TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP. HCM

**KHOA CÔNG NGHỆ THÔNG TIN**

**BÁO CÁO HỌC PHẦN**

**Tên học phần: Lập trình mạng máy tính**

**Đề tài:**

**PHẦN MỀM QUẢN LÝ HỌC TẬP**

**VÀ**

**MÃ HÓA CỔ ĐIỂN PLAYFAIR**

Giảng viên hướng dẫn: **ThS. Đàm Minh Lịnh**

Sinh viên thực hiện:

Họ và tên Mã số sinh viên Lớp

**Nguyễn Đức Hậu 1911066071 19DTHE4**

**Đỗ Thành Công 1911066578 19DTHE4**

**Nguyễn Hữu Anh Tú 1911062281 19DTH**

*Thành phố Hồ Chí Minh, 10/2022*

MỤC LỤC HÌNH

[Hình 1. Phần mềm Netbeans 2](#_Toc117239577)

[Hình 2. Java Development Kid(JDK) 2](#_Toc117239578)

[Hình 3. Ngôn ngữ lập trình Java 3](#_Toc117239579)

[Hình 4. Phần mềm quản lý mã nguồn phân tán Git 4](#_Toc117239580)

[Hình 5. Dịch vụ cung cấp kho lưu trữ mã nguồn Git – GitHub 5](#_Toc117239581)

[Hình 6. Ngôn ngữ truy vấn SQL 6](#_Toc117239582)

[Hình 7. SQL Server 7](#_Toc117239583)

[Hình 8. Giao thức TCP 8](#_Toc117239584)

[Hình 9. Giao thức UDP 9](#_Toc117239585)

[Hình 10. Sơ đồ chức năng 12](#_Toc117239586)

[Hình 11. Background 12](#_Toc117239587)

[Hình 12. Mã hóa đăng ký 13](#_Toc117239588)

[Hình 13. Mã hóa đăng nhập 13](#_Toc117239589)

[Hình 14. Giải mã tài khoản 13](#_Toc117239590)

[Hình 15. Cơ sở dữ liệu sau khi mã hóa 14](#_Toc117239591)

[Hình 16. Giao diện form chính 14](#_Toc117239592)

MỤC LỤC

[NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN vi](#_Toc117239593)

[CHƯƠNG 1: TỔNG QUAN 1](#_Toc117239594)

[1.1. Xu thế hiện nay 1](#_Toc117239595)

[1.2. Công nghệ áp dụng 2](#_Toc117239596)

[1.2.1. Apache Netbeans IDE 2](#_Toc117239597)

[1.2.2. Java Development Kit(JDK) 2](#_Toc117239598)

[1.2.3. Ngôn ngữ lập trình Java 3](#_Toc117239599)

[1.2.4. Phần mềm quản lý mã nguồn phân tán Git 4](#_Toc117239600)

[1.2.5. Dịch vụ cung cấp kho lưu trữ mã nguồn Git dựa trên nền tảng web GitHub 5](#_Toc117239601)

[1.2.6. Ngôn ngữ truy vấn SQL 6](#_Toc117239602)

[1.2.7. SQL Server 7](#_Toc117239603)

[CHƯƠNG 2: CƠ SỞ LÝ THUYẾT 8](#_Toc117239604)

[2.1. Giao thức TCP 8](#_Toc117239605)

[2.2. Giao thức UDP 9](#_Toc117239606)

[2.3. Chương trình mã hóa Playfair 10](#_Toc117239607)

[2.3.1. Tổng quan 10](#_Toc117239608)

[2.3.2. Ưu điểm của Playfair Cipher 11](#_Toc117239609)

[2.3.3. Nhược điểm của Playfair Cipher 11](#_Toc117239610)

[2.3.4. Quy tắc mã hóa Playfair 11](#_Toc117239611)

[CHƯƠNG 3: CHƯƠNG TRÌNH & ĐÁNH GIÁ 12](#_Toc117239612)

[3.1. Sơ đồ chức năng 12](#_Toc117239613)

[3.2. Background 12](#_Toc117239614)

[3.2.1. Mã hóa đăng ký 13](#_Toc117239615)

[3.2.2. Mã hóa thông tin nhập vào khi đăng nhập để trùng khớp 13](#_Toc117239616)

[3.2.3. Giải mã tài khoản để hiện lên form chính 13](#_Toc117239617)

[3.3. Kết luận và đánh giá 14](#_Toc117239618)

[3.3.1. Cơ sở dữ liệu sau khi mã hóa đăng ký 14](#_Toc117239619)

[3.3.2. Sau khi giải mã hiển thị lên form chính 14](#_Toc117239620)

[3.3.3. Đánh giá 14](#_Toc117239621)

[CHƯƠNG 4: HƯỚNG PHÁT TRIỂN, MẶT TÍCH CỰC 15](#_Toc117239622)

[4.1. Hướng phát triển 15](#_Toc117239623)

[4.2. Mặt tích cực 15](#_Toc117239624)

[Tài liệu tham khảo 16](#_Toc117239625)

**LỜI MỞ ĐẦU**

Ngày nay, khi mạng Internet đã kết nối các máy tính ở khắp nơi trên thế giới lại với nhau, thì vấn đề bảo vệ máy tính khỏi sự thâm nhập phá hoại từ bên ngoài là một điều cần thiết. Thông qua mạng Internet, các hacker có thể truy cập vào các máy tính trong một tổ chức (dùng telnet chẳng hạn), lấy trộm các dữ liệu quan trọng như mật khẩu, thẻ tín dụng, tài liệu… Hoặc đơn giản chỉ là phá hoại, gây trục trặc hệ thống mà tổ chức đó phải tốn nhiều chi phí để khôi phục lại tình trạng hoạt động bình thường.Dựa trên kiến thức lập trình đã học với Java, sự đa dạng của các dịch vụ mạng với nhiều tính năng và đòi hỏi ngày càng cao. Từ ý tưởng áp dụng công nghệ thông tin vào việc quản lý, bớt phần gánh nặng về sổ sách cũng như đầu óc con người, đồ án này hướng đến xây dựng mã hóa thông tin người dùng bằng Playfair Cipher.

Để thực hiện việc bảo vệ này, người ta dùng khái niệm “kiểm soát truy cập” (Access Control). Khái niệm kiểm soát truy cập này có hai yếu tố sau:

• Chứng thực truy cập (Authentication): xác nhận rằng đối tượng (con người hay chương trình máy tính) được cấp phép truy cập vào hệ thống. Ví dụ: để sử dụng máy tính thì trước tiên đối tượng phải logon vào máy tính bằng username và password. Ngoài ra, còn có các phương pháp chứng thực khác như sinh trắc học (dấu vân tay, mống mắt…) hay dùng thẻ (thẻ ATM…).

• Phân quyền (Authorization): các hành động được phép thực hiện sau khi đã truy cập vào hệ thống. Ví dụ: bạn được cấp username và password để logon vào hệ điều hành, tuy nhiên bạn chỉ được cấp quyền để đọc một file nào đó. Hoặc bạn chỉ có quyền đọc file mà không có quyền xóa file.

Với nguyên tắc như vậy thì một máy tính hoặc một mạng máy tính được bảo vệ khỏi sự thâm nhập của các đối tượng không được phép. Tuy nhiên thực tế chúng ta vẫn nghe nói đến các vụ tấn công phá hoại. Để thực hiện điều đó, kẻ phá hoại tìm cách phá bỏ cơ chế Authentication và Authorization bằng các cách thức sau:

• Dùng các đoạn mã phá hoại (Malware): như virus, worm, trojan, backdoor… những đoạn mã độc này phát tán lan truyền từ máy tính này qua máy tính khác dựa trên sự bất cẩn của người sử dụng, hay dựa trên các lỗi của phần mềm. Lợi dụng các quyền được cấp cho người sử dụng (chẳng hạn rất nhiều người login vào máy tính với quyền administrator), các đoạn mã này thực hiện các lệnh phá hoại hoặc dò tìm password của quản trị hệ thống để gửi cho hacker, cài đặt các cổng hậu để hacker bên ngoài xâm nhập.

• Thực hiện các hành vi xâm phạm (Intrusion): việc thiết kế các phần mềm có nhiểu lỗ hổng, dẫn đến các hacker lợi dụng để thực hiện những lệnh phá hoại. Những lệnh này thường là không được phép đối với người bên ngoài, nhưng lỗ hổng của phần mềm dẫn đến được phép. Trong những trường hợp đặc biệt, lỗ hổng phần mềm cho phép thực hiện những lệnh phá hoại mà ngay cả người thiết kế chương trình không ngờ tới. Hoặc hacker có thể sử dụng các cổng hậu do các backdoor tạo ra để xâm nhập. Để khắc phục các hành động phá hoại này, người ta dùng các chương trình có chức năng gác cổng, phòng chống. Những chương trình này dò tìm virus hoặc dò tìm các hành vi xâm phạm đển ngăn chặn chúng, không cho chúng thực hiện hoặc xâm nhập. Đó là các chương trình chống virus, chương trình firewall… Ngoài ra các nhà phát triển phần mềm cần có quy trình xây dựng và kiểm lỗi phần mềm nhằm hạn chế tối đa những lỗ hổng bảo mật có thể có.

Trong quá trình xây dựng chương trình do thời gian ngắn và kiến thức còn hạn chế nên không tránh khỏi những sai sót. Kính mong thầy và các bạn đóng góp ý kiến xây dựng để đồ án được hoàn thiện hơn.

Từ những lý do trên, cùng sự hướng dẫn của Giảng viên ThS. **Đàm Minh Lịnh**, chúng em thực hiện đề tài này để vận dụng những kiến thức đã được học.

Chúng em xin chân thành cảm ơn!

# NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN

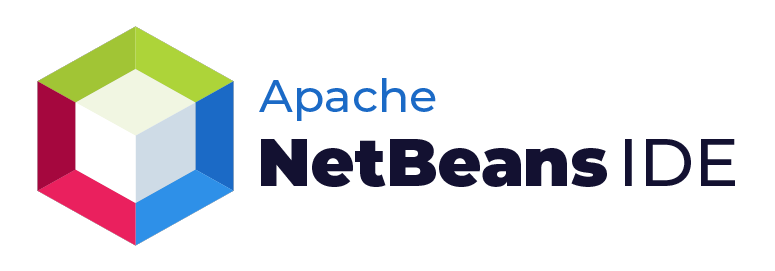
# CHƯƠNG 1: TỔNG QUAN

## Xu thế hiện nay

Ngày nay, công nghệ thông tin đã có những bước phát triển vô cùng mạnh mẽ về cả chiều sâu và chiều rộng. Máy tính, Internet không còn xa lạ với mọi người mà nó đang ngày càng trở nên phổ biến giúp con người rất nhiều trong công việc cũng như giải trí. Bên cạnh đó, trong những năm gần đây với sự phát triển mạnh mẽ cùng sự ra đời của nhiều công ty, xí nghiệp, … thì quản lý truyền thống là bất khả thi và không đem lại hiệu quả công việc, tốn kém nhiều thời gian thì việc ra đời và sử dụng các ứng dụng quản lý cũng là một điều hiển nhiên. Hiện nay, hầu hết các tổ chức kinh doanh, công ty vừa và nhỏ cũng đều sử dụng các phần mềm quản lý để hỗ trợ tối đa cho công việc. Điều đó giúp cho họ có thể triển khai công việc nhanh chóng, dễ dàng và ít tốn kém thời gian hơn rất nhiều. Đi kèm với đó là nhu cầu về an toàn bảo mật thông tin để tránh những trường hợp tin tặc tống tiền hay các đối thủ lợi dụng lỗ hổng để lấy các thông tin quan trọng nhằm cạnh trạng không lành mạnh. Chính vì lẽ đó nên công nghệ thường phải đi kèm với sự an toàn, bảo mật tuyệt đối. Chúng em đã tìm hiểu và sẽ đề cập đến một kiểu bảo mật cổ điển thông dụng đó là PLayfair Cipher.

## Công nghệ áp dụng

* + 1. Apache Netbeans IDE



Hình . Phần mềm Netbeans

NetBeans là một môi trường phát triển tích hợp (IDE) cho Java. NetBeans cho phép các ứng dụng được phát triển từ một tập hợp các thành phần phần mềm được gọi là modules. NetBeans chạy trên Windows, macOS, Linux và Solaris. Ngoài việc phát triển Java, nó còn có các phần mở rộng cho các ngôn ngữ khác như PHP, C, C++, HTML5,[4] và JavaScript. Các ứng dụng dựa trên NetBeans, bao gồm NetBeans IDE, có thể được mở rộng bởi các nhà phát triển bên thứ ba.

* + 1. Java Development Kit(JDK)



Hình . Java Development Kid(JDK)

Java Development Kit (JDK - Bộ công cụ cho người phát triển ứng dụng bằng ngôn ngữ lập trình Java) là một tập hợp những công cụ phần mềm được phát triển bởi Sun Microsystems dành cho các nhà phát triển phần mềm, dùng để viết những applet Java hay những ứng dụng Java - bộ công cụ này được phát hành miễn phí gồm có trình biên dịch, trình thông dịch, trình giúp sửa lỗi (debugger, trình chạy applet và tài liệu nghiên cứu.

* + 1. Ngôn ngữ lập trình Java



Hình . Ngôn ngữ lập trình Java

Java là một một ngôn ngữ lập trình hiện đại, bậc cao, hướng đối tượng, bảo mật và mạnh mẽ. và là một Platform.

Platform: Bất cứ môi trường phần cứng hoặc phần mềm nào mà trong đó có một chương trình chạy, thì được hiểu như là một Platform. Với môi trường runtime riêng cho mình (JRE) và API, Java được gọi là Platform.

Ngôn ngữ lập trình Java ban đầu được phát triển bởi Sun Microsystems do James Gosling khởi xướng và phát hành vào năm 1995. Phiên bản mới nhất của Java Standard Edition là Java SE 8. Với sự tiến bộ của Java và sự phổ biến rộng rãi của nó, nhiều cấu hình đã được xây dựng để phù hợp với nhiều loại nền tảng khác nhau. Ví dụ: J2EE cho các ứng dụng doanh nghiệp, J2ME cho các ứng dụng di động.

Các phiên bản J2 mới đã được đổi tên thành Java SE, Java EE và Java ME. Phương châm của java là "Write Once, Run Anywhere" - viết một lần chạy nhiều nơi, nghĩa là bạn chỉ cần viết một lần trên window chẳng hạn, sau đó vẫn chương trình đó bạn có thể chạy trên Linux, Android, các thiết bị J2ME...

* + 1. Phần mềm quản lý mã nguồn phân tán Git



Hình . Phần mềm quản lý mã nguồn phân tán Git

Git là hệ thống quản lý các phiên bản dưới dạng phân tán. Đây là hệ thống quản lý phổ biến nhất hiện nay. Git là một phiên bản của Distributed Version Control System – DVCS hay còn gọi là VCS. Sử dụng Git sẽ đem tới cho các lập trình viên một kho lưu trữ, trong đó chứa đầy đủ các lịch sử thay đổi của hệ thống.

Git là một VCS. Tuy nhiên, so với các VCS thông thường, Git cũng có một số điểm khác biệt. Trong đó, điểm khác biệt nổi bật nhất của Git đó là cách đọc và lưu trữ dữ liệu của phần mềm này.

Về mặt khái niệm, hầu hết các hệ thống lưu trữ thông tin bằng cách thay đổi dựa trên file và lưu trữ thông tin dưới dạng danh sách. Hệ thống này sẽ tổng hợp và cập nhật thông tin, sau đó lưu trữ dưới dạng một tập hợp danh sách. Các file có thể thay đổi theo thời gian.

Tuy nhiên, cách hoạt động và lưu trữ thông tin của Git lại hoàn toàn khác. Để lưu trữ thông tin, Git sẽ coi các thông tin là một tập hơn snapshot. Đây là tập hợp toàn bộ ảnh chụp các nội dung của file thông tin tại thời điểm.

Khi bạn đưa ra các lệnh, git sẽ chụp lại thông tin ở thời điểm đó và tạo ra một snapshot. Để nâng cao tính hiệu quả, Git sẽ không lưu trữ file nếu các tệp không có sự thay đổi. Thay vào đó, phần mềm sẽ liên kết dữ liệu tới một tệp giống với file đã được lưu trữ trước đó.

Nhờ vào điểm khác biệt với các VCS này, Git sẽ không tốn nhiều thời gian xem xét các thông tin, các bản giải mã của phiên bản/hệ thống trước. Thay vào đó, Git nghĩ về dữ liệu khác đi, giúp việc lưu trữ dễ dàng hơn. Với cách lưu trữ thông minh này, Git giống như một hệ thống gồm nhiều tệp nhỏ khác nhau.

* + 1. Dịch vụ cung cấp kho lưu trữ mã nguồn Git dựa trên nền tảng web GitHub

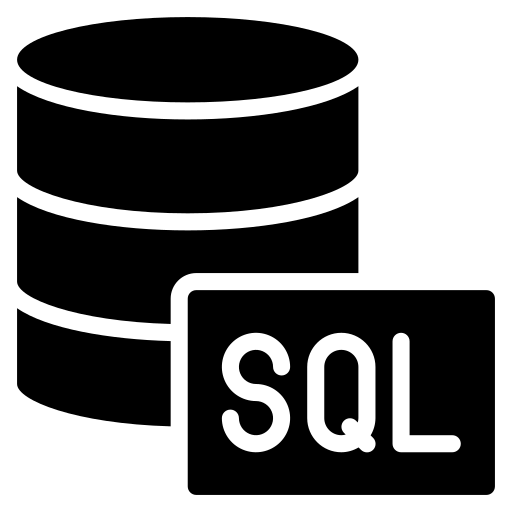


Hình . Dịch vụ cung cấp kho lưu trữ mã nguồn Git – GitHub

GitHub là một hệ thống quản lý dự án và phiên bản code, hoạt động giống như một mạng xã hội cho lập trình viên. Các lập trình viên có thể clone lại mã nguồn từ một repository và Github chính là một dịch vụ máy chủ repository công cộng, mỗi người có thể tạo tài khoản trên đó để tạo ra các kho chứa của riêng mình để có thể làm việc.

GitHub là một dịch vụ nổi tiếng cung cấp kho lưu trữ mã nguồn Git cho các dự án phần mềm. Github có đầy đủ những tính năng của Git, ngoài ra nó còn bổ sung những tính năng về social để các developer tương tác với nhau.

* + 1. Ngôn ngữ truy vấn SQL



Hình . Ngôn ngữ truy vấn SQL

SQL là viết tắt của Structured Query Language, nghĩa là ngôn ngữ truy vấn cơ sở dữ liệu. Có thể coi ngôn ngữ SQL là ngôn ngữ chung mà bất cứ hệ thống cơ sở dữ liệu quan hệ (RDBMS) nào cũng phải đáp ứng, điển hình như: Oracle Database, SQL Server, MySQL…

Bất kì công ty nào lớn cũng cần xây dựng một hệ thống để lưu trữ cơ sở dữ liệu. Mọi thứ trong cơ sở dữ liệu này sẽ được quy ra thành nhiều bảng, có mối quan hệ với nhau. SQL giúp quản lý hiệu quả và truy vấn cơ sở dữ liệu thông tin nhanh hơn, giúp bảo trì thông tin dễ dàng hơn.

* + 1. SQL Server



Hình . SQL Server

SQL server hay còn được gọi là Microsoft SQL Server, nó từ viết tắt của MS SQL Server. Đây chính là một loại phần mềm đã được phát triển bởi Microsoft và nó được sử dụng để có thể dễ dàng lưu trữ cho những dữ liệu dựa theo tiêu chuẩn RDBMS.

Từ đó, người ta sẽ lưu trữ dữ liệu dựa vào tiêu chuẩn RDBMS và nó cũng là một trong những hệ quản trị cơ sở dữ liệu dạng quan hệ đối tượng.

SQL Server có khả năng cung cấp đầy đủ các công cụ cho việc quản lý từ giao diện GUI đến sử dụng ngôn ngữ cho việc truy vấn SQL. Điểm mạnh của SQL điểm mạnh của nó là có nhiều nền tảng được kết hợp cùng như: ASP.NET, C# để xây dựng Winform cũng chính nó có khả năng hoạt động độc lập. Tuy nhiên, SQL Server thường đi kèm với việc thực hiện riêng các ngôn ngữ SQL, T-SQL,... Cụ thể như sau:

T-SQL là một trong những loại ngôn ngữ thuộc quyền sở hữu của Microsoft và được gọi với cái tên Transact-SQL. Nó thường cung cấp thêm rất nhiều cho các khả năng khai báo biến, thủ tục lưu trữ và xử lý ngoại lệ,...

SQL Server Management Studio là một loại công cụ giao diện chính cho máy chủ cơ sở của chính dữ liệu SQL, thông thường thì nó hỗ trợ cho cả môi trường 64 bit và 32 bit.

Và dùng công cụ tìm kiếm google để tìm kiếm tài liệu, tham khảo các quy trình nghiệp vụ.

# CHƯƠNG 2: CƠ SỞ LÝ THUYẾT

## 2.1. Giao thức TCP



Hình . Giao thức TCP

**Transmission Control Protocol (TCP)** là giao thức tiêu chuẩn trên Internet đảm bảo trao đổi thành công các gói dữ liệu giữa các thiết bị qua mạng. TCP là giao thức truyền tải cơ bản cho nhiều loại ứng dụng, bao gồm máy chủ web và trang web, ứng dụng email, FTP và các ứng dụng ngang hàng.

TCP hoạt động với giao thức Internet (IP) để chỉ định cách dữ liệu được trao đổi trực tuyến. IP chịu trách nhiệm gửi từng gói đến đích của nó, trong khi TCP đảm bảo rằng các byte được truyền theo thứ tự mà chúng được gửi mà không có lỗi hoặc thiếu sót nào. Hai giao thức kết hợp với nhau được gọi là TCP/IP.

TCP hoạt động theo tiến trình bắt tay 3 bước (3 way handshake). Tiến trình này hoạt động như sau:

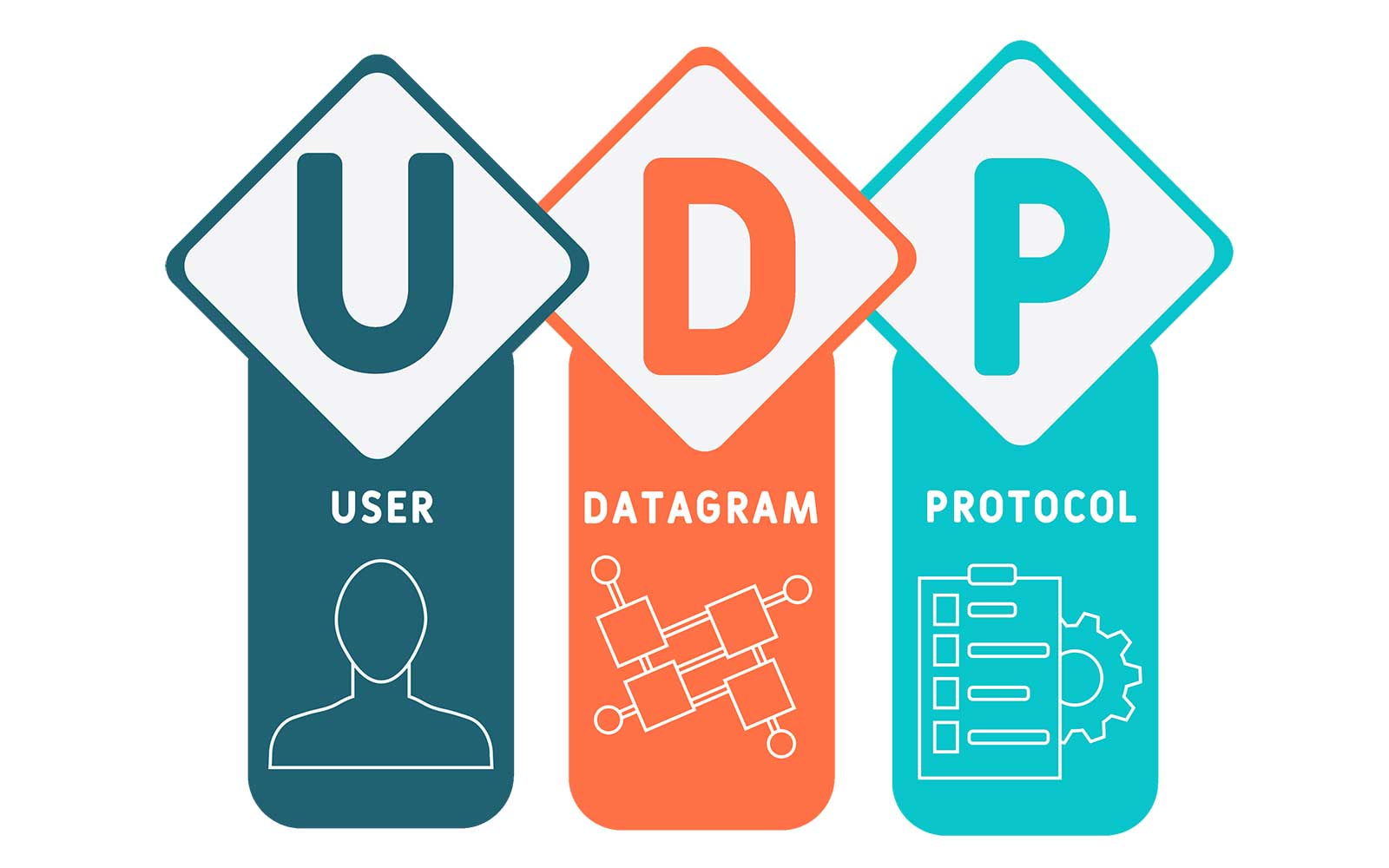
- Máy khách gửi cho máy chủ một gói SYN — một yêu cầu kết nối từ port nguồn của nó đến port đích đến của máy chủ.

- Máy chủ phản hồi bằng gói SYN/ACK, xác nhận việc nhận được yêu cầu kết nối.

- Máy khách nhận gói SYN/ACK và trả lời bằng gói ACK của chính nó.

- Sau khi kết nối được thiết lập, TCP hoạt động bằng cách chia nhỏ dữ liệu đã truyền thành các segment (phân đoạn), mỗi segment được đóng gói thành một gói dữ liệu và được gửi đến đích của nó.

## 2.2. Giao thức UDP



Hình . Giao thức UDP

**UDP (User Datagram Protocol)** – Giao thức dữ liệu người dùng là một giao thức giao tiếp thay thế cho TCP (Transmission Control Protocol) – giao thức kiểm soát đường truyền, được sử dụng chủ yếu để thiết lập các kết nối có độ trễ thấp và không chịu lỗi giữa các ứng dụng trên internet.

**Cách hoạt động của UDP**

Giao thức UDP hoạt động tương tự như TCP nhưng nó không cung cấp kiểm tra lỗi khi truyền gói tin. Khi một ứng dụng sử dụng UDP, các gói tin chỉ được gửi đến người nhận. Người gửi không đợi để đảm bảo người nhận nhận được gói tin hay không, mà nó tiếp tục gửi các gói tiếp theo. Nếu người nhận bỏ lỡ một vài gói tin UDP, gói tin đó bị mất vì người gửi sẽ không gửi lại chúng. Điều này có nghĩa là các thiết bị có thể giao tiếp nhanh hơn.

So sánh giao thức TCP và UDP

| **TCP** | **UDP** |
| --- | --- |
| Hướng kết nối | Hướng không kết nối |
| Độ tin cậy cao | Độ tin cậy thấp |
| Gửi dữ liệu dạng luồng byte | Gửi đi Datagram |
| Không cho phép mất gói tin | Cho phép mất gói tin |
| Đảm bảo việc truyền dữ liệu | Không đảm bảo việc truyền dữ liệu |
| Có sắp xếp thứ tự các gói tin | Không sắp xếp thứ tự các gói tin |
| Tốc độ truyền thấp hơn UDP | Tốc độ truyền cao |

## 2.3. Chương trình mã hóa Playfair

2.3.1. Tổng quan

Mật mã Playfair là kỹ thuật mã hóa đối xứng phổ biến nhất thuộc mật mã thay thế. Nó là một thủ tục mã hóa bao gồm nhiều hơn một ký tự cùng một lúc. Mật mã Playfair là một hệ mã hóa nhiều chữ, giảm bớt tương quan giữa văn bản mã hóa và nguyên bản bằng cách mã hóa đồng thời nhiều chữ cái của nguyên bản. Cơ chế hoạt động như sau: sử dụng một ma trận chữ cái 5x5 trên cơ sở một từ khóa: điền các chữ cái của từ khóa (bỏ các chữ trùng), điền những vị trí còn lại của ma trận với các chữ cái khác của bảng chữ cái; I, J có thể ở trên cùng một ô của ma trận. Playfair cipher là một thuật toán mã hóa để mã hóa hoặc mã hóa một tin nhắn. Nó cũng giống như một mật mã truyền thống. Sự khác biệt duy nhất là nó mã hóa một **digraph** (một cặp hai chữ cái) thay vì một chữ cái duy nhất.

Ban đầu, nó tạo ra một bảng khóa của ma trận 5 \* 5. Ma trận chứa các bảng chữ cái đóng vai trò là khóa để mã hóa bản rõ. Lưu ý rằng không nên lặp lại bất kỳ bảng chữ cái nào. Một điểm khác cần lưu ý rằng có 26 bảng chữ cái và chúng ta chỉ có 25 khối để đặt một chữ cái bên trong nó. Do đó, một chữ cái bị thừa, một chữ cái sẽ bị bỏ qua (thường là J) khỏi ma trận. Tuy nhiên, bản rõ chứa J, sau đó J được thay thế bằng I. Theo đó, nó có nghĩa là coi I và J là cùng một chữ cái.

2.3.2. Ưu điểm của Playfair Cipher

* Đa dạng bản mã nếu chúng ta xem xét kỹ thuật toán, chúng ta có thể nhận thấy ở mọi Giai đoạn, chúng ta đang nhận được các bản mã đa dạng, do đó sẽ gặp nhiều rắc rối hơn đối với nhà phân tích mật mã.
* Tấn công vũ phu không ảnh hưởng đến nó.
* Cryptanalyze (quá trình giải mã mật mã mà không cần biết khóa) là không thể.
* Khắc phục hạn chế của mật mã vuông Playfair đơn giản.
* Dễ dàng thực hiện thay thế.

2.3.3. Nhược điểm của Playfair Cipher

* Chỉ có 25 bảng chữ cái được hỗ trợ.
* Nó không hỗ trợ các ký tự số.
* Chỉ hỗ trợ chữ hoa và chữ thường. Việc sử dụng các ký tự đặc biệt (chẳng hạn như khoảng trống, dòng mới, dấu chấm câu, v.v.) bị cấm.
* Nó không hỗ trợ các ngôn ngữ khác, ngoại trừ tiếng Anh.
* Mã hóa các tệp phương tiện cũng không được hỗ trợ.

2.3.4. Quy tắc mã hóa Playfair

Mã hóa 2 chữ cái một lúc

Nếu 2 chữ giống nhau, tách ra bởi 1 chữ điền thêm thường là X hoặc Q

Ví dụ: EE sẽ dược thay bởi EX

Nếu 2 chữ nằm cùng hàng, thay bởi các chữ bên phải

Ví dụ: EF sẽ thay bằng FG

Nếu 2 chữ nằm cùng cột, thay bởi các chữ bên dưới

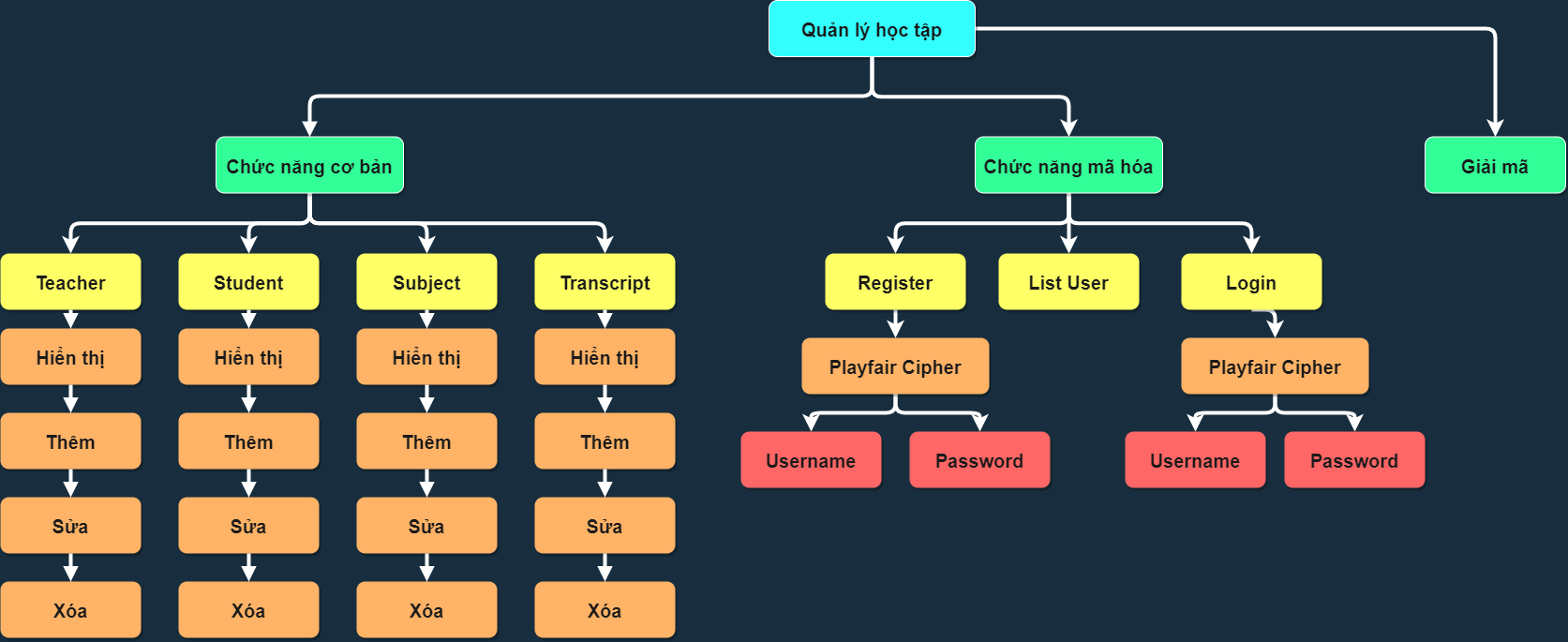
Ví dụ: OF thay bằng HP

Các trường hợp khác, mỗi chữ cái được thay bởi chữ cái khác cùng hàng, trên cột chữ cái cùng cặp

Ví dụ: ET sẽ thay bằng KL

# CHƯƠNG 3: CHƯƠNG TRÌNH & ĐÁNH GIÁ

## 3.1. Sơ đồ chức năng



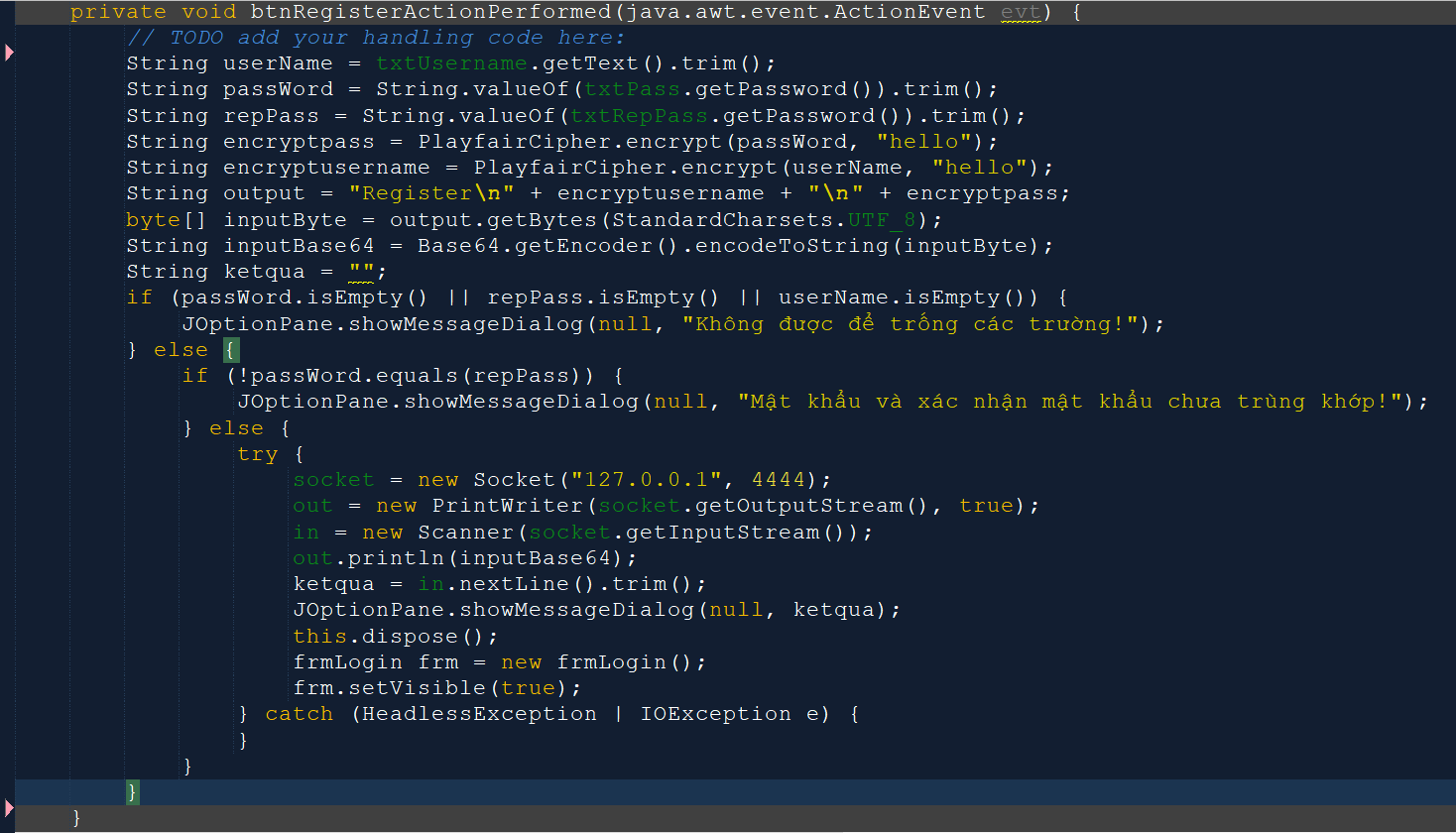
Hình . Sơ đồ chức năng

## 3.2. Background



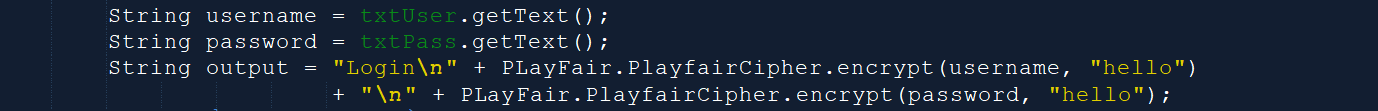
Hình . Background

3.2.1. Mã hóa đăng ký



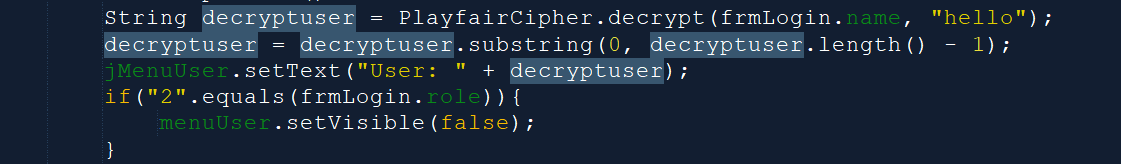
Hình . Mã hóa đăng ký

3.2.2. Mã hóa thông tin nhập vào khi đăng nhập để trùng khớp



Hình . Mã hóa đăng nhập

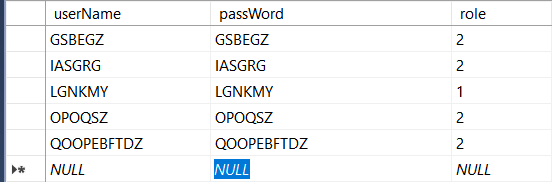
3.2.3. Giải mã tài khoản để hiện lên form chính



Hình . Giải mã tài khoản

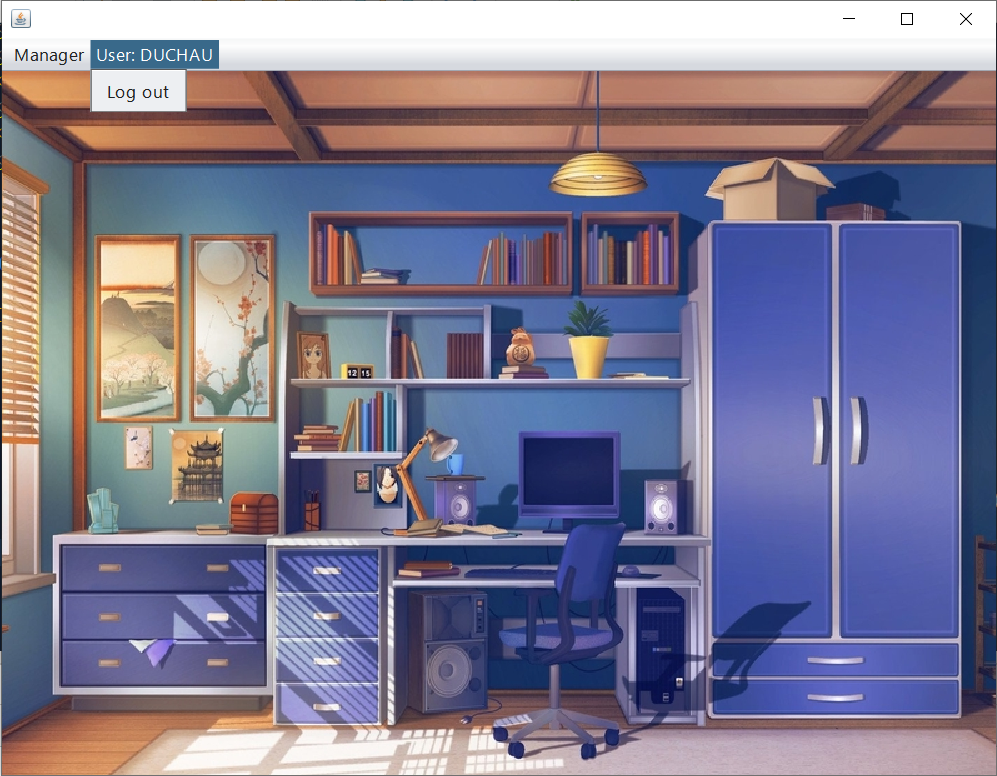
## 3.3. Kết luận và đánh giá

3.3.1. Cơ sở dữ liệu sau khi mã hóa đăng ký



Hình . Cơ sở dữ liệu sau khi mã hóa

3.3.2. Sau khi giải mã hiển thị lên form chính



Hình . Giao diện form chính

3.3.3. Đánh giá

Các chức năng hoạt động bình thường, chức năng mã hóa hoạt động tốt, mã hóa đầy đủ tài khoản và mật khẩu đảm bảo độ bảo mật cao.

Mã khóa Playfair có 26x26=676 cặp chữ cái, do đó các cặp chữ cái này ít bị chênh lệch về tần suất hơn so với sự chênh lệnh tần suất của từng chữ cái. Ngoài ra số lượng các cặp chữ cái nhiều hơn cũng làm cho việc phá mã tần suất khó khăn hơn. Đây chính là lý do mà người ta tin rằng mã hóa Playfair không thể bị phá và được quân đội Anh sử dụng trong chiến tranh thế giới lần thứ nhất.

# CHƯƠNG 4: HƯỚNG PHÁT TRIỂN, MẶT TÍCH CỰC

## 4.1. Hướng phát triển

Do Playfair Cipher là hệ mật mã cổ điển nên việc sử dụng và viết thuật toán khá dài và khó sử dụng trong thời hiện nay để cạnh tranh với các hệ mật mã khác.

Những hệ mật mã cổ điển này tuy ngày nay tuy ít được sử dụng, nhưng chúng thể hiện những nguyên lý cơ bản được ứng dụng trong mật mã hiện đại. Dựa trên nền tảng đó, chúng ta sẽ tìm hiểu về mã hóa đối xứng và mã hóa bất đối xứng, chúng đóng vai trò quan trọng trong mật mã hiện đại. Bên cạnh đó chúng ta cũng sẽ tìm hiểu về hàm Hash, cũng là một công cụ bảo mật quan trọng mà có nhiều ứng dụng lý thú, trong đó có chữ ký điện tử.

## 4.2. Mặt tích cực

Do là mã hóa cổ điển nên đòi hỏi sự tìm hiểu kỹ giúp phát triển tư duy mã hóa của người dùng cũng như lấy đó làm căn bản cho sự phát triển những hệ mật mã khác cao cấp, tối ưu, an toàn hơn cũng như tối ưu thuật toán giúp chương trình chạy nhanh hơn.

# Tài liệu tham khảo

<http://dulieu.tailieuhoctap.vn/books/cong-nghe-thong-tin/an-ninh-bao-mat/file_goc_777324.pdf>

Tài liệu Lập trình mạng máy tính Trường Đại học Công nghệ TP. HCM(HUTECH