 1, 1, 1, 2, 1, 1, 1, 1, 1, 2, 4 };
int tempo = 300;

void playTone(int tone, int duration) {
  for (long i = 0; i < duration * 1000L; i += tone * 2) {
    digitalWrite(speakerPin, HIGH);
    delayMicroseconds(tone);
    digitalWrite(speakerPin, LOW);
    delayMicroseconds(tone);
  }
}

void playNote(char note, int duration) {
  char names[] = { 'c', 'd', 'e', 'f', 'g', 'a', 'b', 'C' };
  int tones[] = { 1915, 1700, 1519, 1432, 1275, 1136, 1014, 956 };

  // play the tone corresponding to the note name
  for (int i = 0; i < 8; i++) {
```

Hình 1. 3 - Lập trình bằng Arduino

+ Biên dịch



```
sketch_nov15a
void playNote(char note, int duration) {
  char names[] = { 'c', 'd', 'e', 'f', 'g', 'a', 'b', 'C' };
  int tones[] = { 1915, 1700, 1519, 1432, 1275, 1136, 1014, 956 };

  // play the tone corresponding to the note name
  for (int i = 0; i < 8; i++) {
    if (names[i] == note) {
      playTone(tones[i], duration);
    }
  }
}

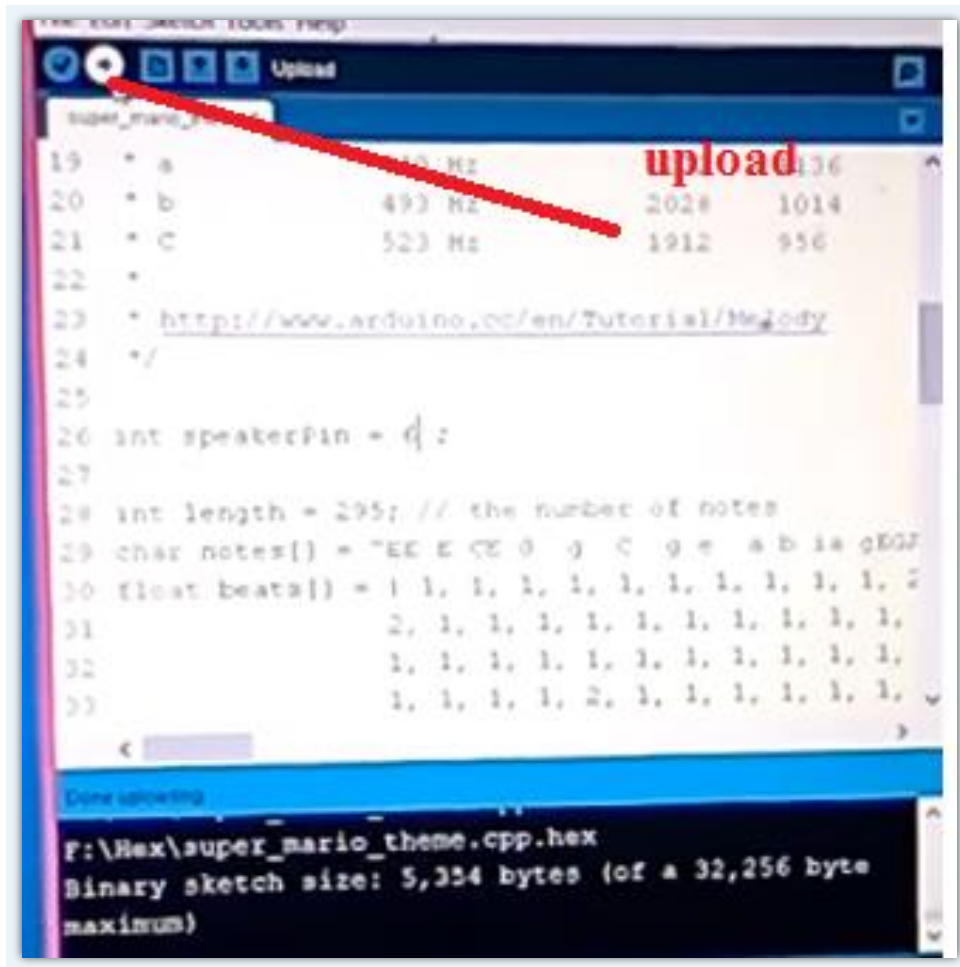
void setup() {
  pinMode(speakerPin, OUTPUT);
}

Done compiling.
C:\Program Files86\Arduino\hardware\tools\avr\bin\avr-ar.exe cs d:\hex\core.a d:\hex\WString.cpp.o
C:\Program Files86\Arduino\hardware\tools\avr\bin\avr-gcc -w -Os -Wl,--gc-sections -mmcu=atmega328p -o
d:\hex\sketch_nov15a.cpp.elf d:\hex\sketch_nov15a.cpp.o d:\hex\core.a -Ld:\hex -lm
C:\Program Files86\Arduino\hardware\tools\avr\bin\avr-objcopy -O ihex -j .eeprom --set-section-flags=.eep
--no-change-warnings --change-section-lma .eeprom=0 d:\hex\sketch_nov15a.cpp.elf d:\hex\sketch_nov15a.cpg
C:\Program Files86\Arduino\hardware\tools\avr\bin\avr-objcopy -O ihex -R .eeprom d:\hex\sketch_nov15a.cpg
d:\hex\sketch_nov15a.cpg.hex
```

biên dịch

Hình 1. 4 - Biên dịch chương trình

+ Nhúng:



Hình 1. 5 - Nhúng vào thiết bị

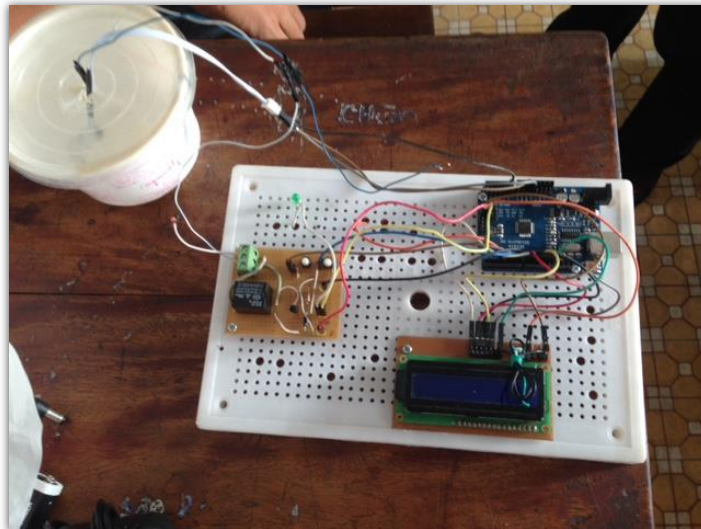
+ Tự hành :



Hình 1. 6 - Vận hành sản phẩm

2.3.2. Lò ấp trứng

- + Phần cứng: Arduino uno R3
- + Cảm biến LM 35
- + LCD
- + Phần mềm: Arduino Ide

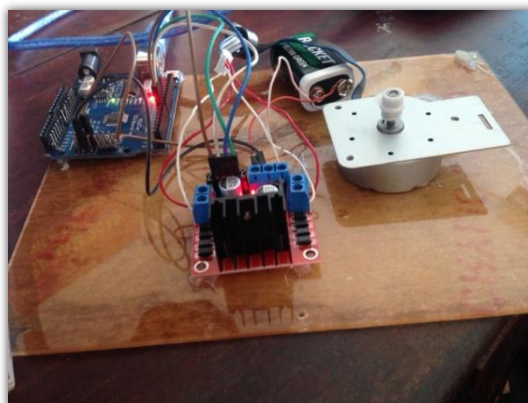


Hình 1. 7 - Mô hình lò ấp trứng (sinh viên thực hiện)

Dự án này có thể mở rộng cho các cơ sở công nghiệp hoạt động có liên quan điều khiển nhiệt độ

2.3.3. Điều khiển moteur bước

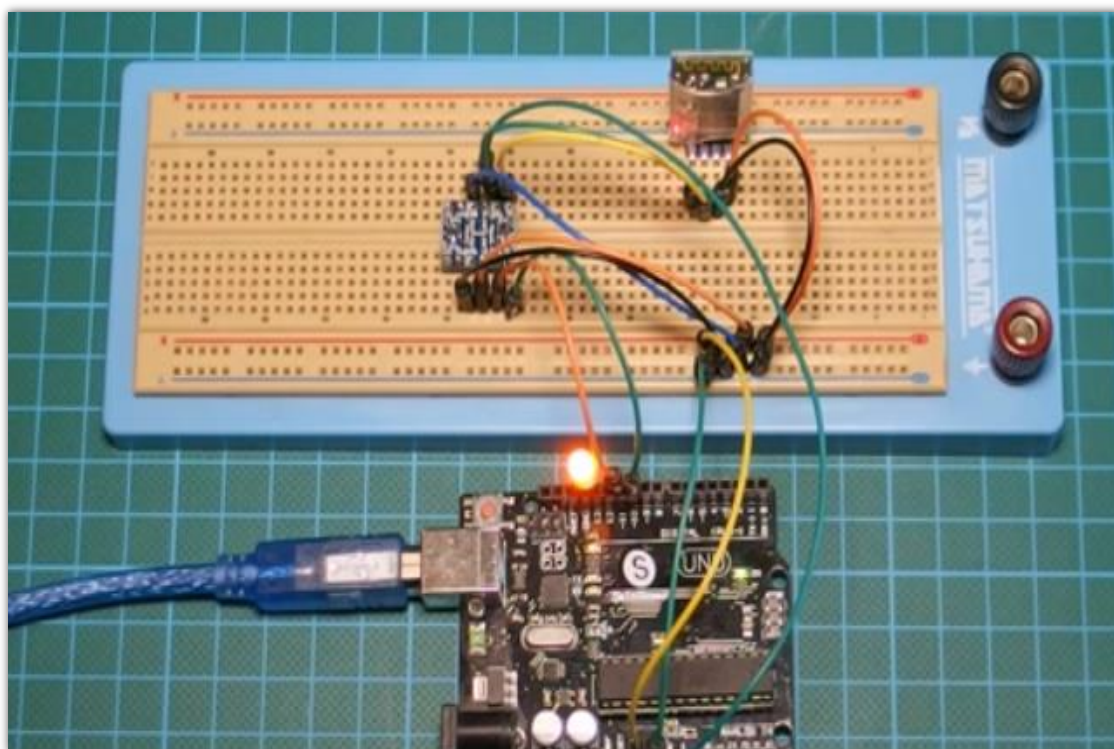
- + Phần cứng: Arduino uno R3
- + Moteur bước
- + Cầu H
- + Phần mềm arduino Ide



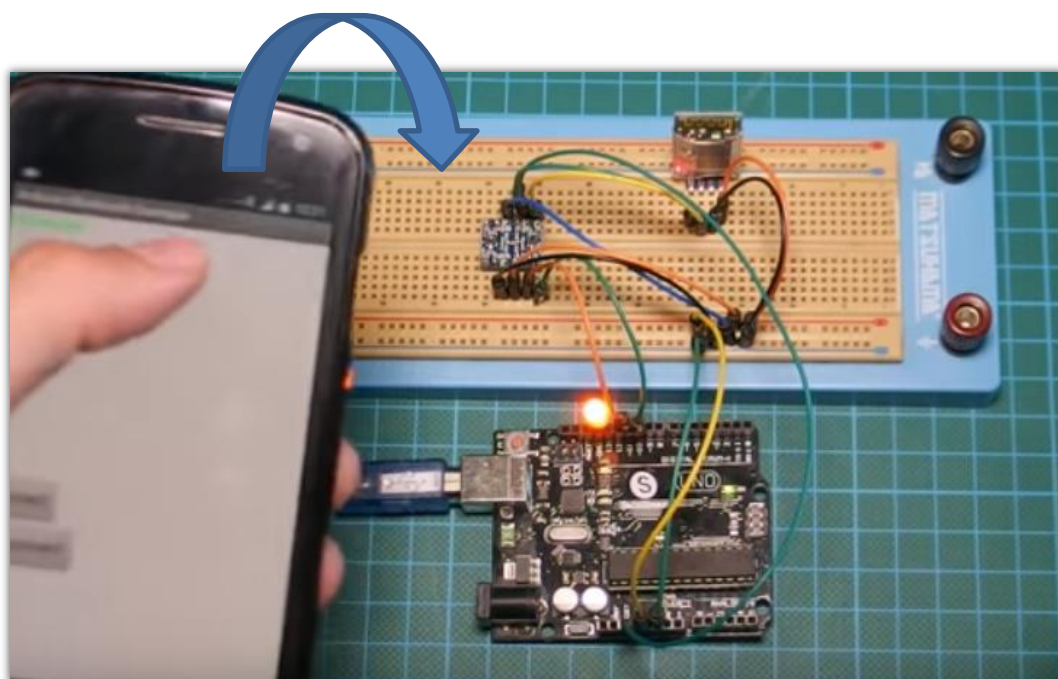
Hình 1. 8 - Mô hình điều khiển moteur (sinh viên thực hiện)

Dự án có thể triển khai các lĩnh vực: Robot, thang máy, moto, nông nghiệp, công nghiệp...

2.3.4. Điều khiển thiết bị qua Bluetooth



Hình 1. 9 - Mạch điều khiển Bluetooth (sinh viên thực hiện)



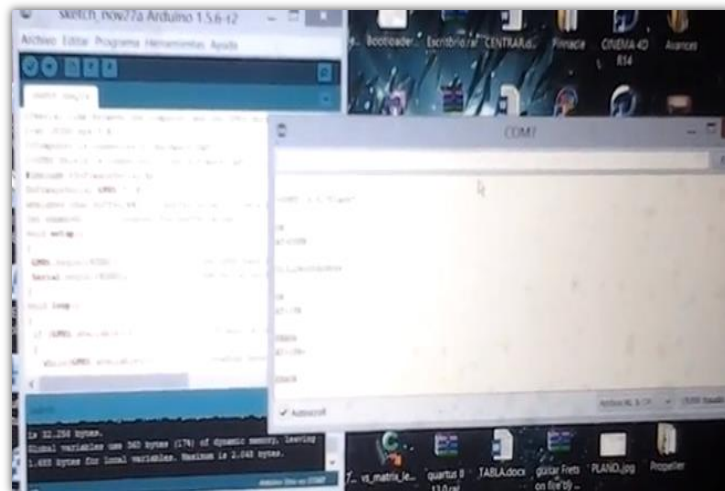
Hình 1. 10 - Thực hiện kết nối Bluetooth

Triển khai dự án: SmartHome, tracking xe, báo động...

2.3.5. Shield sim900 và GPRS



Hình 1. 11 - Mạch Shield sim900 (sinh viên thực hiện)



Hình 1. 12 - Viết chương trình nhúng sim900



Hình 1. 13 - Vận hành sản phẩm sim900

3. PHẦN KẾT

Từ những ví dụ minh họa trên, chúng ta có thể kết luận rằng Hệ thống nhúng là một chuyên ngành rất hấp dẫn và có nhu cầu tuyển dụng cao. Tuy nhiên, chúng ta cần phải định hướng và phát triển hệ thống nhúng theo sát yêu cầu thực tế để hướng dẫn cho sinh

viên phát huy hết khả năng. Chúng ta không chờ đợi những dự án lớn mà hãy bắt đầu bằng những dự án sát với thực tế để phục vụ đời sống, từ đó làm nền tảng cho việc bổ sung nguồn nhân lực Hệ thống nhúng cho đất nước.

Hiện nay, lĩnh vực hệ thống nhúng của Việt Nam đã có những thành quả ban đầu, tuy nhiên chúng ta cũng gặp nhiều thách thức lớn.

Bên cạnh ông “hàng xóm” Trung Quốc với sự phát triển công nghệ vượt bậc làm cho việc sản xuất các chip xử lý (phần cứng) của chúng ta khó có khả năng cạnh tranh được.

Công nghệ phần mềm chúng ta cũng yếu ớt không kém và chủ yếu là gia công cho nước ngoài, do đó có rất nhiều hãng sản xuất phần mềm lớn đã và đang “đổ bộ” vào thị trường Việt Nam để tận dụng lợi thế nguồn nhân lực giá rẻ và khai thác một thị trường tiềm năng mới như IBM, CSC, Altera...

Nếu ta hiểu một cách trực quan thì một hệ thống nhúng về cơ bản có “phần cứng” và “phần mềm”, nếu “phần cứng” là một thực thể “vật lý”, thì “phần mềm” chính là “phần hồn” của hệ thống, như vậy, chúng ta sẽ ưu tiên phần nào đây?

Về chính phủ, đã có những dự án tốn kém cho việc sản xuất chip, nhưng kết quả rất khiêm tốn và lãng phí. Ngược lại, những thiết bị của “kỹ sư chân đất” lại có nhiều ứng dụng thiết thực, có thể xem những “kỹ sư” này đã làm được cái phần “hồn” của nó bằng việc sử dụng phần cứng có sẵn và nhúng vào sản phẩm, đó là việc chúng ta phải nghiêm túc nghiên cứu.

B-Phone cũng vậy, sự tích hợp phần mềm trong hệ thống quyết định thành bại của sản phẩm (dĩ nhiên phần cứng mua về không quá tồi), cái mà người ta trông chờ ở B-Phone chính là sự đột phá trong công nghệ, thổi “cái hồn” vào phần cứng SmartPhone để tạo ra sản phẩm Hệ thống nhúng “Made in Vietnam”, một việc cực kỳ khó khăn trong giai đoạn hiện nay.

Như vậy, việc lựa chọn hướng đi chủ lực nào trong giai đoạn hiện nay để phát triển là chiến lược trong việc phát triển công nghệ, dù rằng cả phát triển phần cứng hay phần mềm cũng đều là thế mạnh của nguồn nhân lực Việt Nam.

Con người là yếu tố quan trọng nhất, việc đào tạo nguồn nhân lực Hệ thống nhúng bắt đầu từ trong nhà trường là một nhu cầu bức thiết và là một nền tảng rất căn bản cho việc phát triển đất nước. Tác giả nhận thấy có 2 việc cần phải thực hiện:

Cần phải có một giáo trình hoàn chỉnh, một đội ngũ giảng viên nhiệt tình và kinh nghiệm. Điều này làm cho các sinh viên hào hứng tiếp thu công nghệ và phát huy tính sáng tạo trong từng sản phẩm cụ thể, làm nền tảng cho các dự án to lớn sau này.

Muốn phát triển ngành phần mềm hệ thống nhúng lên một tầm cao mới như có thể sản xuất, ứng dụng thực tế và xuất khẩu phần mềm hệ thống nhúng, cần phải tập trung nghiên cứu phát triển và hợp tác với các hãng lớn nước ngoài. Hiện nay, Việt Nam đã là đối tác nghiên cứu với các hãng lớn như Toshiba, Panasonic, Samsung..., chúng ta phải biến sự hợp tác này trở thành đối tác chiến lược để nâng cao năng lực đội ngũ chuyên

viên, từ đó sẽ làm chủ công nghệ (kể cả phần cứng và phần mềm) làm tiền đề phát triển đất nước.[4]

TÀI LIỆU THAM KHẢO

- [1] Hải, 2009, *Lập trình hệ thống nhúng sử dụng vi điều khiển MSP430 (Embedded System I)*
- [2] Ngô Đức Hoàng, 2012, *Ngành thiết kế vi mạch Việt Nam: Thiếu thầy, thiếu thợ*, Trung tâm Nghiên cứu và đào tạo thiết kế vi mạch (ICDREC)
- [3] VN. C.Đ.A., *Lập trình vi điều khiển*
- [4] Available from: <http://thanhnt.com/blog/he-thong-nhung-la-gi/>

CHỮ KÝ SỐ RSA ÁP DỤNG GIẢNG DẠY HỌC PHẦN AN NINH MẠNG NÂNG CAO VÀ ỨNG DỤNG TRONG THỰC TIỄN

*Tác giả: ThS. NGUYỄN VĂN ĐÔN
Trưởng bộ môn, Khoa CNTT
Trường CĐ Kỹ thuật Lý Tự Trọng TP.HCM*

4. ĐẶT VẤN ĐỀ

Hiện nay, các giao dịch điện tử đang phát triển mạnh mẽ và là xu thế chung trên toàn cầu. Ở Việt Nam, việc ứng dụng chữ ký số vào cuộc sống không còn xa lạ, đầu tiên là báo cáo thuế qua mạng, sau đó là các hóa đơn điện tử... Ứng dụng công nghệ này đã giúp giải quyết nhiều vấn đề như đáp ứng nhanh chính xác và tiết kiệm thời gian và chi phí.

Việt Nam đã có hệ thống luật, văn bản và thông tư hướng dẫn cụ thể cho vấn đề này. Hầu hết các doanh nghiệp lớn đã và đang triển khai các hệ thống thanh toán, hóa đơn chứng từ điện tử.

Tuy không phải là mới, nhưng nhiều doanh nghiệp còn e ngại và chưa nắm rõ được tính ưu việt cũng như tính an toàn của công nghệ này. Trong các chương trình đào tạo, cũng chưa cập nhật đầy đủ nên sinh viên ra trường còn rất ngỡ ngàng khi tiếp cận các hệ thống này.

Cùng với sự phát triển của công nghệ, mà đặc biệt là một chiếc smartphone, chúng ta có thể có (gần như tức thời) các thông tin về: tình hình hoạt động doanh nghiệp, chính sách, thuế, điện, nước... và không còn tốn thời gian chạy đến các cơ quan đối tác để chỉ ký một chữ ký.

Vấn đề ở đây là an toàn mạng có được đảm bảo hay không? Học phần “An ninh mạng nâng cao” đã đề cập đến vấn đề này nhưng chưa thật sự đầy đủ. Tham luận này giúp cho giảng viên, sinh viên có được các kiến thức, thông tin và ứng dụng thực tiễn của chữ ký số.

5. NỘI DUNG

5.1. Tổng quan về chữ ký số

5.1.1. Một số khái niệm

- **Chữ kí số** (Digital Signature) là một chuỗi dữ liệu liên kết với một thông điệp (message) và thực thể tạo ra thông điệp.
- **Giải thuật tạo ra chữ ký số** (Digital Signature Generation Algorithm) là một phương pháp sinh chữ ký số.
- **Giải thuật kiểm tra chữ ký số** (Digital Signature Verification Algorithm) là một phương pháp xác minh tính xác thực của chữ ký số, có nghĩa là nó thực sự được tạo ra bởi một bên chỉ định.

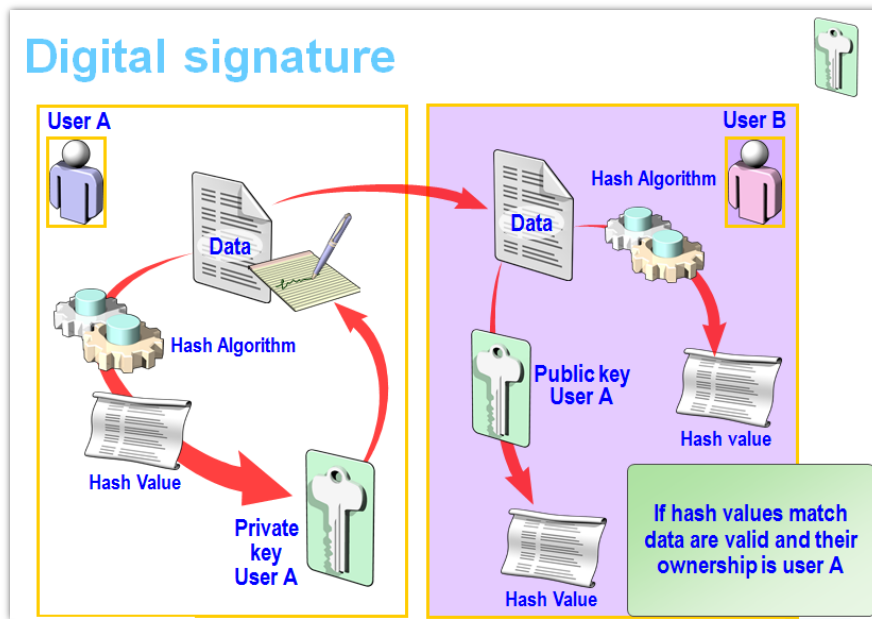
- **Một hệ chữ ký số** (Digital Signature Scheme) bao gồm giải thuật tạo chữ số và giải thuật kiểm tra chữ ký số.
- **Quá trình tạo chữ ký số** (Digital Signature Signing Process) bao gồm:
 - + Giải thuật tạo chữ ký số
 - + Phương pháp chuyển dữ liệu thông điệp thành dạng có thể ký được
- **Quá trình kiểm tra chữ ký số** (Digital Signature Verification Process) bao gồm:
 - + Giải thuật kiểm tra chữ ký số
 - + Phương pháp khôi phục dữ liệu từ thông điệp
- **Hàm băm** (Hash Function) làm hàm toán học chuyển đổi thông điệp (message) có độ dài bất kỳ (hữu hạn) thành một dãy bit có độ dài cố định (tùy thuộc vào thuật toán băm). Dãy bit này được gọi là thông điệp rút gọn MD (Message Digest) hay giá trị băm (hash value), đại diện cho thông điệp ban đầu.
 - + Hàm băm SHA-1: Thuật toán SHA-1 nhận thông điệp ở đầu vào có chiều dài $k < 264$ bits, thực hiện xử lý và đưa ra thông điệp thu gọn MD có chiều dài cố định 160 bits. Quá trình tính toán cũng thực hiện theo từng khối 512 bits, nhưng bộ đệm xử lý dùng 5 thanh ghi 32 bits. Thuật toán này chạy tốt với các bộ vi xử lý có cấu trúc 32 bits.

5.1.2. Lược đồ chữ ký số RSA

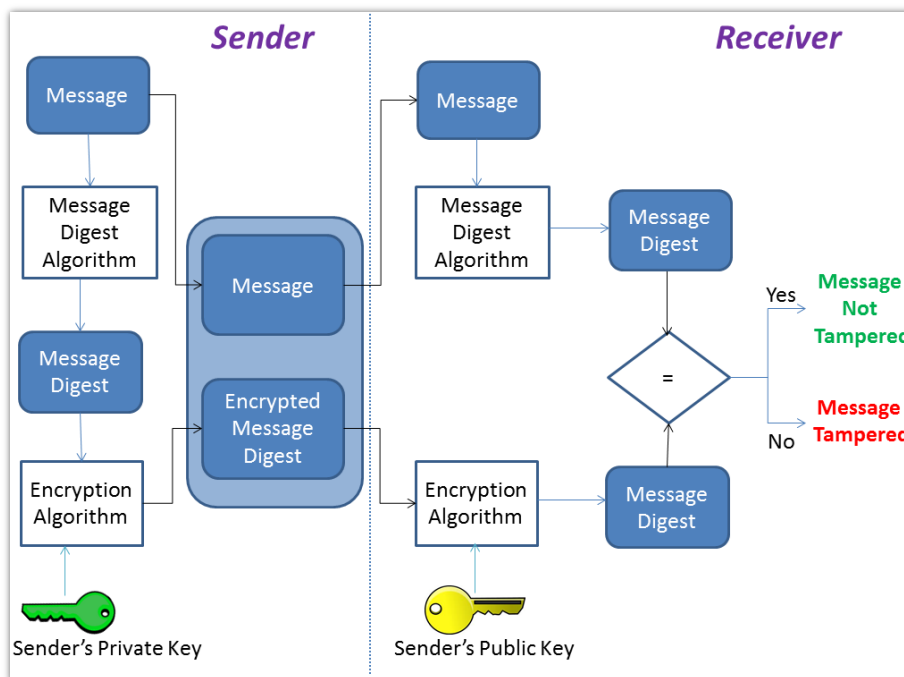
Độ an toàn của lược đồ chữ ký RSA dựa vào độ an toàn của hệ mã RSA. Lược đồ bao gồm cả chữ ký số kèm theo bản rõ và tự khôi phục thông điệp từ chữ ký số.

- Thuật toán sinh khóa cho lược đồ chữ ký RSA
- Thuật toán sinh chữ ký RSA
- Thuật toán chứng thực chữ ký RSA

5.1.3. Kiến trúc tổng quát



Hình 2. 1 - Kiến trúc tổng quát của chữ ký số

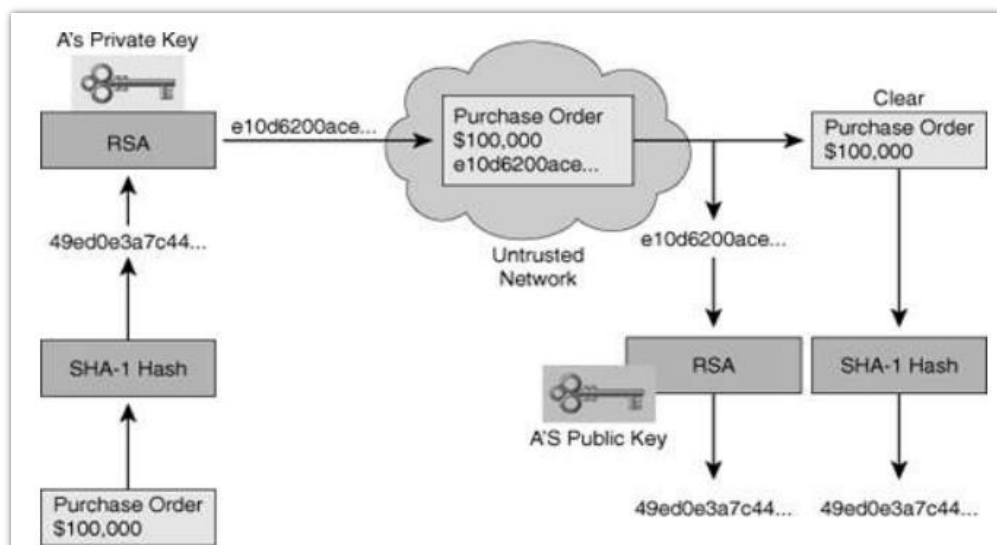


Hình 2. 2 - Sơ đồ khối kiến trúc của chữ ký số

- Quá trình ký (bên gửi)
 - + Tính toán chuỗi đại diện (message digest/ hash value) của thông điệp sử dụng một giải thuật băm (hashing algorithm)
 - + Chuỗi đại diện được ký sử dụng khóa riêng (private key) của người gửi và một giải thuật tạo chữ ký (signature/encryption algorithm). Kết quả chữ ký số (digital signature) của thông điệp hay còn gọi là chuỗi đại diện được mã hóa (encrypted message digest)

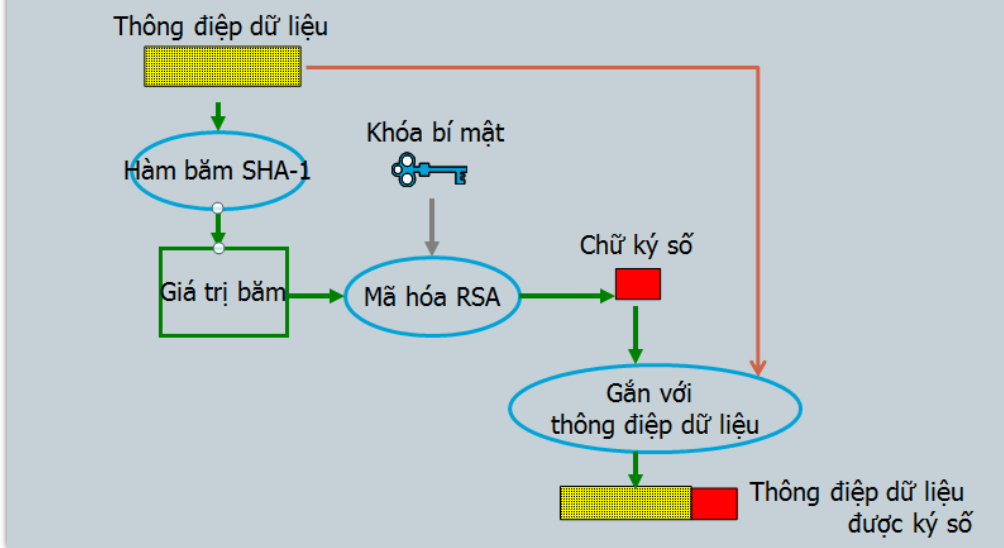
- + Thông điệp ban đầu (message) được ghép với chữ ký số (digital signature) tạo thành thông điệp đã được ký (signed message)
- + Thông điệp đã được ký (signed message) được gửi cho người nhận
- Quá trình kiểm tra chữ ký (bên nhận)
 - + Tách chữ ký số và thông điệp gốc khỏi thông điệp đã ký để xử lý riêng;
 - + Tính toán chuỗi đại diện MD1 (message digest) của thông điệp gốc sử dụng giải thuật băm (là giải thuật sử dụng trong quá trình ký)
 - + Sử dụng khóa công khai (public key) của người gửi để giải mã chữ ký số được chuỗi đại diện thông điệp MD2
 - + So sánh MD1 và MD2:
 - Nếu MD1 = MD2 thì chữ ký kiểm tra thành công. Thông điệp đảm bảo tính toàn vẹn và thực sự xuất phát từ người gửi (do khóa công khai được chứng thực).
 - Nếu MD1 $\neq$ MD2 thì chữ ký không hợp lệ. Thông điệp có thể đã bị sửa đổi hoặc không thực sự xuất phát từ người gửi.

5.2. Thuật toán SHA-1



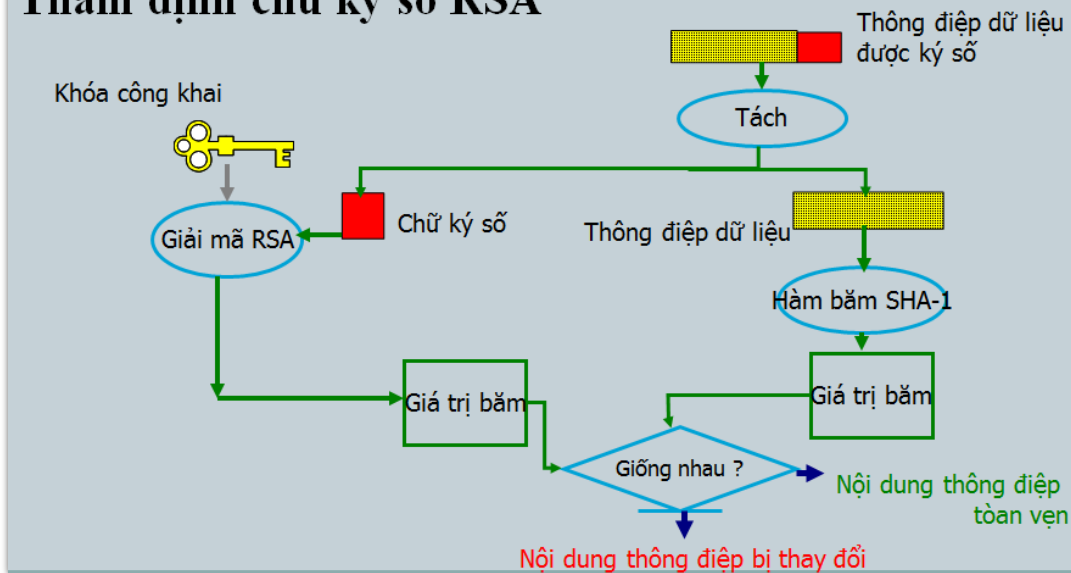
Hình 2. 3 - Sơ đồ áp dụng thuật toán SHA-1

Tạo chữ ký số RSA



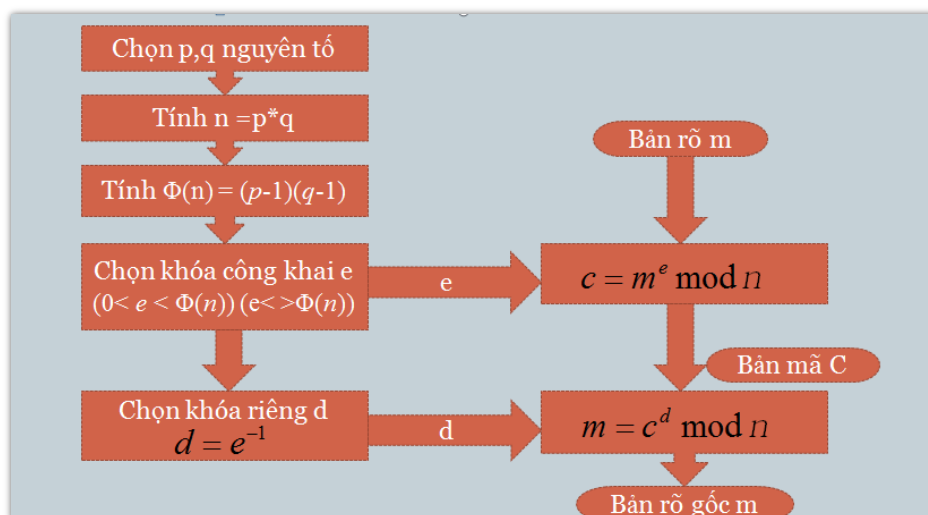
Hình 2. 4 - Sơ đồ chi tiết tạo chữ ký số bằng SHA-1

Thẩm định chữ ký số RSA



Hình 2. 5 - Sơ đồ chi tiết thẩm định chữ ký số

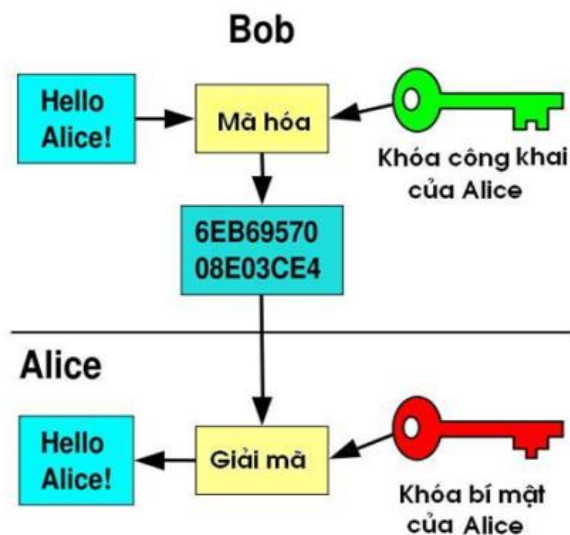
5.2.1. Thuật toán RSA



Hình 2. 6 - Sơ đồ thuật toán RSA

Thuật toán RSA có hai Khóa:

- Khóa công khai* (Public Key): được công bố rộng rãi cho mọi người và được dùng để mã hóa.
- Khóa bí mật* (Private Key): Những thông tin được mã hóa bằng khóa công khai chỉ có thể được giải mã bằng khóa bí mật tương ứng.



Hình 2. 7 - Cặp khóa Public và Private

Tạo khóa

Lý thuyết

Bước 1: B (người nhận) tạo hai số nguyên tố lớn ngẫu nhiên p và q

Bước 2: tính $n=p*q$ và $\Phi(n) = (p-1)(q-1)$

Bước 3: chọn một số ngẫu nhiên e ($0 < e < \Phi(n)$) sao cho $\text{ƯCLN}(e, \Phi(n))=1$

Bước 4: tính $d = e^{-1}$ bằng cách dùng thuật toán Euclide
Tìm số tự nhiên x sao cho $d = \frac{x * \Phi(n) + 1}{e}$

Bước 5:

- n và e làm khoá công khai (**public key**),
- d làm khoá bí mật (**private key**).

Ví dụ:

Bước 1: Chọn số **23** và **41**
(hai số này là 2 số nguyên tố)

Bước 2: $n = 23 * 41 = 943$
 $\Phi(n) = 22 * 40 = 880$

Bước 3:

chọn $e = 7$ vì $\text{ƯCLN}(7, 880)=1$

Bước 4: $d = \frac{x * \Phi(n) + 1}{e} \Rightarrow 7d = 1 + 880x$
 $\Rightarrow d = 503$ và $x = 4$

Bước 5:

- $n = 943$ và $e = 7$
- $d = 503$

Hình 2. 8 - Quá trình tạo khóa

Mã hoá và giải mã

Lý thuyết

Bước 1: A nhận khoá công khai của B.

Bước 2: A biểu diễn thông tin cần gửi thành số m ($0 \leq m \leq n-1$)

Bước 3: Tính $c = m^e \bmod n$

Bước 4: Gửi c cho B

Bước 5: Giải mã
tính $m = c^d \bmod n$
 $\Rightarrow m$ là thông tin nhận được.

Ví dụ:

Bước 1: A nhận khoá công khai
 $n = 943$ và $e = 7$

Bước 2: Thông tin cần gửi
 $m = 35$

Bước 3: $c = 35^7 \bmod 943$

Bước 4: $c = 545$

Bước 5: Giải mã

$m = 545^{503} \bmod 943$
 $\Rightarrow m = 35$

Hình 2. 9 - Quá trình giải mã

5.2.2. Cài đặt (ngôn ngữ JAVA)

Sử dụng `java.math.*` cung cấp hầu hết các hàm sử dụng để cài đặt

- `BigInteger (int bitLength, int certainty, Random rnd)`, sinh số nguyên tố ngẫu nhiên với số bit cho trước.
- `BigInteger add(BigInteger val)`, cộng 2 số nguyên lớn.
- `BigInteger subtract(BigInteger val)`, trừ 2 số nguyên lớn.
- `BigInteger multiply(BigInteger val)`, nhân 2 số nguyên lớn.
- `gcd(BigInteger val)`, tìm USCLN của 2 số lớn.
- `mod(BigInteger m)` tính modulo (phần dư) của phép chia nguyên.

- `BigInteger modInverse(BigInteger m)`, tính modulo nghịch đảo.
- `BigInteger modPow(BigInteger exponent, BigInteger m)`, tính $(this \text{ exponent mod } m)$.

```

51 public void KeyRSA(int bits){
52     SecureRandom r = new SecureRandom();
53     BigInteger p = new BigInteger(bits / 2, 100, r);
54     BigInteger q = new BigInteger(bits / 2, 100, r);
55     n = p.multiply(q);
56     BigInteger m = (p.subtract(BigInteger.ONE)).multiply(q
57         .subtract(BigInteger.ONE));
58     boolean found = false;
59     do {
60         e = new BigInteger(bits / 2, 50, r);
61         if (m.gcd(e).equals(BigInteger.ONE) && e.compareTo(m) < 0) {
62             found = true;
63         }
64     } while (!found);
65     d = e.modInverse(m);
66
67 }

```

Hình 2. 10 - Hàm tạo khóa

5.3. Ứng dụng thực tiễn

5.3.1. Hóa đơn điện tử

Tập hợp các thông điệp dữ liệu điện tử về bán hàng hoá, cung ứng dịch vụ, được khởi tạo, lập, gửi, nhận, lưu trữ và quản lý theo quy định tại Luật Giao dịch điện tử và các văn bản hướng dẫn thi hành. Hóa đơn điện tử khác với hóa đơn tự in ở những điểm sau:

Hóa đơn điện tử ở dạng dữ liệu điện tử lưu trên máy tính, sử dụng chữ ký điện tử để đảm bảo tính pháp lý. Hóa đơn điện tử phải sử dụng các biên nhận thanh toán để thu tiền. Khi kê khai thuế sử dụng phần mềm để xác thực công tác kê khai của khách hàng.

Ưu điểm:

Về hoạt động: Nâng cao năng lực cạnh tranh, hiện đại hoá quản trị doanh nghiệp, giúp doanh nghiệp kê khai thuế nhanh chóng, kết nối trực tiếp đến hệ thống kế toán.

Về mặt xã hội: Giảm thanh toán tiền mặt, góp phần bảo vệ môi trường (không sử dụng hoá đơn giấy).

Về chi phí: Giảm chi phí in, gửi, bảo quản, lưu trữ hóa đơn.

Về thanh toán: Việc thanh toán sẽ nhanh hơn do việc lập, gửi/nhận hóa đơn được thực hiện thông qua các phương tiện điện tử được áp dụng các hình thức thanh toán tiên tiến như: Internet Banking, SMS Banking



Hình 2. 11 - Máy P.O.S và hóa đơn điện tử

“Cầm máy P.O.S in biên nhận hoặc thông báo trực tiếp khi thu tiền Theo EVN Hà Nội, để hòa nhập với xu hướng phát triển của công nghệ thông tin và thực hiện tốt chủ trương của Chính phủ tại Thông tư số 32/2011/TT-BTC ngày 14/3/2012 của Bộ Tài Chính về việc hướng dẫn khởi tạo và sử dụng hóa đơn điện tử bán hàng hóa, cung ứng dịch vụ và văn bản số 1137/TCT-DNL ngày 30/3/2012 của Tổng cục thuế về hướng dẫn thực hiện hóa đơn điện tử, văn bản số 28924/CT-QLAC của Cục thuế Hà Nội về việc phát hành, sử dụng hóa đơn điện tử tiền điện, EVN Hà Nội triển khai thí điểm chuyển đổi từ hình thức hóa đơn tiền điện dạng giấy sang hình thức hóa đơn điện tử tại quận Hoàn Kiếm và quận Cầu Giấy.” (Theo vietnamnet.vn)



Hình 2. 12 - Máy rút tiền tự động

a. Phòng chống virus

Quét virus online là công việc nên làm khi mà máy tính của bạn không cài đặt bất cứ một phần mềm diệt virus nào. Hiện nay, nhiều phần mềm, chương trình tải về từ Internet khi cài đặt thường bị dính kèm virus. Virustotal.com được đánh giá tốt nhất với khả năng phân tích, phát hiện virus, các chương trình độc hại tốt nhất hiện nay. Nó có thể xử lý đối với tập tin upload lên hoặc đường dẫn URL trang web hoặc địa chỉ tải tập tin bất kì.



The screenshot shows the VirusTotal website. At the top is the VirusTotal logo. Below it, a paragraph describes the service as free and capable of analyzing files and URLs. There are three tabs: 'Tập tin' (Files), 'Đường dẫn URL' (URLs), and 'Tìm kiếm' (Search). The 'Tập tin' tab is selected. Below the tabs is a file upload area with a text box containing 'Chưa chọn tập tin' and a 'Chọn tập tin' button. Below this, it states the maximum file size is 128MB. A disclaimer mentions that using the service implies agreement with the terms of service. At the bottom is a large blue button labeled 'Quét!' (Scan!).

Hình 2. 13 - Giao diện virustotal quét tập tin



The screenshot shows a dialog box titled 'Đang tải tập tin lên...' (Uploading file...). It contains the following text: 'Vui lòng chờ, không đóng cửa sổ cho đến khi quá trình tải lên kết thúc.' (Please wait, do not close the window until the upload process is complete.), 'Thời gian yêu cầu cho hoạt động này phụ thuộc vào kích thước tập tin, mức độ sử dụng và tốc độ kết nối mạng.' (The time required for this activity depends on the file size, usage level, and network connection speed.), and 'Đang tải tập tin lên...' (Uploading file...). At the bottom is a red progress bar.

Hình 2. 14 - Virustotal tải tập tin lên để quét (cho phép 128MB)



SHA256: ff840d798744e5d9bde00cd26471e59fa3c6dba44e63654965317c48962588eb

Tên tập tin: Crck + Serial Key.rar

Tỷ lệ phát hiện: 1 / 55

Ngày phân tích: 2015-06-30 14:52:06 UTC (2 phút trước)

Phân tích Chi tiết về tập tin Thông tin khác Ý kiến 0 Đánh giá

Chương trình	Kết quả	Cập nhật
Symantec	WS.Reputation.1	20150630
ALYac	✓	20150630
AVG	✓	20150630
AVware	✓	20150630
Ad-Aware	✓	20150630
AegisLab	✓	20150630
Agnitum	✓	20150629
AhnLab-V3	✓	20150630

Hình 2. 15 – Kết quả virustotal phát hiện 1/55



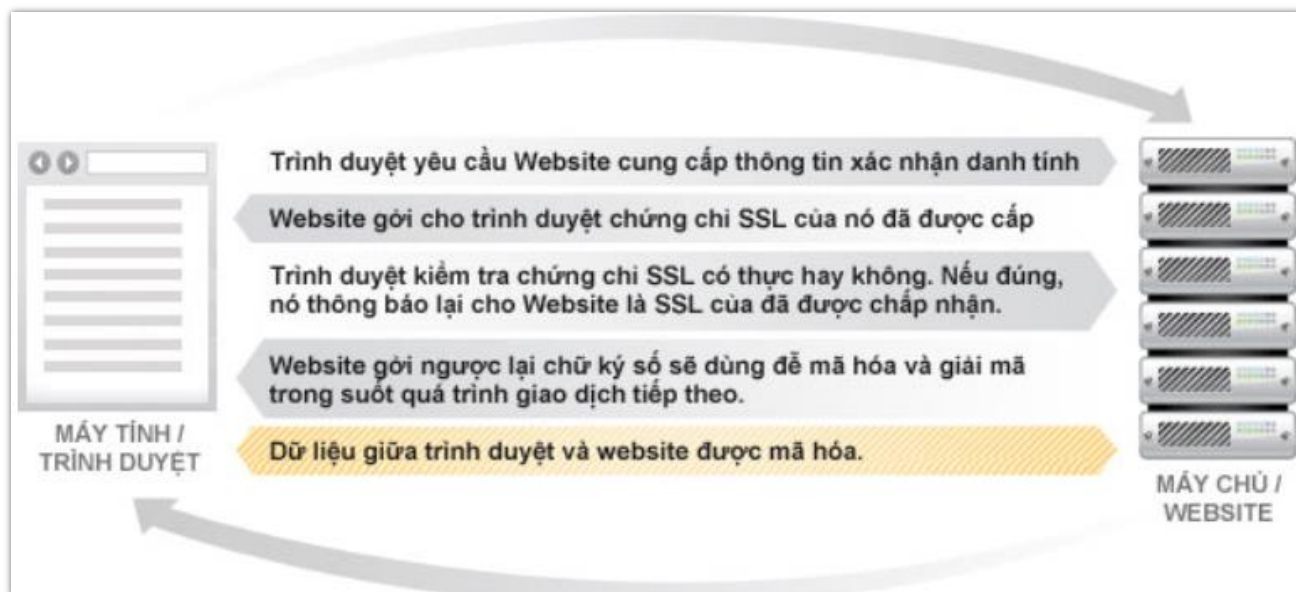
URL: http://ltd.edu.vn/

Tỷ lệ phát hiện: 0 / 66

Ngày phân tích: 2015-11-12 03:38:22 UTC (0 phút trước)

Hình 2. 16 – Kết quả virustotal quét URL

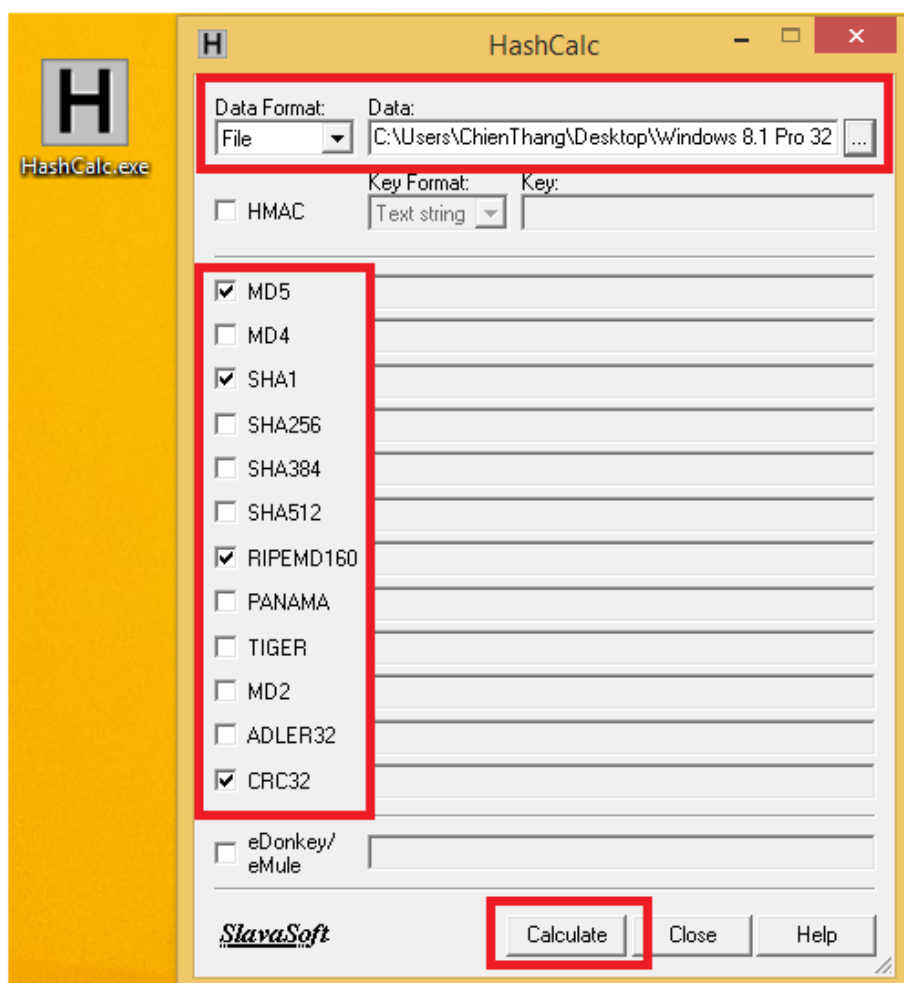
5.3.2. Kiểm tra tính toàn vẹn dữ liệu



Hình 2. 17 - Duyệt web an toàn (SSL)



Hình 2. 18 - Một số nhà cung cấp chứng chỉ số



Hình 2. 19 - Phần mềm HashCalc tính mã băm bằng nhiều giải thuật

5.3.3. Token con dấu điện tử



Hình 2. 20 - Token OTP



Hình 2. 21 - Giao diện chương trình demo

5.4. Các hạn chế của chữ ký số

Sự lệ thuộc vào máy móc và chương trình phần mềm: chữ ký số là một chương trình phần mềm máy tính. Để kiểm tra tính xác thực của chữ ký cần có hệ thống máy tính và phần mềm tương thích. Đây là hạn chế chung khi sử dụng văn bản điện tử và chữ ký số.

Tính bảo mật không tuyệt đối: Nếu chữ ký bằng tay được thực hiện trên giấy, được ký trực tiếp và luôn đi kèm với vật mang tin, chữ ký tay không thể chuyển giao cho người khác, thì chữ ký số không như vậy. Chữ ký số là một bộ mật mã được cấp cho người sử dụng, đây là phần mềm máy tính không phụ thuộc vào vật mang tin. Chính vì vậy, trở ngại lớn nhất khi sử dụng chữ ký số là khả năng tách biệt khỏi chủ nhân của chữ ký. Nói cách khác, chủ nhân của chữ ký số không phải là người duy nhất có được mật mã của chữ ký. Tồn tại một số nhóm đối tượng có thể có được mật mã, đó là: bộ phận cung cấp phần mềm; bộ phận cài đặt phần mềm, những người có thể sử dụng máy tính có cài đặt phần mềm. Ngoài ra, mật mã có thể bị đánh cắp. Cũng có thể, chủ nhân chữ ký số chuyển giao cho người khác mật mã của mình. Như vậy, tính bảo mật của chữ ký số không phải là tuyệt đối.

Vấn đề bản gốc, bản chính: Nếu đối với tài liệu giấy, chữ ký được ký một lần và chỉ có một bản duy nhất (được coi là bản gốc). Bản gốc được ký bằng chữ ký sẽ không thể cùng lúc ở hai chỗ khác nhau. Có thể tin tưởng rằng, nếu bản gốc duy nhất mất đi thì sẽ không thể có bản thứ hai giống hệt như vậy. Nhưng với văn bản điện tử đã được ký bằng

chữ ký số, người ra có thể copy lại và bản copy từ bản chính và bản copy từ bản copy không có gì khác biệt so với bản chính duy nhất được ký. Đây là một thách thức đối với công tác văn bản và cả nền hành chính. Khái niệm bản gốc, bản chính trong văn bản hành chính sẽ phải xem xét lại đối với văn bản điện tử.

Sự có thời hạn của chữ ký điện tử. Chữ ký điện tử là chương trình phần mềm được cấp có thời hạn cho người sử dụng. Về lý thuyết, văn bản sẽ có hiệu lực pháp lý khi được ký trong thời hạn sử dụng của chữ ký. Tuy nhiên, thực tế hiệu lực pháp lý của văn bản hoàn toàn có thể bị nghi ngờ khi chữ ký số hết thời hạn sử dụng. Đây cũng là một hạn chế và thách thức rất lớn đối với việc sử dụng chữ ký số.

6. PHẦN KẾT

Tham luận giới thiệu được kiến trúc, cài đặt giải thuật, các điểm yếu của chữ ký số sử dụng giải thuật RSA. Cài đặt được chương trình demo bằng ngôn ngữ Java. Giới thiệu các ứng dụng thực tế hiện nay của giải thuật SHA-1.

Hướng phát triển của đề tài là hoàn thiện một chương trình có thể xác thực được nội dung văn bản để áp dụng trong nhà trường. Ứng dụng này cho phép xác định nguồn gốc và tính toàn vẹn của văn bản (vd: đề thi). Để đảm bảo rằng văn bản là hợp lệ, không bị sửa đổi.

TÀI LIỆU THAM KHẢO

- [1] Hoàng Xuân Dậu, 2015, *Giáo trình An Toàn Bảo Mật Hệ Thống Thông Tin*
- [2] <http://vi.wikipedia.org/wiki/RSA>
- [3] <http://docs.oracle.com/javase/7/docs/api/java/math/BigInteger.html>
- [4] http://www.java2s.com/Tutorial/Java/0490__Security/UseSHA1.htm

ĐỊNH TUYỂN BẰNG GIAO THỨC LINK-STATE (OSPF) THÔNG QUA THIẾT BỊ ROUTER CỦA CISCO ỨNG DỤNG GIẢNG DẠY HỌC PHẦN THIẾT LẬP HỆ THỐNG MẠNG

Tác giả: CN. DƯƠNG NGỌC VỌNG

Giảng viên, Khoa CNTT

Trường CĐ Kỹ thuật Lý Tự Trọng TP.HCM

1. ĐẶT VẤN ĐỀ

Trong những năm qua, việc giảng dạy môn TLHTM (Thiết lập hệ thống mạng) đối với các hệ Trung cấp chuyên nghiệp và Cao đẳng vẫn đang thực hiện theo chương trình khung. Là giảng viên đã từng nhiều năm giảng dạy môn học này, nhận thấy những hạn chế nhất định về nội dung của chương trình chi tiết chưa mang tính cập nhật cao. Đặc biệt đối với những sinh viên chuyên ngành mạng khi học tại trường, thì kiến thức trọng tâm cũng như kỹ năng thực hành cho môn học này chiếm hơn 50%. Hơn nữa, khi sinh viên thi tốt nghiệp thì môn thi thực hành nghề nghiệp được chọn mà trong đó lượng kiến thức chiếm gần hết chính là môn Thiết lập hệ thống mạng. Vậy vấn đề cần đặt ra ở đây là với hàm lượng kiến thức cũng như kỹ năng như vậy sinh viên có đủ tự tin khi tham gia vào thị trường tuyển dụng lao động hay không.

Thêm một yếu tố nữa là việc giảng dạy môn học này vẫn dạy chưa đi sâu vào công nghệ của hãng sản xuất thiết bị mạng hàng đầu hiện nay là Cisco. Cụ thể như phần định tuyến mạng, vẫn thực hiện trên router mềm RRAS (Routing Remote Access Service) của Microsoft. Vốn chỉ phục vụ giảng dạy là chính, không thể thực hiện một cách khả thi trong môi trường thực (dùng một máy tính PC bình thường làm chức năng Router). Thậm chí có một số giao thức định tuyến cũ được tích hợp trong môi trường hệ điều hành Windows của Microsoft như giao thức RIP V2 cũng không còn được sử dụng nhiều. Đặc biệt hơn trong tài liệu mới nhất của Cisco cũng không còn nhắc đến.

Ngoài ra, người dạy cũng nhận ra thêm một số yếu tố khó khăn như: Việc trang bị cho một hệ thống theo hướng Cisco là quá đắt tiền, giáo viên khó tiếp cận với trang thiết bị để nâng cao kỹ năng chuyên môn. Tuy nhiên, bên cạnh những khó khăn vừa nêu cũng có những mặt thuận lợi khi chính hãng Cisco cũng đã hỗ trợ người dùng một số phần mềm ảo hóa, tương tác trên thiết bị ảo thông qua Package Tracer, GNS3 và những công cụ hỗ trợ từ những hãng khác nhau.

Đối với phần mềm Package Tracer đó là người dùng chỉ thao tác trên toàn bộ thiết bị thuần Cisco, mặc hạn chế là không giao tiếp được với các thiết bị đầu cuối (terminal) chạy hệ điều hành Windows, Linux, Androi... và hạn chế về tập lệnh trên mỗi phiên bản của thiết bị.

Phần mềm GNS3 thì có nhiều thuận lợi hơn vì người dùng trực tiếp cấu hình trên hệ điều hành IOS image ảo như là đang cấu hình với thiết bị thực (Vì chính thiết bị thực cũng đang chạy IOS image này). Ngoài ra phần mềm cũng giao tiếp được với các

hệ điều hành thương mại hiện nay... Như vậy rất thuận lợi khi sinh viên vừa học theo hướng Microsoft vừa có thể kết nối để tham gia vào hệ thống hạ tầng mạng Cisco cũng như những hãng khác.

Trong bài biết này tôi có đã chọn phần mềm GNS3 để thực hiện minh họa phần định tuyến mạng trên thiết bị Cisco. Có nhiều giao thức định tuyến thông dụng hiện nay như giao thức định tuyến tĩnh (Static Route) và định tuyến động. Trong những giao thức đó, ngoài giao thức định tuyến tĩnh có hai giao thức định tuyến động phổ biến hiện nay đó là giao thức EIGRP (Distance Vector) và giao thức OSPF (Link-state). Giao thức EIGRP vốn là giao thức chuẩn của Cisco, còn OSPF vốn phổ biến vừa cho thiết bị Cisco vừa cho các thiết bị của những hãng khác.

Trong bài tham luận này, tác giả chọn giao thức OSPF để trình bày nội dung chính là “Định tuyến bằng giao thức Link-state (OSPF) thông qua thiết bị router của Cisco”. Với chủ đề này tác giả không đi sâu quá vào chi tiết của giao thức mà chỉ trình bày khái quát sau đó là tập trung vào yếu tố mang tính kỹ năng ứng dụng vào môi trường vừa kết hợp yếu tố giữa thiết bị Cisco và các hệ thống xử lý trạm cuối của những hãng như Microsoft và môi trường Linux. Tác giả cũng nhận thức rằng trong quá trình tham gia viết bài tham luận vẫn tồn tại những mặt hạn chế nhất định và không tránh khỏi sai sót, mong quý đồng nghiệp góp ý để cho những lần sau được tốt hơn.

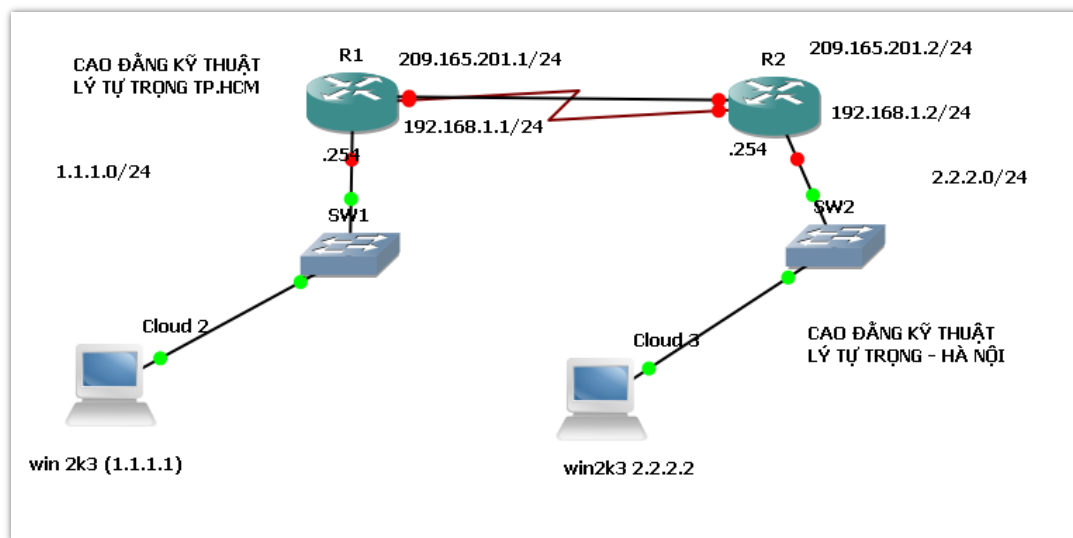
2. NỘI DUNG

2.1. Giao thức OSPF (Open Shortest Path First)

OSPF là một giao thức định tuyến Link-state điển hình. Đây là một giao thức được sử dụng rộng rãi trong các mạng doanh nghiệp có phạm vi lớn. Một số đặc điểm chính của giao thức OSPF:

- OSPF là một giao thức Link-state (lắng nghe trạng thái đường truyền). Mỗi router khi chạy giao thức sẽ gửi các trạng thái đường link của nó cho tất cả các router trong vùng (area). Sau một thời gian trao đổi, các router sẽ đồng nhất được bảng cơ sở dữ liệu trạng thái đường link (Link State Database – LSDB) với nhau, mỗi router đều có được “bản đồ mạng” của cả vùng (area). Từ đó mỗi router sẽ chạy giải thuật tìm đường đi để tính toán ra một cây đường đi ngắn nhất (Shortest path tree) và dựa vào cây này để xây dựng nên bảng định tuyến.
- OSPF có AD = 110.
- Metric của OSPF còn gọi là cost, được tính theo bandwidth trên cổng chạy OSPF.
- OSPF chạy trực tiếp trên nền IP, có protocol – id là 89.
- OSPF là một giao thức chuẩn quốc tế, được định nghĩa trong RFC – 2328.

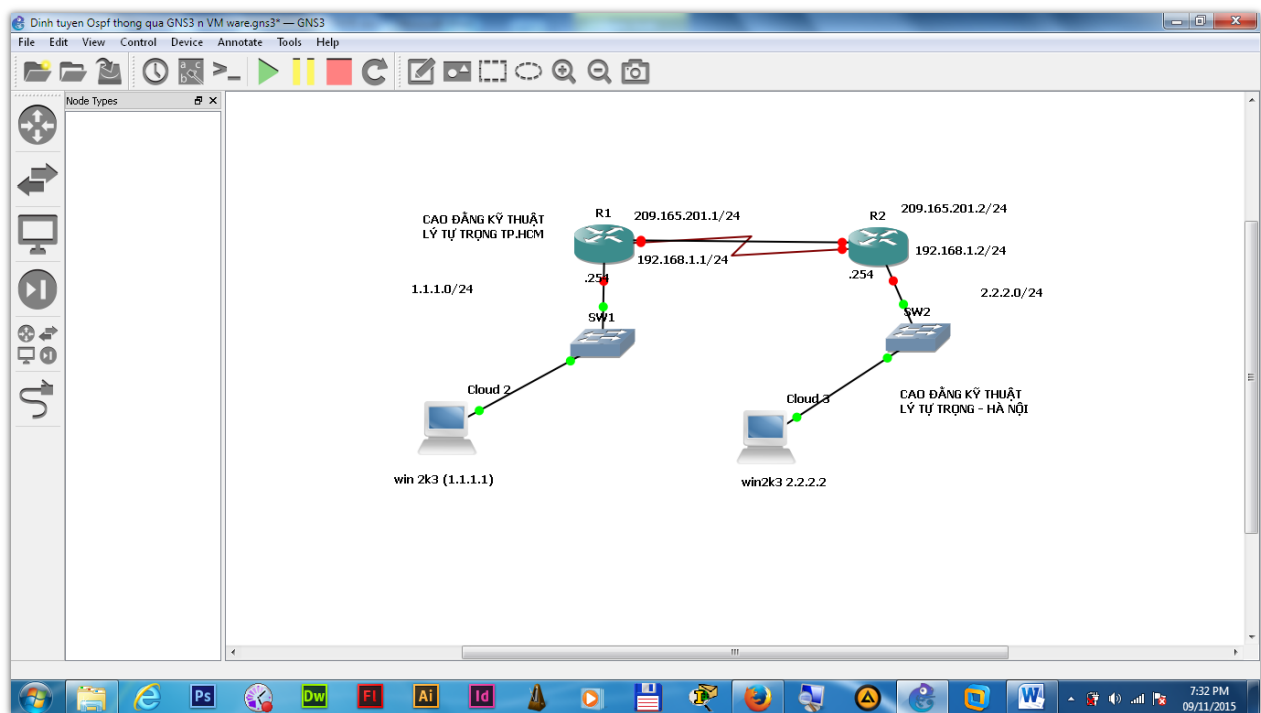
2.2. Mô hình mạng



Hình 3. 1 - Mô hình mạng thực tế

2.3. Phần mềm

2.3.1. GNS3



Hình 3. 2 - Xây dựng mô hình trên GNS3

2.3.2. Phần mềm VMware



Hình 3. 3 - Sử dụng phần mềm máy ảo VMware

2.3.3. Một số tiện ích kết nối

Phần giả lập sử dụng các tiện ích nhằm phục vụ cho quá trình cấu hình và kiểm tra hệ thống như: Putty, Tftpd32/64 bits, Windows (7/8/XP/2k3/2k8), Linux (CentOS/Fedora/Ubuntu)

2.4. Cấu hình hệ thống

Bảng 3. 1 - Bảng mô tả thông tin cấu hình

Thiết bị	Card giao tiếp	Địa chỉ IP	IOS Image	Chi nhánh
Router(R1)	FastEthernet0/0	192.168.1.1/24	c2691-adventerprisek9_sna-mz.124-17.bin	Tp.HCM (HCM)
Router(R1)	FastEthernet0/1	1.1.1.254/24	c2691-adventerprisek9_sna-mz.124-17.bin	
Router(R1)	Serial0/0	209.165.201.1/24		
Switch-cisco	VLAN_1			
PC01	Vnet1(Host	IP:1.1.1.1/24	Winddows server 2k3	

	only)			
PC01	Nnet1(Host only)	DG:1.1.1.254		
Router(R2)	FastEthernet0/0	192.168.1.2/24	c2691-adventerprisek9_sna-mz.124-17.bin	HÀ NỘI (HN)
Router(R2)	FastEthernet0/1	2.2.2.254/24	c2691-adventerprisek9_sna-mz.124-17.bin	
Router(R2)	Serial0/0	209.165.201.2/24		
Switch-cisco	VLAN_2			
PC02	Vnet1(Host only)	IP:2.2.2.2/24	Winddows server 2k3	
PC02	Nnet1(Host only)	DG:2.2.2.254		

Bảng 3. 2 - Bảng các lệnh của thiết bị Cisco

Lệnh thao tác	Mô tả mục đích
Configure terminal	Vào chế độ cấu hình
Interface <interface>	Vào chế độ cấu hình cổng giao tiếp
Ip address <IP> <Netmask>	Gán địa chỉ IP trên card giao tiếp
Host name	Gán tên thiết bị
Show IP Interface brief	Xem trạng thái card/cổng giao tiếp
No shutdown	Chuyển cổng giao tiếp về trạng thái up
Shutdown	Chuyển cổng giao tiếp về trạng thái down
Router Ospf <ID-Number>	Định tuyến với giao thức OSPF
Network <Subnet> <wildcard mask> area <id_number>	Quảng bá đường mạng cần định tuyến
Show ip route	Xem kết quả thông tin định tuyến
Exit	Thoát từng cấp chế độ cấu hình
Wr	Lưu thông tin cấu hình vào file cấu hình startup-config

```

R1
HCM(config)#interface serial 0/0
HCM(config-if)#ip address 192.168.1.1 255.255.255.0
HCM(config-if)#no shut
HCM(config-if)#
*Mar 1 00:04:26.735: %LINK-3-UPDOWN: Interface Serial0/0, changed state to up
HCM(config-if)#
*Mar 1 00:04:27.739: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up
HCM(config-if)#
*Mar 1 00:04:53.867: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to down
HCM(config-if)#
*Mar 1 00:08:33.863: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up
HCM(config-if)#exit
HCM(config)#router ospf
HCM(config)#router ospf 1
HCM(config-router)#network 10.1.1.0 0.0.0.3 area 0
HCM(config-router)#network 1.1.1.0 0.0.0.255 area 0
HCM(config-router)#network 209.165.201.0 0.0.0.31 area 0
HCM(config-router)#network 192.168.1.0 0.0.0.
*Mar 1 00:13:57.431: %OSPF-5-ADJCHG: Process 1, Nbr 20.1.1.1 on FastEthernet0/0 from LOADING to FULL, Loading
Done
HCM(config-router)#network 192.168.1.0 0.0.0.255 area 0
HCM(config-router)#
*Mar 1 00:14:02.271: %OSPF-5-ADJCHG: Process 1, Nbr 20.1.1.1 on Serial0/0 from LOADING to FULL, Loading Done
HCM(config-router)#

```

Hình 3. 4 - Thực hiện Routing tại router R1(HCM)

```

R2
HN(config-if)#
*Mar 1 00:05:57.739: %LINK-3-UPDOWN: Interface Serial0/0, changed state to up
HN(config-if)#
*Mar 1 00:05:58.743: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up
HN(config-if)#exit
HN(config)#rout
HN(config)#router os
HN(config)#router ospf 1
HN(config-router)#network 20.1.1.0 0.0.0.3 area 0
HN(config-router)#network 2.2.2.0 0.0.0.255 area 0
HN(config-router)#network 209.165.201.0 0.0.0.31 area 0
HN(config-router)#network 192.168.1.0 0.0.0.255 area 0
HN(config-router)#end
HN#wr
Building configuration...
[OK]
HN#
*Mar 1 00:10:36.915: %SYS-5-CONFIG_I: Configured from console by console
HN#
*Mar 1 00:11:37.395: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.1.1 on FastEthernet0/0 from LOADING to FULL, Loading
Done
HN#
*Mar 1 00:11:42.227: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.1.1 on Serial0/0 from LOADING to FULL, Loading Done
HN#

```

Hình 3. 5 - Thực hiện định tuyến tại Router R2(HN)

Bảng 3. 3 - Bảng thông tin cấu hình file running-config

Router tại chi nhánh TP.HCM	Router tại chi nhánh Hà Nội
Current configuration : 1384 bytes	Current configuration : 1383 bytes
!	!
version 12.4	version 12.4
service timestamps debug datetime msec	service timestamps debug datetime msec
service timestamps log datetime msec	service timestamps log datetime msec
no service password-encryption	no service password-encryption
!	!
hostname HCM	hostname HN
!	!

<pre> boot-start-marker boot-end-marker ! ! no aaa new-model memory-size iomem 5 no ip icmp rate-limit unreachable ip cef ! ! no ip domain lookup ! ! ! ip tcp synwait-time 5 ! ! interface Loopback1 ip address 10.1.1.1 255.255.255.252 ! interface FastEthernet0/0 ip address 209.165.201.1 255.255.255.224 duplex auto speed auto ! interface Serial0/0 ip address 192.168.1.1 255.255.255.0 clock rate 2000000 ! interface FastEthernet0/1 ip address 1.1.1.254 255.255.255.0 duplex auto speed auto ! interface Serial0/1 no ip address shutdown clock rate 2000000 ! interface Serial0/2 no ip address shutdown clock rate 2000000 ! interface FastEthernet1/0 no ip address </pre>	<pre> boot-start-marker boot-end-marker ! ! no aaa new-model memory-size iomem 5 no ip icmp rate-limit unreachable ip cef ! ! no ip domain lookup ! ! ! ip tcp synwait-time 5 ! ! interface Loopback2 ip address 20.1.1.1 255.255.255.252 ! interface FastEthernet0/0 ip address 209.165.201.2 255.255.255.224 duplex auto speed auto ! interface Serial0/0 ip address 192.168.1.2 255.255.255.0 clock rate 2000000 ! interface FastEthernet0/1 ip address 2.2.2.254 255.255.255.0 duplex auto speed auto ! interface Serial0/1 no ip address shutdown clock rate 2000000 ! interface Serial0/2 no ip address shutdown clock rate 2000000 ! interface FastEthernet1/0 no ip address </pre>
--	--

<pre> shutdown duplex auto speed auto ! ! router ospf 1 log-adjacency-changes network 1.1.1.0 0.0.0.255 area 0 network 10.1.1.0 0.0.0.3 area 0 network 192.168.1.0 0.0.0.255 area 0 network 209.165.201.0 0.0.0.31 area 0 ! ip forward-protocol nd ! ! no ip http server no ip http secure-server ! no cdp log mismatch duplex ! ! ! ! control-plane ! ! line con 0 exec-timeout 0 0 privilege level 15 logging synchronous line aux 0 exec-timeout 0 0 privilege level 15 logging synchronous line vty 0 4 login ! </pre>	<pre> shutdown duplex auto speed auto ! ! router ospf 1 log-adjacency-changes network 2.2.2.0 0.0.0.255 area 0 network 20.1.1.0 0.0.0.3 area 0 network 192.168.1.0 0.0.0.255 area 0 network 209.165.201.0 0.0.0.31 area 0 ! ip forward-protocol nd ! ! no ip http server no ip http secure-server ! no cdp log mismatch duplex ! ! ! ! control-plane ! ! line con 0 exec-timeout 0 0 privilege level 15 logging synchronous line aux 0 exec-timeout 0 0 privilege level 15 logging synchronous line vty 0 4 login ! </pre>
--	--

```

R1
HCM#copy run
HCM#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

  1.0.0.0/24 is subnetted, 1 subnets
C    1.1.1.0 is directly connected, FastEthernet0/1
  2.0.0.0/24 is subnetted, 1 subnets
O    2.2.2.0 [110/20] via 209.165.201.2, 00:18:48, FastEthernet0/0
  20.0.0.0/32 is subnetted, 1 subnets
O    20.1.1.1 [110/11] via 209.165.201.2, 00:18:48, FastEthernet0/0
  209.165.201.0/27 is subnetted, 1 subnets
C    209.165.201.0 is directly connected, FastEthernet0/0
  10.0.0.0/30 is subnetted, 1 subnets
C    10.1.1.0 is directly connected, Loopback1
C    192.168.1.0/24 is directly connected, Serial0/0
HCM#
  
```

Hình 3. 6 - Bảng định tuyến Router1

```

R2
HN#sh ip route
HN#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

  1.0.0.0/24 is subnetted, 1 subnets
O    1.1.1.0 [110/20] via 209.165.201.1, 00:20:30, FastEthernet0/0
  2.0.0.0/24 is subnetted, 1 subnets
C    2.2.2.0 is directly connected, FastEthernet0/1
  20.0.0.0/30 is subnetted, 1 subnets
C    20.1.1.0 is directly connected, Loopback2
  209.165.201.0/27 is subnetted, 1 subnets
C    209.165.201.0 is directly connected, FastEthernet0/0
  10.0.0.0/32 is subnetted, 1 subnets
O    10.1.1.1 [110/11] via 209.165.201.1, 00:20:30, FastEthernet0/0
C    192.168.1.0/24 is directly connected, Serial0/0
HN#
  
```

Hình 3. 7 - Bảng định tuyến Router2



```
C:\WINDOWS\system32\cmd.exe
Reply from 1.1.1.1: bytes=32 time<1ms TTL=128
Reply from 1.1.1.1: bytes=32 time<1ms TTL=128
Reply from 1.1.1.1: bytes=32 time<1ms TTL=128
Reply from 1.1.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 1.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\admin>ping 1.1.1.254

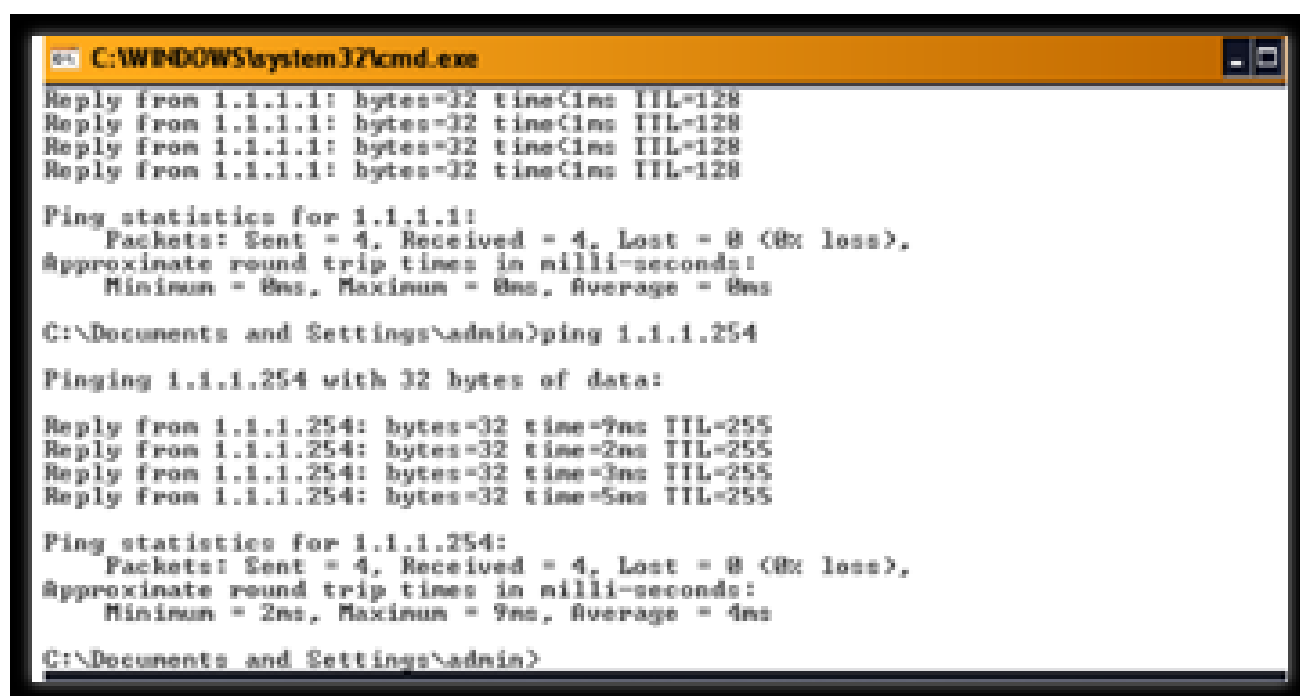
Pinging 1.1.1.254 with 32 bytes of data:

Reply from 1.1.1.254: bytes=32 time=9ms TTL=255
Reply from 1.1.1.254: bytes=32 time=2ms TTL=255
Reply from 1.1.1.254: bytes=32 time=3ms TTL=255
Reply from 1.1.1.254: bytes=32 time=5ms TTL=255

Ping statistics for 1.1.1.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 9ms, Average = 4ms

C:\Documents and Settings\admin>
```

Hình 3. 8 - Kiểm tra trạm cuối tại chi nhánh TP.HCM



```
C:\WINDOWS\system32\cmd.exe
Reply from 1.1.1.1: bytes=32 time<1ms TTL=128
Reply from 1.1.1.1: bytes=32 time<1ms TTL=128
Reply from 1.1.1.1: bytes=32 time<1ms TTL=128
Reply from 1.1.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 1.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\admin>ping 1.1.1.254

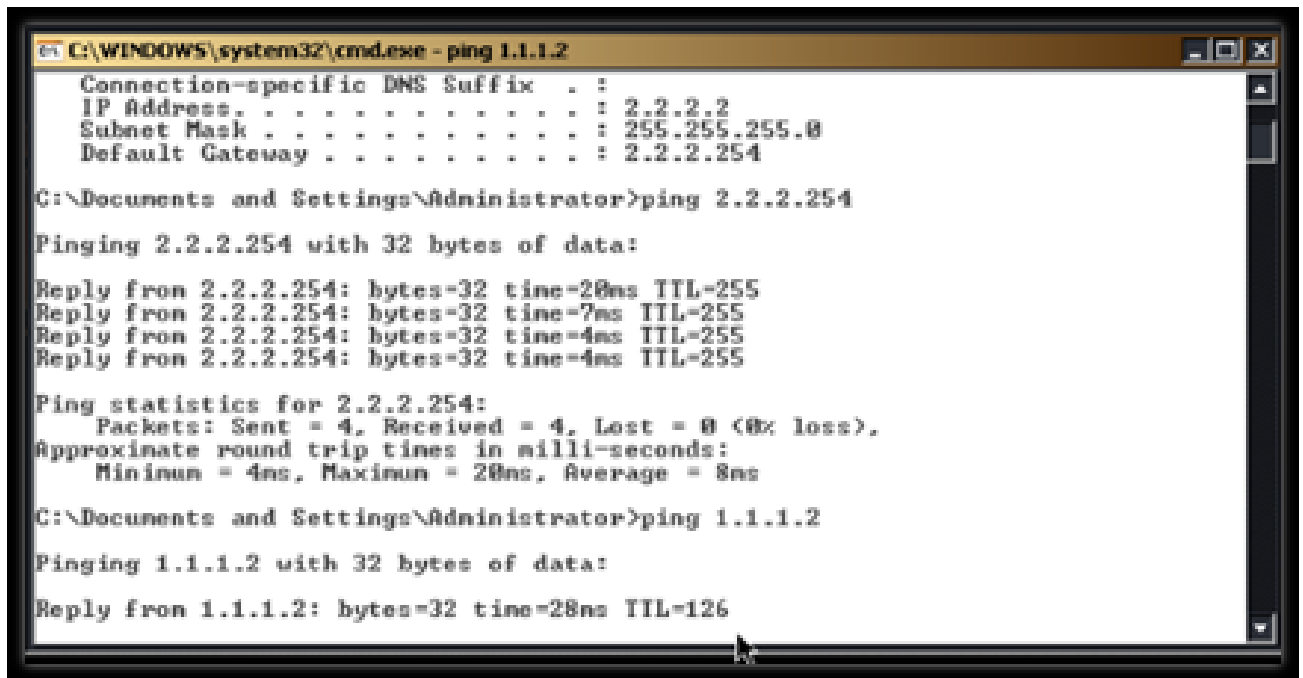
Pinging 1.1.1.254 with 32 bytes of data:

Reply from 1.1.1.254: bytes=32 time=9ms TTL=255
Reply from 1.1.1.254: bytes=32 time=2ms TTL=255
Reply from 1.1.1.254: bytes=32 time=3ms TTL=255
Reply from 1.1.1.254: bytes=32 time=5ms TTL=255

Ping statistics for 1.1.1.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 9ms, Average = 4ms

C:\Documents and Settings\admin>
```

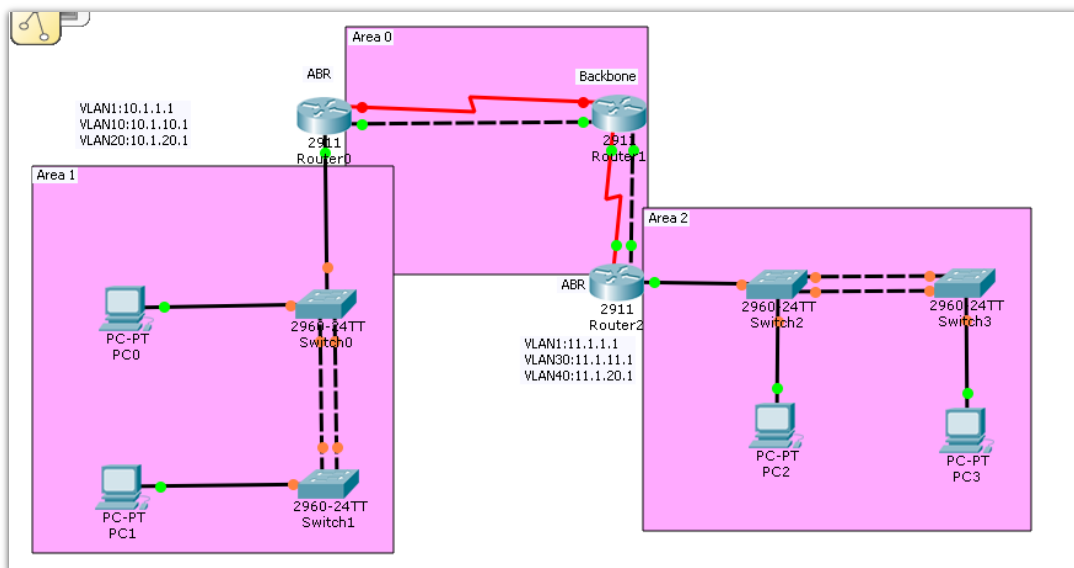
Hình 3. 9 - Kiểm tra trạm cuối tại chi nhánh TP.HCM



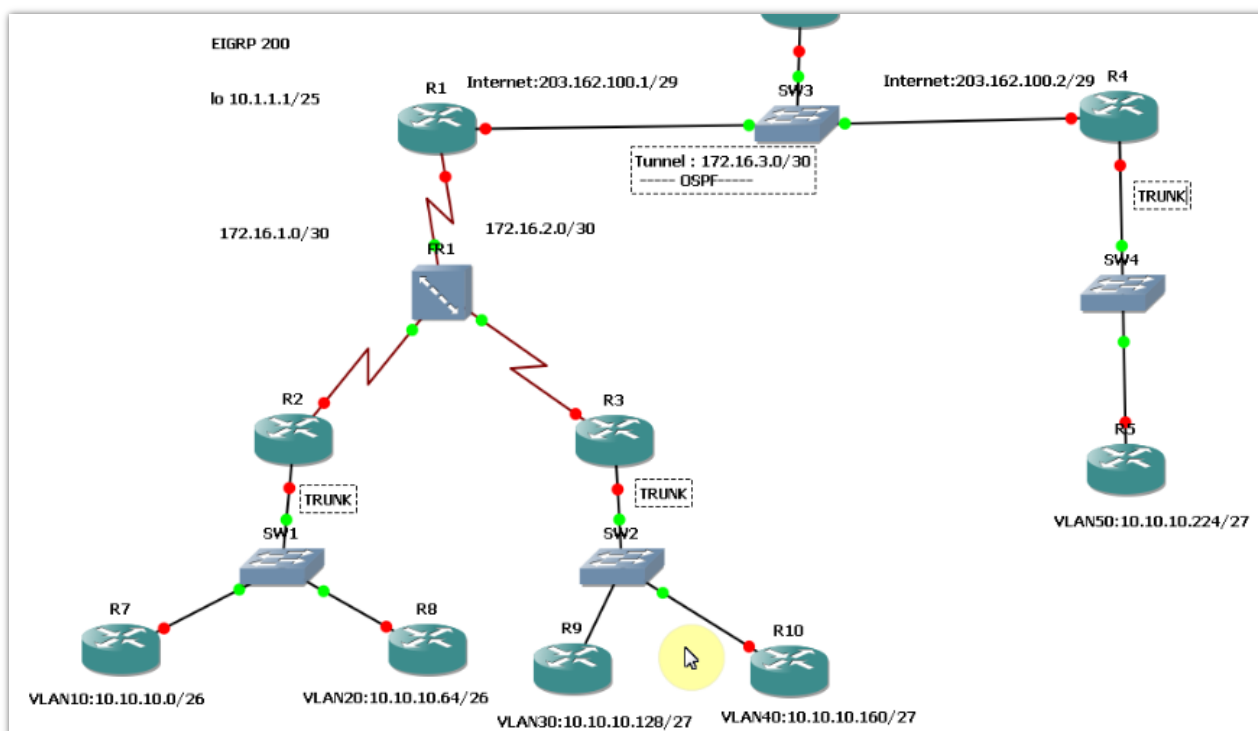
Hình 3. 10 - Kiểm tra trạm cuối tại chi nhánh TP.HN

3. PHỤ LỤC

MỘT SỐ MÔ HÌNH MẠNG ỨNG DỤNG GIAO THỨC OSPF



Hình 3. 11 - Mô hình OSPF Multi-Area tích hợp cơ chế VLAN



Hình 3. 12 - Mô hình OSPF tích hợp VLAN, DHCP, DHCP Agent, Frame Relay và VPN

```

R3
File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
R1 R2 R3 x
R3(config-subif)#
*Mar 1 00:10:11.191: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to down
R3(config-subif)#exit
R3(config)#int se0/0
R3(config-if)#no shut
R3(config-if)#
*Mar 1 00:10:31.191: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up
R3(config-if)#exit
R3(config)#int fa0/0.30
R3(config-subif)#encap
R3(config-subif)#encapsulation dot
R3(config-subif)#encapsulation dot1q 30
R3(config-subif)#ip address 10.10.10.129 255.255.255.192
R3(config-subif)#ip help
R3(config-subif)#ip helper-address 10.1.1.1
R3(config-subif)#exit
R3(config)#int fa0/0.40
R3(config-subif)#encap
R3(config-subif)#encapsulation dot
R3(config-subif)#encapsulation dot1q 40
R3(config-subif)#ip address 10.10.10.161 255.255.255.192
% 10.10.10.128 overlaps with FastEthernet0/0.30
R3(config-subif)#exit
R3(config)#int fa0/0.40
R3(config-subif)#encap
R3(config-subif)#encapsulation dot
R3(config-subif)#encapsulation dot1q 40
R3(config-subif)#ip add
R3(config-subif)#ip address 10.10.10.161 255.255.255.192
R3(config-subif)#ip help
R3(config-subif)#ip helper-address 10.1.1.1
R3(config-subif)#exit
R3(config)#int fa0/0
R3(config-if)#no shut
% 10.10.10.128 overlaps with FastEthernet0/0.40
FastEthernet0/0.30: incorrect IP address assignment
R3(config-if)#no shut
% 10.10.10.128 overlaps with FastEthernet0/0.40
FastEthernet0/0.30: incorrect IP address assignment
R3(config-if)#exit
R3(config)#int fa0/0.30
R3(config-subif)#encap
R3(config-subif)#encapsulation dot
R3(config-subif)#encapsulation dot1q 30
R3(config-subif)#no ip address 10.10.10.129 255.255.255.192
R3(config-subif)#ip address 10.10.10.129 255.255.255.224

```

Hình 3. 13 - Thông tin cấu hình Router R1, R2 và R3

```

R4
File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
R1 R2 R3 R7 R8 R9 R10 R4 x
*Mar 1 00:29:58.443: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up
R4(config-if)#exit
R4(config)#exit
R4#ping
*Mar 1 00:30:05.083: %SYS-5-CONFIG_I: Configured from console by console
R4#ping 172.16.3.1

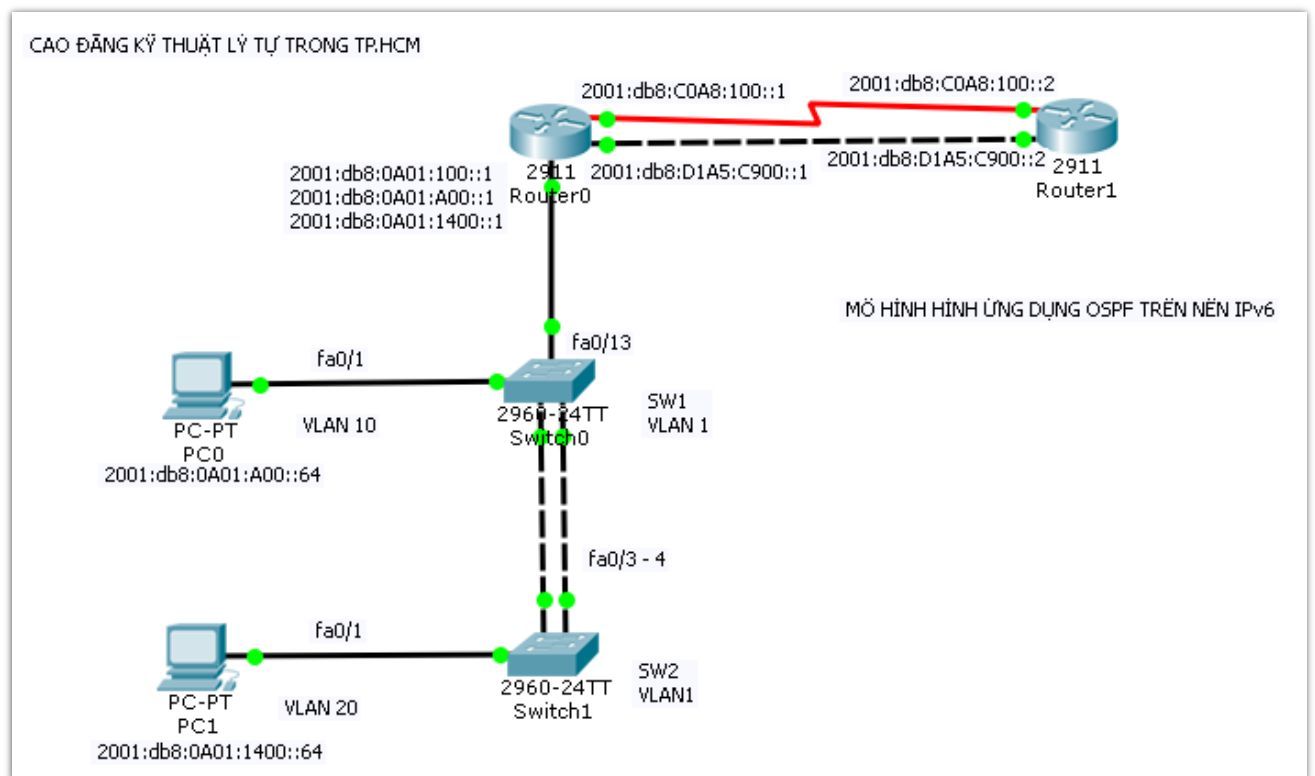
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.3.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/25/44 ms
R4#config t
Enter configuration commands, one per line. End with CNTL/Z.
R4(config)#router
R4(config)#router of
R4(config)#router os
R4(config)#router ospf 1
R4(config-router)#network 172.16.3.0 0.0.0.3 area 0
R4(config-router)#
*Mar 1 00:34:07.819: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.1.1 on Tunnel0 from LOADING to FULL, Loading Done
R4(config-router)#network 10.10.10.224 0.0.0.31 area 0
R4(config-router)#network 10.10.10.224 0.0.0.31 area 0
R4(config-router)#
R4(config-router)#end
R4#
*Mar 1 00:35:04.547: %SYS-5-CONFIG_I: Configured from console by console
R4#sh ip rou
R4#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        I - IS-IS, SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

    203.162.100.0/29 is subnetted, 1 subnets
C       203.162.100.0 is directly connected, FastEthernet0/0
    172.16.0.0/30 is subnetted, 1 subnets
C       172.16.3.0 is directly connected, Tunnel0
    10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O       10.1.1.1/32 [110/11112] via 172.16.3.1, 00:00:10, Tunnel0
C       10.10.10.224/27 is directly connected, FastEthernet0/1.50
R4#

```

Hình 3. 14 - Thông tin bảng định tuyến tại R4



Hình 3. 15 - Mô hình ứng dụng giao thức định tuyến OSPF trên nền IPv6

TÀI LIỆU THAM KHẢO

[1] Interconnecting Cisco Networking Devices – Part 2