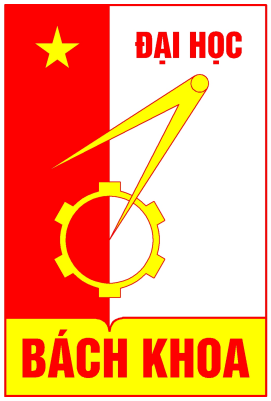
TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI
VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

_____*******_____



ĐỒ ÁN TỐT NGHIỆP
NGÀNH KHOA HỌC MÁY TÍNH

Cài đặt bảo mật cho các thiết bị IOT

Sinh viên thực hiện:
Đặng Quang Trung 20134145 CNTT2.03-K58

Giảng viên:
TS. Trần Vĩnh Đức

Hà Nội 21-04-2018

Lời cảm ơn

Trước khi trình bày nội dung của đồ án này, tôi xin được gửi lời cảm ơn sâu sắc và chân thành nhất đến TS. Trần Vĩnh Đức, người đã tận tình hướng đẫn tôi trong suốt quá trình thực hiện đồ án này cũng như những năm tháng học tại trường Đại học Bách Khoa Hà Nội. Đồng thời tôi cũng xin bày tỏ lòng biết ơn đến các thầy cô trường Đại học Bách Khoa Hà Nội, Viện công nghệ thông tin và truyền thông, đặc biệt là các thầy cô bộ môn Khoa học máy tính đã tận tình chỉ dạy cho tôi trong những năm tháng học tập ở trường.

Đồng thời tôi xin gửi lời cảm ơn đến gia đình, bạn bè đã luôn ở bên tôi, đông viên và giúp đỡ tôi trong suốt quá trình học tập và thực hiện đồ án tốt nghiệp.

Mục lục

Bảng chữ viết tắt

Danh sách hình vẽ

Giới thiệu chung

Mật mã học là một lĩnh vực liên quan với các kỹ thuật ngôn ngữ và toán học để đảm bảo an toàn thông tin, cụ thể là trong thông tin liên lạc. Về phương diện lịch sử, mật mã học gắn liền với quá trình mã hóa, điều này có nghĩa là nó gắn với các cách thức để chuyển đổi thông tin từ dạng này sang dạng khác nhưng ở đây là từ dạng thông thường có thể nhận thức được thành dạng không thể nhận thức được, làm cho thông tin trở thành dạng không thể đọc được nếu như không có các kiến thức bí mật. Quá trình mã hóa được sử dụng chủ yếu để đảm bảo tính bí mật của các thông tin quan trọng, chẳng hạn trong công tác tình báo, quân sự hay ngoại giao cũng như các bí mật về kinh tế, thương mại. Trong những năm gần đây, lĩnh vực hoạt động của mật mã hóa đã được mở rộng: mật mã hóa hiện đại cung cấp cơ chế cho nhiều hoạt động hơn là chỉ duy nhất việc giữ bí mật và có một loạt các ứng dụng như: chứng thực khóa công khai, chữ ký số, bầu cử điện tử hay tiền điện tử. Ngoài ra, những người không có nhu cầu thiết yếu đặc biệt về tính bí mật cũng sử dụng các công nghệ mật mã hóa, thông thường được thiết kế và tạo lập sẵn trong các cơ sở hạ tầng của công nghệ tính toán và liên lạc viễn thông.

Mật mã học là một lĩnh vực liên ngành, được tạo ra từ một số lĩnh vực khác. Các dạng cổ nhất của mật mã hóa chủ yếu liên quan với các kiểu mẫu trong ngôn ngữ. Gần đây thì tầm quan trọng đã thay đổi và mật mã hóa sử dụng và gắn liền nhiều hơn với toán học, cụ thể là toán học rời rạc, bao gồm các vấn đề liên quan đến lý thuyết số, lý thuyết thông tin, độ phức tạp tính toán, thống kê và tổ hợp. Mật mã hóa cũng được coi là một nhánh của công nghệ, nhưng nó được coi là không bình thường vì nó liên quan đến các sự chống đối ngầm (xem công nghệ mật mã hóa và công nghệ an ninh). Mật mã hóa là công cụ được sử dụng trong an ninh máy tính và mạng.

Chương 1

Cơ sở lý thuyết

1.1 Cơ sở mật mã

1.2 Khóa đối xứng

1.3 Khóa công khai

1.4 Hàm băm

1.5 Chữ ký điện tử

1.6 Chứng thư số

Chương 2

Mật mã dựa trên đường cong Elliptic

2.1 Đường cong Elliptic

2.2 Mật mã dựa trên đường cong Elliptic

Chương 3

Chứng thư số ẩn dựa trên đường cong Elliptic

Chương 4

Cài đặt cho thiết bị IoT

Kết luận và hướng phát triển

Lập kế hoạch vận tải hàng hoá là một lĩnh vực đặc biệt quan trọng trong nền kinh tế mỗi quốc gia. Các mô hình vận tải mới không ngừng được đề xuất mang lại thuận tiện, giảm chi phí vận tải. Trong đồ án này, chúng tôi khảo sát mô hình vận tải hang hoá kết hợp xe tải và thiết bị bay Drone. Xe tải có khả năng vận chuyển các hang hoá nặng, di chuyển trên hành trình dài, trong khi thiết bị bay Drone chỉ có khả năng vận chuyển hang hoá nhẹ, nhanh, nhưng quãng đường di chuyển ngắn do hạn chế về năng lượng nạp.

Cụ thể, đồ án dựa trên nghiên cứu của Hà Quang Minh và cộng sự trong đó đề xuất thuật toán heuristics giải bài toán lập lộ trình vận tải kết hợp 1 xe tải và 1 thiết bị bay với mục tiêu là chi phí nhỏ nhất. Chúng tôi đã đề xuất thử nghiệm mô hình 1 xe tải kết hợp với nhiều thiết bị bay (2,3,4). Chúng tôi đã cài đặt thuật toán được đề xuất bởi Hà Quang Minh cho mô hình với nhiều Drone***. Kết quả thử nghiệm cho thấy bằng việc kết hợp với nhiều hơn 1 drone thì chi phí sẽ giảm hơn so với việc sử dung 1 drone.

Trong tương lai, chúng tôi sẽ cố gắng phát triển thuật toán trên các mô hình vận chuyển hàng hóa kết hợp xe tải và drone khác như: bài toán vận chuyển hàng hóa kết hợp xe tải và drone nhiều lộ trình, bài toán nhận hàng và đón hàng kết hợp xe tải và drone .... Ngoài ra chúng tôi cũng thiết kế và cài đặt thêm một vài thuật toán với heuristic mới để đem lại kết quả tốt hơn nữa cho bài toán.

Tài liệu tham khảo

[1] http://www.csplib.org/Problems/prob030/

[2] Slide Trí tuệ nhân tạo thầy Nguyễn Nhật Quang. Chương 5 : Thỏa mãn ràng buộc

[3] Stuart Russell and Peter Norvig *Artificial Intelligence: A Modern Approach* 2nd edition, Prentice Hall, page 137, 2003.

[4] Ha Quang Minh and Deville Yves and Pham Quang Dung and Ha Minh Hoang, *On the min cost traveling salesman problem with drone*, arXiv preprint arXiv:1509.08764, 2015

[5] S. Banker, Amazon and drones – here is why it will work (dec 2013). URL http://www.forbes.com/sites/stevebanker/2013/12/19/amazon-drones-here-is-why-it-will-work/

[6] Nguyễn Đức Nghĩa, Nguyễn Tô Thành *Toán rời rạc* 3rd edition, Nhà xuất bản đại học quốc gia Hà Nội, page 107-108, 2006.

[7] Slide Tối ưu hóa tổ hợp thầy Nguyễn Đức Nghĩa. Chương mở đầu, Bài toán vận tải.

[8] Slide Tìm kiếm cục bộ dựa trên ràng buộc thầy Phạm Quang Dũng. Chương 5: Contraint-base local search applications.

[9] Slide Phân tích và thiết kế thuật toán thầy Nguyễn Đức Nghĩa. Chương 5: Quy hoạch động, Chương 3: Greedy Algorithms.

[10] Francesca Rossi, Peter van Beek, Toby Walsh *Handbook of Constraint Programming* 1st edition, Elsevier Science, page 107-108, 2006.

[11] Bài giảng môn tính toán tiến hóa cô Huỳnh Thị Thanh Bình. Thuật giải di truyền.

[12] Rupert Howell,Jonathon Wong *Apache OFBiz Development: The Beginner's Tutorial*, Paperback , page 53, 2008. truyền.

[13] Ruth Hoffman *Apache OFBiz Cookbook*, Paperback , page 28, 2010.

[14] Apache Ofbiz (wikipedia) https://en.wikipedia.org/wiki/Apache_OFBiz