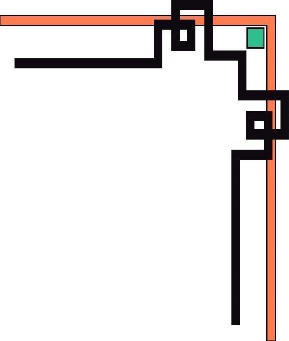
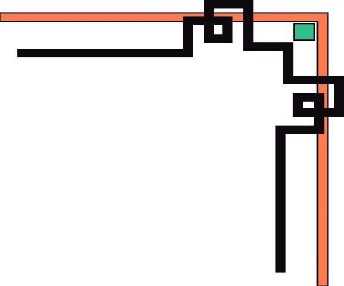
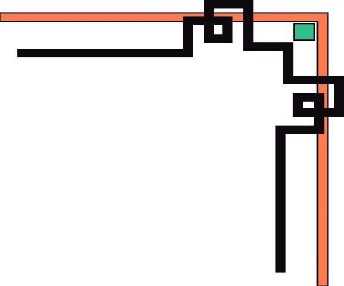
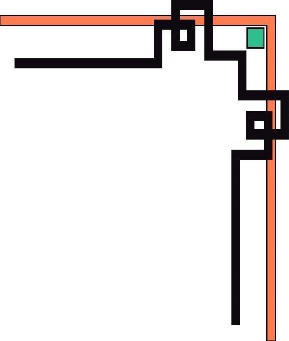
TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI



**VIỆN ĐIỆN TỬ - VIỄN THÔNG**

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

****

**BÁO CÁO**

**THỰC TẬP KĨ THUẬT**

**Đề tài:**

**THIẾT KẾ HỆ THỐNG CHỮ KÝ SỐ BẰNG MATLAB**

**TÌM HIỂU HỆ THỐNG BẢO MẬT THÔNG TIN VỆ TINH**

|  |  |
| --- | --- |
| **Giảng viên hướng dẫn** | **: PGS.TS Đỗ Trọng Tuấn**  **TS. Hán Trọng Thanh** |
| **Sinh viên thực hiện** | **: Nguyễn Quang Thịnh** |
| **Mã số sinh viên** | **: 20153598** |
| **Lớp** | **: Điện tử 08 – K60** |

Hà Nội, 8/2018

**MỤC LỤC**

[A. LỜI NÓI ĐẦU 2](#_Toc524036476)

[B. NỘI DUNG 5](#_Toc524036477)

[Chương 1 : GIỚI THIỆU ASE LAB 5](#_Toc524036478)

[Chương 2 : NỘI DUNG THỰC TẬP 7](#_Toc524036479)

[2.1 Các lĩnh vực hoạt động và yêu cầu chuyên môn của ASE Lab 7](#_Toc524036480)

[2.1.1 Nghiên cứu, phát triển UAV 7](#_Toc524036481)

[2.1.2 Nghiên cứu, phát triển các hệ thống thông minh 7](#_Toc524036482)

[2.1.3 Nghiên cứu, phát triển về thông tin quang vô tuyến 7](#_Toc524036483)

[2.1.4 Nghiên cứu, phát triển về xử lý tín hiệu vô tuyến 7](#_Toc524036484)

[2.1.5 Yêu cầu khác 8](#_Toc524036485)

[2.2 Các công việc được giao trong đợt thực tập 8](#_Toc524036486)

[2.2.1 Thiết kế hệ thống chữ ký số 8](#_Toc524036487)

[2.2.2 Tìm hiểu về bảo mật trong thông tin vệ tinh 12](#_Toc524036488)

[C. KẾT LUẬN 23](#_Toc524036489)

[TÀI LIỆU THAM KHẢO 24](#_Toc524036490)

[PHỤ LỤC : Code Arduino 25](#_Toc524036491)

# LỜI NÓI ĐẦU

***Thực tập kỹ thuật*** là một học phần bắt buộc và rất quan trọng trong chương trình đào tạo sinh viên tại viện Điện tử - Viễn thông, giúp cho sinh viên được thực hành, vận dụng kiến thức của mình đã được học cũng như tự học, tự tìm hiểu tài liệu vào môi trường thực tế cụ thể. Qua đó, sinh viên có thể hiểu sâu hơn các kiến thức đã được học, nhận thức rõ ràng hơn về đặc thù của ngành nghề, có ý thức trang bị kiến thức chuyên môn cũng như các kỹ năng cần thiết để phục vụ cho công việc sau này. Đây cũng là một cơ hội rất tốt để sinh viên hệ thống lại toàn bộ kiến thức đã được học, từ đó củng cố những phần mà mình còn chưa nắm chắc. Ngoài ra, đây cũng là cơ hội tốt để sinh viên mở rộng các mối quan hệ lành mạnh với các thầy, các anh chị đi trước cũng như các bạn cùng thực tập.

Xác định được tầm quan trọng của môn học, em đã đăng ký thực tập tại ASE Lab trong khoảng 6 tuần (từ 09/07/2018 – 12/8/2018), tại phòng Lab C9 – 415, Đại học Bách Khoa Hà Nội. Lĩnh vực nghiên cứu của Lab bao gồm: Hệ thống UAV, Hệ thống thông minh Smart System, Truyền thông sử dụng ánh sáng và Xử lý tín hiệu vô tuyến. ASE Lab – Lab trực thuộc viện Điện tử - Viễn thông, có các thầy PGS.TS. Đỗ Trọng Tuấn, TS. Hán Trọng Thanh, PGS.TS. Hà Duyên Trung, ThS. Phương Xuân Quang hướng dẫn. Trong quá trình thực tập, em được giao đề tài tìm hiểu về **“Thiết kế hệ thống chữ ký số bằng matlab.** Đây là những đề tài thực sự hay và thú vị, vì từ trước khi thực tập, em chưa bao giờ tiếp xúc với các thuật ngữ chuyên ngành mới lạ đến vậy. Trong khi nhận đề tài thực tập, bản thân em đã gặp một số thuận lợi và khó khăn sau :

*Về thuận lợi :*

* Tại Lab - môi trường thực tập rất khoa học, năng động, chuyên nghiệp và luôn vui vẻ, luôn khơi dậy niềm đam mê để em chủ động nghiên cứu, tìm hiểu và hoàn thành nhiệm vụ được giao.
* Trong quá trình thực tập, em đã nhận được sự hướng dẫn tận tình từ các thầy, các anh chị khóa trên và các bạn để nhanh chóng nắm bắt, tiếp thu và ứng dụng luôn vào thực tế.
* Trong quá trình học các môn học lý thuyết trên lớp, em đã được học các môn như Điện tử tương tự I & II, Ngôn ngữ lập trình, Điện tử số, Kỹ thuật vi xử lý… Đó là những môn học cơ sở ngành giúp em có kiến thức nền tảng cơ bản để học tập và nghiên cứu.
* Có nhiều cơ hội được trau dồi kiến thức Tiếng Anh chuyên ngành.

*Về khó khăn:*

* Do kiến thức chuyên ngành chưa thật vững nên em vẫn chưa vận dụng hết được tối đa để hoàn thiện đề tài tốt hơn.
* Đây là lần đầu em tham gia thiết kế sản phẩm thực tế nên thời gian đầu có gặp  
  khó khăn do chưa có kinh nghiệm và chưa quen với áp lực công việc thực tế.
* Và cũng do vấn đề trình độ ngoại ngữ còn hạn chế nên đọc tài liệu cũng khó khăn hơn.

Hết kỳ thực tập, em đã có được cái nhìn toàn diện về một mô hình thực tế và đi sâu vào mô phỏng nhiều hệ thống truyền thông với những đánh giá khách quan so với lý thuyết đã được học từ các kỳ trước. Bên cạnh đó, chúng em còn được nâng cao trình độ ngoại ngữ, rèn luyện kỹ năng làm việc nhóm cũng như khả năng làm việc độc lập. Kỳ thực tập này cũng là điều kiện tốt để em có thể học hỏi kinh nghiệm học tập, nghiên cứu và làm việc với mọi người.

Em xin gửi lời cảm ơn chân thành đến Ban lãnh đạo viện Điện tử - Viễn thông đã tạo điều kiện thuận lợi để chúng em có được những trải nghiệm bổ ích, thú vị về công việc được thực hiện. Em xin cảm ơn PGS.TS Đỗ Trọng Tuấn, TS. Hán Trọng Thanh đã trực tiếp hướng dẫn, cùng các anh chị sinh viên K58, K59 và các bạn nghiên cứu, học tập tại ASELAB đã rất tận tình hướng dẫn cũng như giúp đỡ em hoàn thành công việc được giao.

Trong quá trình thực tập, do kiến thức chuyên môn cũng như kiến thức xã hội hạn chế nên em không thể tránh khỏi những thiếu sót. Em rất mong nhận được ý kiến đóng góp, nhận xét của các thầy, các anh chị và các bạn để có thể điều chỉnh và hoàn thiện bản thân. Trong thời gian tới, em rất mong sẽ tiếp tục nhận được sự hướng dẫn quý báu, sự hợp tác thiện chí từ các thầy cô, các anh chị và các bạn.

Sinh viên

Nguyễn Quang Thịnh

# NỘI DUNG

# GIỚI THIỆU ASE LAB

Đơn vị tiếp nhận : ASE Laboratory.

Địa chỉ : C9-415, Đại học Bách Khoa Hà Nội.

Lab được thành lập từ ngày 26/3/2012 dưới sự hướng dẫn của các thầy PGS.TS Đỗ Trọng Tuấn, TS. Hán Trọng Thanh, PGS.TS. Hà Duyên Trung, ThS.Phương Xuân Quang.

Lab có quan hệ hợp tác với Viện Cơ khí động lực Đại học BKHN, Đại học Công nghệ Sydney (Úc), Trường Đại học Tohoku, Chiba, Wakayama (Nhật Bản), Trung tâm Vệ tinh quốc gia Việt Nam, Đại học Phòng Cháy Chữa Cháy, Trung tâm khí tượng thủy văn Quốc gia, Cục Kỹ thuật Bộ Công An, Viện Điện tử - Tin học Tự động hóa (Bộ Công thương),…

Các nhóm nghiên cứu chính:

* Nhóm nghiên cứu phát triển UAV (UAVG = Unmanned Aerial Vehicle Group)
* Nhóm nghiên cứu phát triển các hệ thống thông minh (ISSG = Integrated Smart System Group).
* Nhóm nghiên cứu phát triển về thông tin quang vô tuyến (OpWiG = Optical Wireless Communication Group).
* Nhóm nghiên cứu phát triển về xử lý tín hiệu vô tuyến (RSPG = Radio Signal Processing Group).

Qua quá trình nghiên cứu, ASE Lab đã đạt được các kết quả đáng kể như sau:

* Tham gia một đề tài tiềm năng cấp nhà nước.
* Tham gia một đề tài NCKH của sở KHCN thành phố Hà Nội.
* Tham gia Sinh viên NCKH và đạt được giải của Viện Điện Tử Viễn Thông các năm 2012, 2013, 2014.
* Công bố và xuất bản 6 bài báo khoa học (2 trong nước và 4 quốc tế)
* 5 học viên cao học đã tốt nghiệp (1 ThS. KH điểm bảo vệ TN 10/10, 4 ThS. KT).

Một số bài báo đã công bố trong các năm gần đây:

1. Diem P. G**.**, **Anh P. H**., Khanh N. P., Hung N. P., Hien N. V., A Hybrid Control Model to Develop the Trajectory-Tracking Controller for a Quadrotor UAV, the 5th ICMAE, Madrid, Spain, July 18-19, 2014, Proc. of ICMAE2014, ISBN-13: 978-3-03835-223-5; Advanced Materials Research (**Indexed in Scopus, SCImago,** **http://www.scopus.com/**), ISSN: print 1022-6680 ISSN, cd 1022- 6680 ISSN, web 1662-8985,Volume 1016, pp. 678-685, 2014.
2. **Diem P. G.**, Hien N. V., Khanh, N. P., An Object-Oriented Analysis and Design Model to Implement Controllers for Quadrotor UAVs by Specializing MDA’s Features with Hybrid Automata and Real-Time UML, WSEAS Transactions on Systems (**Indexed in** **Scopus****, SCImago, http://www.scopus.com/**), E-ISSN 2224-2678, Issue 10, Volume 12, pp. 483-496, October 2013.
3. **Anh P. H., Diem P. G.**, Tuan D. T., Hien N. V., A Hybrid AutomataBased Model to Develop Controllers for Quadrotor UAVs, Proc. of RCMME2014, ISBN: 978-604-911-942-2, pp. 397-401, Hanoi, Vietnam, 2014.
4. **Phạm Hoàng Anh, Phạm Gia Điềm**, Đỗ Trọng Tuấn, Ngô Văn Hiền, Nguyễn Phú Hùng, Mô hình thiết kế hệ thống điều khiển cho Quadrotor UAV dựa trên nền công nghệ Arduino. Hội nghị Khoa học Cơ học Thuỷ khí Toàn quốc năm 2014, tổ chức từ 24 đến 26 tháng 7 năm 2014, tại Hoàn Cầu Resort, Tp. Phan Rang, tỉnh Ninh Thuận, Việt Nam.

# NỘI DUNG THỰC TẬP

## Các lĩnh vực hoạt động và yêu cầu chuyên môn của ASE Lab

### Nghiên cứu, phát triển UAV

Đây là hướng nghiên cứu mũi nhọn của Lab. Để làm việc theo hướng này, sinh viên cần có kiến thức vững chắc của các môn Trường điện từ, Anten và truyền sóng, Hệ thống viễn thông, Thông tin vô tuyến, Thông tin quang, Kỹ thuật vệ tinh,… Sinh viên cũng cần biết cách sử dụng các phần mềm thiết kế chuyên ngành như Matlab, Matlab Simulink, Arduino, Visual Studio, Android Studio,… và các phần mềm chuyên dụng cho từng thiết bị bay như: X-Plane, Misson Planner, Adupilot,… Hiện tại nhóm nghiên cứu đang tập trung vào việc nghiên cứu, thiết kế các thiết bị multicopter, cảm biến từ trường, INS, MPU, anten, máy thu GPS, Bộ lọc PID, Bộ nguồn và điểu khiển nguồn để phục vụ cho các mục đích liên quan tới quân sự, bảo vệ môi trường,…

### Nghiên cứu, phát triển các hệ thống thông minh

Để làm việc theo hướng này, sinh viên cần có kiến thức vững chắc của các môn Cấu kiện điện tử, Điện tử số, Điện tử tương tự, Tín hiệu và hệ thống, Xử lý số tín hiệu, Kỹ thuật vi xử lý, Ngôn ngữ lập trình,… Đây cũng là hướng nghiên cứu đang phát triển của lab, đã đạt được nhiều thành tích cao.

### Nghiên cứu, phát triển về thông tin quang vô tuyến

Để làm việc theo hướng này, sinh viên cần có kiến thức vững chắc của các môn học Thông tin số, Thông tin vô tuyến, Anten và truyền sóng, Ngôn ngữ lập trình, Mạng thông tin, nắm vững các kỹ thuật mã hóa, điều chế tín hiệu, Kĩ thuật vi xử lý, lập trình vi điều khiển, Lập Trình nhúng, lập trình Arduino, và thiết kế mạch, sử dụng thành thạo phần mềm Matlab, Altium.

### Nghiên cứu, phát triển về xử lý tín hiệu vô tuyến

Để làm việc theo hướng này, sinh viên cần có kiến thức vững chắc của các môn Điện tử số, Điện tử tương tự, Tín hiệu và hệ thống, Xử lý số tín hiệu, Kỹ thuật vi xử lý, Ngôn ngữ lập trình, Lý thuyết mật mã,… Ngoài ra, sinh viên cũng cần nắm được ngôn ngữ lập trình Matlab, C/C++,… cũng như biết cách sử dụng và làm việc với vi điều khiển. Đây là hướng nghiên cứu có truyền thống của Lab, và đang được phát triển mạnh mẽ, hứa hẹn sẽ có nhiều thành công trong tương lai.

### Yêu cầu khác

Để tham gia nghiên cứu và thành công trong một lĩnh vực nào đó thì ngoài kiến thức chuyên môn, sinh viên cần trang bị cho mình những kỹ năng mềm và phải rèn luyện cho mình phẩm chất của một người kỹ sư :

* Nghiêm túc trong công việc, có niềm đam mê với công việc. Nghiên cứu khoa học không phải là vấn đề đơn giản, vì vậy phải có quyết tâm cao độ. Mặt khác, hầu hết các kiến thức đều mới và tài liệu đều sử dụng ngoại ngữ, nên sinh viên cũng cần trau dồi vốn ngoại ngữ của mình.
* Có tinh thần ham học hỏi, tinh thần làm việc tập thể, chia sẻ, hỗ trợ nhau trong quá trình học tập, nghiên cứu vì các lĩnh vực đều có mối liên hệ với nhau.
* Tinh thần kỷ luật, tôn trọng và tuân thủ các quy tắc tập thể, có sự chia sẻ, có ý thức bảo vệ và xây dựng tập thể phát triển vững mạnh.

## Các công việc được giao trong đợt thực tập

### Thiết kế hệ thống chữ ký số

Hiện nay, vấn đề bảo mật thông tin, dữ liệu cá nhân là hết sức quan trọng, trong môi trường số không thể dùng chữ ký tay nhưng lại có rất nhiều ứng dụng phải cần đến một cơ chế ký và xác thực người sử dụng như chữ ký tay. Các công nghệ mã hóa và chữ ký số ra đời để giúp giải quyết các trường hợp giao dịch cần đến chữ ký tay nhưng lại phải thực hiện trong môi trường số.

Nội dung và kết quả công việc cụ thể như sau :

#### Chữ ký số - Chữ ký điện tử là gì?

Cũng giống như chữ ký tay, nếu bạn dùng chữ ký tay để xác nhận cho những gì mình viết thì bạn có thể dùng chữ ký điện tử để xác nhận cho những dữ liệu điện tử (email, file,…) của bạn.

Xác thực người gửi: Bạn có thể thông báo với khách hàng hoặc đối tác của bạn là chỉ những email có chữ ký điện tử của bạn mới có giá trị trong giao dịch & khả năng làm giả là 0%. Bạn cũng nên khuyến khích những người hay gửi email liên quan đến công việc cho bạn sử dụng chữ ký điện tử của họ.

Mã hoá dữ liệu: Nếu bạn đã từng email cho ai đó có chữ ký của bạn. Người đó có thể dùng chữ ký của bạn để mã hoá dữ liệu và gửi cho bạn. Lúc này, mọi thông tin trong email bao gồm cả file đính kèm sẽ được mã hoá và chỉ duy nhất bạn mới có thể đọc được những thông tin đó.

#### Tạo chữ ký điện tử như thế nào

Chữ ký điện tử khoá công khai dựa trên nên tảng mã hoá công khai. Để có thể trao đổi thông tin trong môi trường này, mỗi người sử dụng có một cặp khóa: một công khai và một bí mật. Khóa công khai được công bố rộng rãi còn khóa bí mật phải được người sử dụng giữ kín. Không thể tìm được khóa bí mật nếu chỉ biết khóa công khai.

Quá trình tạo và kiểm tra chữ ký số sử dụng 3 thuật toán:

* Thuật toán tạo khoá bí mật và khoá công khai
* Thuật toán tạo chữ ký số bằng khoá bí mật
* Thuật toán kiểm tra chữ ký số bằng khoá công khai hiện

#### Thiết kế chi tiết

* 1. Tạo khoá bí mật và khoá công khai:

Sử dụng hệ mật RSA để tạo khoá công khai và khoá bí mật.

Tạo khoá:

* Bước 1: Chọn 2 số nguyên tố lớn p và q với p khác q , lựa chọn ngẫu nhiên và độc lập.
* Bước 2: Tính: n = p.q
* Bước 3: Tính giá trị hàm số Ơle Φ(n) = (p – 1)(q – 1).
* Bước 4: Chọn một số tự nhiên *e* sao cho 1 < e < Φ(n) và là số nguyên tố cùng nhau với Φ(n).
* Tính: *d* sao cho *de ≡ 1* ( modΦ(n) )

**Khóa công khai** bao gồm:

*n*: môđun

*e*: số mũ công khai (cũng gọi là *số mũ mã hóa*).

**Khóa bí mật** bao gồm:

*n*: môđun, xuất hiện cả trong khóa công khai và khóa bí mật

*d:* số mũ bí mật (cũng gọi là *số mũ giải mã*).

* 1. Tạo chữ ký số bằng khoá bí mật:
  2. Kiểm tra chữ ký số bằng khoá công khai:

#### Kết nối hệ thống

#### Kết quả - Hướng phát triển đề xuất

* + - * 1. Kết quả :
* Mạch chạy ổn định, có thể điều chỉnh độ sâu mong muốn.
* Đáp ứng yêu cầu về khối lượng và năng lượng.
* Chưa đáp ứng được tính chống nước nên chưa thể kiểm thử thực tế ở hồ.
* Mạch khá cồng kềnh nên chắc chắn là không hợp lý nếu phải sử dụng 4 hệ thống lấy nước riêng biệt tương ứng với 4 điểm Waypoint.
* Ống bơm kim tiêm chỉ lấy được ít nước (khoảng 6ml), dẫn đến cần phải, hoặc đổi sang tay Arm (của Servo) có biên độ lớn hơn (có thể làm hệ thống cồng kềnh hơn), hoặc sử dụng cách hút khác.
  + - * 1. Hướng phát triển đề xuất :

Sử dụng máy bơm mini đẩy nước, duy chỉ có máy bơm là ngập trong nước, và đẩy nước lên 4 lọ đã được chuẩn bị sẵn – gắn chặt với UAV, có các lợi thế sau :

* Triển khai hệ thống đơn giản hơn nhiều so với Servo, có thể sử dụng tay điều khiển kiểm thử, trước khi tính tới hệ thống tự động.
* Chỉ cần 1 máy bơm để đẩy nước vào 4 lọ chứa làm cho lượng nước lấy được nhiều hơn vì chỉ phụ thuộc vào dung tích lọ chứa. Đồng thời, mạch sẽ không cồng kềnh, cộng với khối lượng máy bơm nhỏ, sẽ giữ được độ ổn định của UAV.
* Đảm bảo tính chống nước của máy bơm dễ hơn so với hệ thống Servo.

#### Kết luận

*“Thiết kế hệ thống chữ ký số bằng Matlab”* là một đề tài mang tính thực tế cao, hướng tới đóng góp quan trọng trong bảo mật thông tin truyền thông. Việc tham gia đề tài này đã giúp em ôn tập lại được kiến thức Lý Thuyết Mật Mã, Ngôn Ngữ Lập Trình,...đặc biệt là trong 3 tuần “toàn tâm toàn ý” với thực tập, em đã phần nào tạo được cho mình một tác phong làm việc chuyên nghiệp hơn, quy củ, nghiêm túc. Quan trọng hơn, em đã rèn luyện được tinh thần làm việc kiên trì, không ngại khó, ngại vất vả. Những buổi thầy Tuấn ngồi lại làm việc ở Lab, nghe và nhận xét tiến độ cho chúng em tới 8 – 9 giờ tối, mặc dù mọi người cùng đói, nhưng ai nấy đều cảm nhận được tâm huyết và sự tận tâm của thầy. Chính những điều này đã phần nào thôi thúc em và các bạn làm việc chăm chỉ hơn, không chỉ vì từng cá nhân mà còn vì tinh thần tập thể, tinh thần trách nhiệm với công việc.

### Tìm hiểu về bảo mật trong thông tin vệ tinh

#### Tổng quan về bảo mật thông tin vệ tinh

* + - * 1. Tại sao phải bảo mật trong thông tin vệ tinh ?

Ngày nay, thông tin vệ tinh đóng vai trò quan trọng, cũng như có những ứng dụng rộng rãi :

* Vệ tinh thông tin liên lạc
* Hệ thống định vị toàn cầu GPS
* Dự báo thời tiết, giảm nhẹ thiên tai
* Ứng dụng trong quân sự, quốc phòng
* Internet
* Truyền hình số vệ tinh

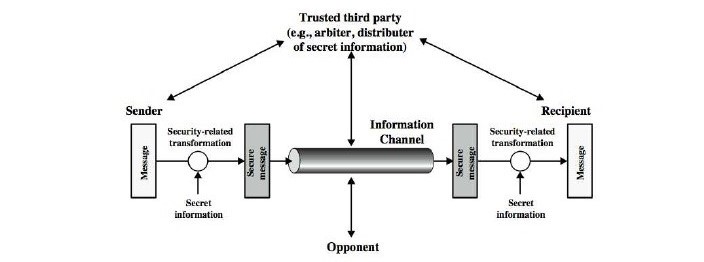
Bảo mật là vấn đề tối quan trọng trong thông tin vệ tinh, bởi việc các hệ thống thông tin vệ tinh có điểm yếu và lỗ hổng bảo mật có thể dẫn tới những hậu quả cực kỳ nghiêm trọng :

* Các cuộc gọi có thể bị nghe lén, mất cắp thông tin
* Dữ liệu truyền – nhận có thể bị mất mát, nhiễu, tệ hơn là bị làm sai lệch có chủ đích
* Quân đội có thể bị định vị, các hệ thống có thể bị vô hiệu hóa
* Sự đe dọa lớn tới các thông tin tuyệt mật trong an ninh – quốc phòng
  + - * 1. Các khía cạnh trong bảo mật thông tin vệ tinh
* Kiểm soát truy cập :Quy trình cấp quyền để truy cập hệ thống chỉ dành cho người sử dụng được ủy quyền. Chỉ cho phép những người dùng đã được phê chuẩn truy cập vào hệ thống điều khiển.
* Chứng thực: Xác minh danh tính của người dùng hoặc thiết bị. Chỉ những lệnh đã được chứng thực mới được hệ thống tuân theo và xử lý.
* Tính sẵn sàng: Đảm bảo cho dữ liệu luôn sẵn sàng khi nó được yêu cầu. Kỹ thuật trải phổ và nhảy tần có thể được sử dụng để ngăn ngừa tắc nghẽn.
* Tính bí mật :Đảm bảo dữ liệu chỉ được để lộ cho các hệ thống đã được chứng thực.
* Ngăn chặn việc để lộ các thông tin quan trọng trong hệ thống dữ liệu
* Bảo mật dữ liệu đường lên và đường xuống
* Ngăn chặn việc do thám thông tin từ các hệ thống trái phép
* Tính toàn vẹn **:** Đảm bảo rằng dữ liệu được truyền đi không bị sửa đổi, thay đổi hoặc phá hủy. Trong suốt quá trình truyền, dữ liệu sẽ không bị thao tác bằng bất kỳ cách nào.
* Nhiệm vụ : Đảm bảo rằng các hoạt động của hệ thống được ghi lại với nhận dạng của người dùng cũng như thời gian mà các hành động đã xảy ra.

#### Các phương pháp mật mã hóa hiện đại

**Mật mã học** là khoa học bảo vệ dữ liệu, cung cấp phương tiện và cách thức để chuyển đổi dữ liệu thành dạng không thể đọc được (*Hình 2.6*), để mà :

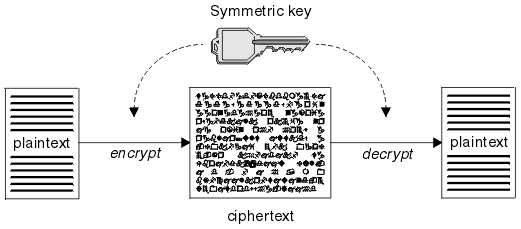
* + Không thể truy cập dữ liệu để sử dụng trái phép
  + Nội dung của khung dữ liệu được ẩn đi
  + Tính xác thực của dữ liệu có thể được thiết lập
  + Người tạo ra tin nhắn không thể phủ nhận dữ liệu của mình



Hình 2.6 Mô hình mật mã hóa, giải mật mã đơn giản

Mật mã khóa đối xứng

Mật mã khóa đối xứng hay còn gọi là mật mã khóa bí mật, cả người gửi và người nhận đều sử dụng chung một khóa cho việc mã hóa và giải mật mã. Bản mật thu được an toàn tới đâu phụ thuộc hoàn toàn vào tính bí mật của khóa. *Hình 2.7* mô tả cấu trúc của một hệ mật khóa đối xứng đơn giản.



Hình 2.7 Mô hình hệ mật đối xứng đơn giản

Ưu – nhược điểm của hệ mật khóa đối xứng :

* Ưu điểm : Rất nhanh, an toàn, ví như hệ mật AES, muốn phá được ở thời điểm hiện tại, cần hàng triệu năm
* Nhược điểm : Quá trình chuyển khóa bí mật tới người nhận (để giải mật mã) là khá nguy hiểm. Đôi khi, người ta phải sử dụng một bên thứ 3 được ủy quyền để đóng vai trò chuyển khóa.

Hệ mật khóa đối xứng được chia thành hai loại chính :

* Hệ mật khối : Mã hóa và giải mã các khối bit có độ dài cố định
* Hệ mật dòng : Mã hóa 1 bit hoặc 1 byte của bản rõ tại một thời điểm. Khóa được sử dụng là một dòng vô hạn bit giả ngẫu nhiên.

Hệ mật khối :

Hệ mật khối có Input và Output là các khối có độ dài cố định (ví dụ DES là 64 bit). Vì vậy, để làm cho bản tin đầu vào có thể chia thành các khối phù hợp với Input, cần có các bit đệm, rồi cắt bản rõ thành nhiều khối, mật mã hóa, rồi ghép các khối thu được theo một sơ đồ nào đó để có được bản mật. Các loại sơ đồ (chế độ) hay sử dụng :

* Chế độ bảng tra mã điện tử (Electronic Code Book Mode – ECB)
* Chế độ móc xích (Cipher Block Chaining Mode – CBC)
* Chế độ mã phản hồi (Cipher Feedback Mode – CFB)
* Chế độ mật mã kết quả phản hồi (Output Feedback Mode – OFB)
* Chế độ mật mã con đếm (Counter Mode – CTR)

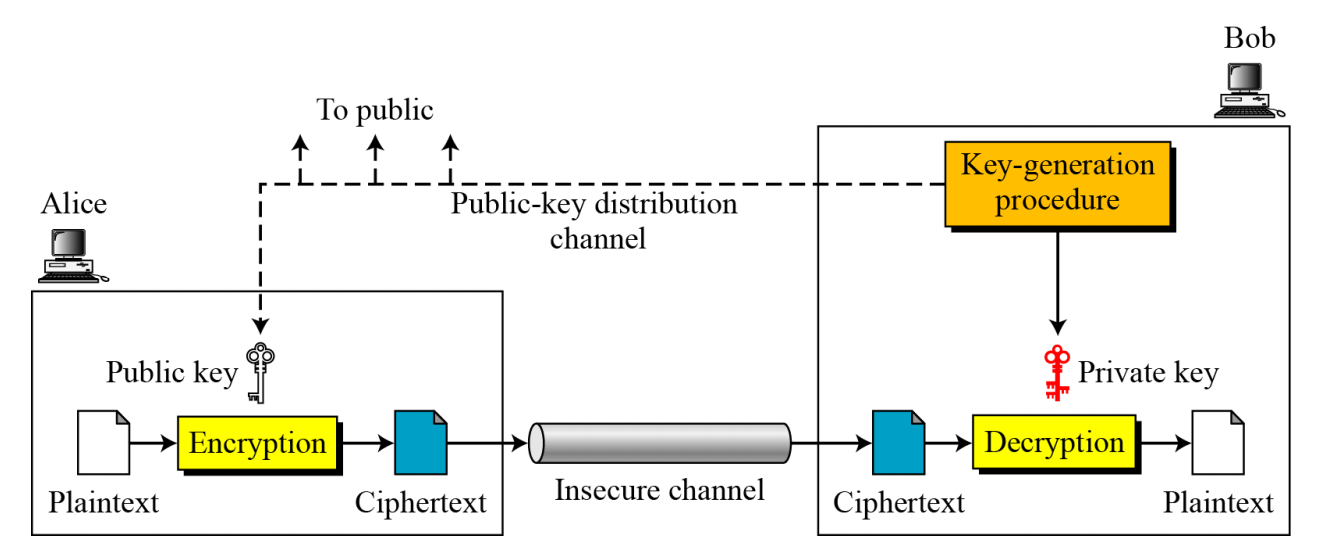
Hệ mật dòng :

Với hệ mật dòng (Stream Cipher), ta sẽ xử lý trên từng bit của bản tin đầu vào. Vì vậy ta không cần có bit đệm như hệ mật khối. Hệ mật dòng được chia thành hai loại chính :

* **Hệ mật dòng đồng bộ :** Người gửi và người nhận phải chính xác trong bước đồng bộ hóa để việc giải mã thành công. Nếu các ký tự được thêm, hoặc loại bỏ khỏi bản tin trong suốt quá trình truyền, thì sẽ mất đồng bộ, tuy vậy, chỉ mất 1 bit đơn và lỗi sẽ không lan rộng.
* **Hệ mật dòng tự đồng bộ :** Nếu các kí tự được thêm, hoặc loại bỏ, thì việc đồng bộ sẽ tự đạt được lại bằng thuật toán.

Hệ mật mã khóa công khai :

**Mật mã khóa công khai** (hay còn gọi là Hệ mật khóa bất đối xứng)sử dụng 2 khóa riêng biệt : khóa bí mật và khóa công khai. Trong đó, khóa công khai dùng để mật mã hóa, còn khóa bí mật dùng để giải mã. Điểm khác biệt của hệ mật khóa công khai so với hệ mật khóa đối xứng là việc tạo khóa diễn ra hoàn toàn ở bên người nhận (Bob). Sau khi Bob tạo khóa, Alice (người gửi) sẽ tiến hành mật mã hóa bản rõ sử dụng khóa công khai vừa được tạo. Bob giữ lại khóa bí mật, và sử dụng nó để giải mật mã từ bản mật nhận được *(Hình 2.8).*



Hình 2.8 Mô hình của một hệ mật khóa công khai

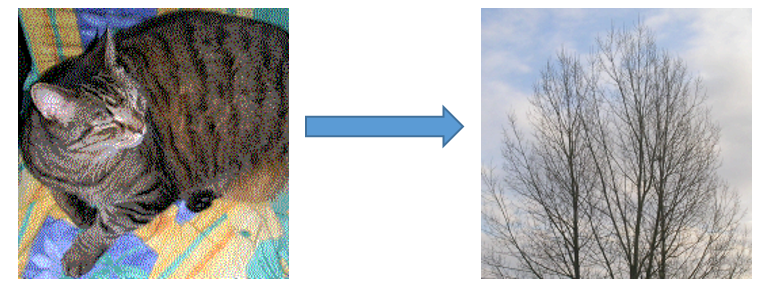
Ưu – nhược điểm của hệ mật mã khóa công khai :

* Ưu điểm : Tăng tính bảo mật : khóa bí mật không cần phải truyền hoặc chia sẻ cho bất kỳ ai. Vì vậy, không cần tới bên thứ 3 trong quá trình truyền – nhận dữ liệu. Hơn nữa, vì không cần để lộ khóa bí mật, nên có thể sử dụng một bộ khóa để giao tiếp và truyền dữ liệu với nhiều người khác nhau.
* Nhược điểm : Tốc độ là vấn đề lớn nhất của mật mã khóa công khai, nó chậm hơn rất nhiều so với các phương pháp mã hóa sử dụng khóa bí mật.

Hai phương pháp mật mã hóa là khóa công khai và khóa bí mật là bù trừ cho nhau, lợi thế của hệ mật này chính là những bất lợi của hệ mật kia. Sự phát triển của hệ mật khóa công khai thì không loại trừ sự cần thiết của hệ mật khóa đối xứng.

Kỹ thuật giấu tin (Steganography)

Steganography là kỹ thuật ẩn giấu một file, message, image hoặc video bên trong một file, message, image hoặc video khác. Nó thay các bit vô ích hoặc không sử dụng trong tập tin bằng các bit cần che giấu. Mục đích chính là để ẩn một vài thông tin quan trọng trong tập tin sao cho ngoại trừ người gửi và người nhận, thì không ai biết được sự có mặt của thông tin đó. *Hình 2.9* là kết quả giấu tin bằng hình ảnh, hình ảnh con mèo đã được giấu hoàn toàn vào hình cây, mà ta gần như không thấy có điểm gì khác thường hoặc đặc biệt để có thể nhận ra.



Hình 2.9 Kỹ thuật giấu tin vào hình ảnh

#### Tấn công một hệ mật mã

Có hai loại tấn công cơ bản trong một hệ mật mã : Tấn công bị động và Tấn công chủ động.

**Tấn công bị động** : thường được thực hiện bằng cách nghe trộm, và không thể sửa đổi dữ liệu. Một hệ thống hàng không có thể bị 2 kiểu tấn công bị động :

* Phá hoại bảo mật dữ liệu : Tiết lộ thông tin được truyền giữa trạm mặt đất và hệ thống ở không gian.
* Phá hoại bảo mật đường truyền: Tiết lộ thông tin về lưu lượng, nguồn và đích đến của thông tin.

**Tấn công chủ động :** Hacker hoàn toàn công khai và chủ động với mục đích làm giảm hiệu năng hoặc tê liệt hoạt động của hệ thống. Một vài loại tấn công cho các hệ thống hàng không :

* Modification of messages :bản tin gửi đi bị hacker thay đổi, chỉnh sửa dẫn đến sai lệch về kết quả.
* Replay Attack : một (hoặc một phần) bản tin bị hacker lưu trữ và phát lại sau đó.
* Insider Attack : người trong nội bộ cố ý nghe trộm, ăn cắp thông tin, sử dụng gian lận và truy cập trái phép.
* Software threads : các chương trình như virus, worms,… cho phép bỏ qua các điều kiện bảo mật thông thường, nên có thể trực tiếp thao tác hoặc gửi các bản tin.

Tấn công một hệ mật dòng :

**Tấn công biết bản mật (Known Ciphertext Attack) :** là mô hình tấn công căn bản nhất, hacker chỉ biết các bản mật, với mục tiêu là biết được một (vài) bản rõ, hoặc khóa (là phá giải hoàn hoàn).

**Tấn công biết bản rõ (Known Plaintext Attack)** : Hacker biết một số cặp bản rõ - bản mật tương ứng. Mục tiêu là giống nhưng mô hình này mạnh hơn nhiều so với việc chỉ biết các bản mật.

**Tấn công bản rõ chọn sẵn (Chosen Plaintext Attack) :** Giống như mô hình biết bản rõ, nhưng mô hình này hacker còn có thể soạn ra một số bản rõ và lấy được các bản mật tương ứng. Việc này sẽ giúp hacker có thêm nhiều thông tin để phân tích, qua đó làm giảm tính bảo mật của hệ thống.

**Tấn công bản mật chọn sẵn (Known Ciphertext Attack) :** tương tự mô hình bản rõ chọn sẵn. Với cả 2 mô hình, hacker thường chọn các bản mật (hoặc bản rõ) dựa vào thông tin đã được phân tích từ các cặp có sẵn.

**Tấn công kênh bên (Side Channel Attack) :** tấn công vào khu vực thông tin được tạo ra do quá trình hoạt động của thiết bị phần cứng, phổ biến nhất là *nguồn điện tiêu thụ, tín hiệu bức xạ điện từ, độ trễ thời gian*. Thông tin rò rỉ được phân tích thống kê để tìm các mối liên quan tới các phép toán, hoặc thậm chí là khóa.

**Tấn công lật bit (Bit Flipping Attack) :** Hacker có thể thay đổi bản mật để làm sai lệch bản rõ (có chủ đích), kể cả khi không thực sự biết bản rõ là gì. Loại tấn công này có thể tránh bằng cách sử dụng mã MAC (Message Authentication Code) để tăng khả năng phát hiện giả mạo.

*Ví dụ* : Một bản tin “*I owe you $100.00*” bị thay đổi một chi tiết rất nhỏ, thành “*I owe you $10000*” cũng có thể dẫn đến sự sai lệch lớn về thông tin nhận được.

Tấn công một hệ mật khối :

**Tấn công vét cạn (Brute Force Attack)** : Thử từng chuỗi khóa cho đến khi tìm được khóa chính xác. Loại này cần thời gian rất lâu nên thường chỉ được sử dụng khi các phương pháp khác đều không hiệu quả.

**Thám mã tuyến tính (Linear Cryptanalysis)** : Hacker sử dụng lợi thế của các quan hệ phi tuyến giữa đầu vào và đầu ra của khóa. Cách tiếp cận thông thường là phân tích các thành phần phi tuyến và xấp xỉ chúng.

**Thám mã vi sai (Differential Cryptanalysis) :** Hacker phân tích sự khác nhau của những bản rõ đối với sự khác biệt của các bản mật kết quả. Những khác biệt này dùng để gán xác suất cho các khóa và tìm ra những khóa có khả năng cao nhất.

#### So sánh các thuật toán bảo mật trong thông tin vệ tinh được đề xuất

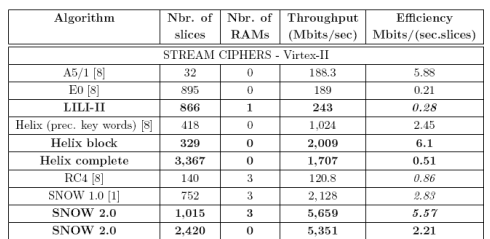
1. Các tiêu chí so sánh

Các hệ mật có các cách triển khai khác nhau, do đó các thông số yêu cầu để triển khai trên phần cứng, cũng như kết quả, độ an toàn, thời gian thực hiện cũng là khác nhau. Đồng thời, với mỗi mục đích, mỗi kênh truyền, cũng có những tiêu chí đánh giá khác nhau. Trong thông tin vệ tinh, ta sẽ quan tâm tới 3 thông số chính, đó là :

* **Thông lượng (Throughput)** : tổng số bit được mã hóa và giải mã trong một đơn vị thời gian.
* **Throughput per slice** : Thông lượng đáp ứng với mỗi slice, thông số này tính toán hiệu quả của chi phí phần cứng sử dụng để triển khai.
* **Độ trễ (Latency) :** Thời gian cần thiết để mã hóa và giải mã một khối đơn của bản rõ hoặc bản mật.

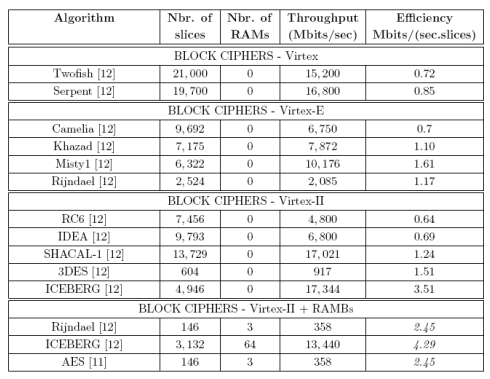
1. So sánh hiệu suất của các thuật toán

Đối với các hệ mật dòng :



Hình 2.10 So sánh hiệu suất của các hệ mật dòng

Đối với các hệ mật khối :



Hình 2.11 So sánh hiệu suất của các hệ mật khối

Một vài kết luận rút ra từ các bảng so sánh :

* Thuật toán A5/1 tỏ ra hiệu quả nhất, nhưng trên thực tế, nó lại là yếu nhất, nên gần như không thể sử dụng.
* Helix tỏ ra hiệu quả nhưng lại không thực tế vì nó yêu cầu phần mềm tính toán trước, đòi hỏi chi phí và phần cứng triển khai sẽ tăng lên nhiều so với các hệ mật khác.
* SNOW2.0 được xem là hệ mật dòng phù hợp nhất và có thể so sánh với ICEBERG.
* So sánh giữa AES với ICEBERG chỉ ra rằng AES là phù hợp hơn với các thiết bị hàng không, vì không cần thông lượng quá cao.

1. Đề xuất lựa chọn của CCSDS

CCSDS (The Consultative Committee for Space Data Systems), được thành lập năm 1982, là nơi đưa ra các khuyến nghị và tiêu chuẩn cho các hệ thống dữ liệu thông tin không gian. Các tiêu chuẩn của CCSDS giúp giảm gánh nặng chi phí nghiên cứu bằng cách chia sẻ giữa các cơ quan và thương mại hóa một cách có hiệu quả.

CCSDS đề xuất sử dụng hệ mật khối thay vì hệ mật dòng vì :

* Hệ mật khối nhanh hơn và nhiều thuật toán có thể được triển khai mà không cần phải thay đổi về phần cứng.
* Hệ mật dòng có thể dễ gặp phải những vấn đề bảo mật nghiêm trọng nếu sử dụng không đúng cách.

*Bỏ qua BLOWFISH, TEA, IDEA, SEED, Ủy ban CCSDS đã giới thiệu hệ mật AES, với sơ đồ Counter Mode để sử dụng cho các ứng dụng vệ tinh.*

#### Kết luận

Đề tài “***Tìm hiểu về Bảo mật trong thông tin vệ tinh***” không phải là một đề tài để em có thể triển khai thực tế, mà chủ yếu là việc tổng hợp các tài liệu từ nhiều nguồn khác nhau, cả tiếng Việt lẫn tiếng Anh, để tóm tắt lại thành một báo cáo (hoặc slide) cụ thể. Việc tổng hợp các tài liệu này trong thời gian 2 tuần đã giúp em ôn lại một phần kiến thức của các môn học Lý thuyết mật mã, Tín hiệu và hệ thống, Thông tin số,… Một kỹ năng quan trọng hơn em có được sau khi thực hiện công việc này là kỹ năng đọc tài liệu chuyên ngành bằng tiếng Anh. Mặc dù có thể đọc – dịch tiếng Anh khá tốt, nhưng với lượng tài liệu nhiều và chuyên sâu, cũng đòi hỏi em về kỹ năng đọc lướt tìm thông tin, đọc kỹ và bóc tách từng vấn đề để hiểu sâu hơn, cũng như loại bỏ các phần lan man, hoặc không cần thiết, hoặc quá sâu trong một bài báo (journal), một bài luận án (thesis),… Đây sẽ là những kỹ năng tuyệt vời cho em, không chỉ với các môn học chuyên ngành tiếp theo, mà còn với các công việc mới sau này.

# KẾT LUẬN

Bài báo cáo là những nội dung chính em được thực tập và được học tại ASE Lab. Ngoài ra em còn được học rất nhiều điều khác mà không phải lý thuyết là có thể định nghĩa được. Thời gian vừa qua là một sự trải nghiệm khá thú vị đối với em tại Lab, khác hẳn với hình thức “thầy giảng – trò nghe” trên lớp học khoảng 3 tiết/môn/tuần. Ở đây, em được chủ động tìm hiểu nội dung được giao hơn, ý thức được trách nhiệm của bản thân hơn, dám mạnh dạn đưa ra ý kiến của mình nhiều hơn, để được lắng nghe những phản hồi của các thầy để cùng tiến bộ với các bạn. Hơn nữa, em còn được học nhiều kỹ năng khác, mà chỉ có “lăn xả” vào công việc thực tế, em mới có thể rèn luyện được. Hy vọng trong tương lai, tiếp tục gắn bó với ASE Lab, tiếp tục làm việc với các thầy, các anh chị, các bạn, các em trong Lab, em chắc chắn sẽ quyết tâm cố gắng học tập nhiều hơn, trau dồi cải thiện kỹ năng nhiều hơn để hướng tới những mục tiêu dài hạn hơn trong tương lai.

Em xin chân thành cảm ơn Viện Điện tử - Viễn thông đã tạo điều kiện để em có thể được thực tập tại ASE Lab. Em cũng cảm ơn thầy Đỗ Trọng Tuấn, thầy Hán Trọng Thanh, và các anh chị K55, K57, K58, cũng như các bạn cùng thực tập, đã nhiệt tình hướng dẫn, giúp em không chỉ có thêm nhiều kiến thức mới, mà còn giúp em rèn luyện được thêm nhiều kỹ năng mềm như tiếng Anh, làm việc nhóm, báo cáo, thuyết trình,…

# TÀI LIỆU THAM KHẢO

|  |  |
| --- | --- |
| [1] | Phạm Hoàng Anh, *Giới thiệu về phòng ASE Lab*, Hà Nội, 2015. |
| [2] | Carrick Detweiler, Sebastian Elbaum [Online] <http://research.unl.edu/annualreport/2014/water-slurping-drones-have-broad-potential/>, 2013 – 2014 UNL Research Report |
| [3] | <https://www.tinkercad.com/> |
| [4] | Các file datasheet được tìm kiếm tại Google |
| [5] | Rajesh Azmera, Shakun Yawatkar, Slide “A study of Cryptography for Satellite Applications” |
| [6] | Omar M.Barukab, Asif Irshad Khan, Mahaboob Sharief Shaik , MV Ramana Murthy, Shahid Ali Khan, “Secure Communication using Symmetric and Asymmetric Cryptographic Techniques”, Modern Education and Computer Science Press, 2012 |
| [7] | Bộ môn Điện tử Hàng không Vũ trụ - Viện Điện tử Viễn thông, Đại học Bách Khoa Hà Nội, Slide “Lý thuyết mật mã” |

# PHỤ LỤC : Code Arduino

#include <Servo.h>

#define SERVO\_PIN 9

Servo myServo;

float count = 0; // bien dem so xung

float radius=15; // (mm) chon ban kinh cua rong roc bang 15mm

// ham dem so xung khi keng A ngat canh xuong

void pulse()

{

if(digitalRead(4) == LOW)

count++;

else

count--;

}

void setup()

{

myServo.attach(SERVO\_PIN);

//chan 9 la chan output cua arduino ra servo

Serial.begin(9600); // giao tiep voi cong serial

pinMode(2, INPUT\_PULLUP); // chan 2 la  dau vao xung

pinMode(4, INPUT\_PULLUP);

attachInterrupt(0, pulse, FALLING);

// khi kenh A chuyen tu muc cao xuong thap thi goi ham pulse

}

void loop()

{

static int set = -1;

// -1 la trang thai ban dau

float l=(count/334)\*2\*3.14\*radius;

// tinh chieu dai day the radius

Serial.println(l);

if (l>1000&&l<1200&&set==-1)

set = 1;

// 1 la trang thai lay mau nuoc

else if (set == 1)

set =0;

if (set==-1){

myServo.write(85);

};

if (set== 1){

for (int i=85; i<=164; i++){

Serial.println(l);

if (l<1000||l>1200) break;

myServo.write(i);

delay(100);

}

set=0;

// 0 la trang thai da lay xong -> khong thay doi

}

}