BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP. HCM

PHẠM PHI HÙNG

NGHIÊN CỨU MÃ HÓA KHÓA BÍ MẬT SỬ DỤNG GIẢI THUẬT DI TRUYỀN VÀ ỨNG DỤNG BẢO MẬT NGÂN HÀNG ĐỀ THI

LUẬN VĂN THẠC SĨ

Chuyên ngành: Công Nghệ Thông Tin

Mã số ngành: 60480201

TP. Hồ Chí Minh, Tháng 8 Năm 2016

BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP. HCM

PHẠM PHI HÙNG

NGHIÊN CỨU MÃ HÓA KHÓA BÍ MẬT SỬ DỤNG GIẢI THUẬT DI TRUYỀN VÀ ỨNG DỤNG BẢO MẬT NGÂN HÀNG ĐỀ THI

LUẬN VĂN THẠC SĨ

Chuyên ngành: Công Nghệ Thông Tin

Mã số ngành: 60480201

CÁN BỘ HƯỚNG DẪN KHOA HỌC: TS LƯ NHẬT VINH

TP. Hồ Chí Minh, Tháng 8 Năm 2016

CÔNG TRÌNH ĐƯỢC HOÀN THÀNH TẠI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP. HCM

Cán bộ hướng dẫn khoa học: TS Lư Nhật Vinh
(Ghi rõ họ, tên, học hàm, học vị và chữ ký)

TS. Lư Nhật Vinh

Luận văn Thạc sĩ được bảo vệ tại Trường Đại học Công nghệ TP. HCM ngày 10 tháng 9 năm 2016

Thành phần Hội đồng đánh giá Luận văn Thạc sĩ gồm:

TT	Họ và tên	Chức danh Hội đồng
1	Ts.Nguyễn Thị Thúy Loan	Chủ tịch
2	Ts.Trần Đức Khánh	Phản biện 1
3	Ts.Phạm Thị Thiết	Phản biện 2
4	Ts.Cao Tùng Anh	Ủy viên
5	Ts.Văn Thiên Hoàng	Ủy viên, Thư ký

Xác nhận của Chủ tịch Hội đồng đánh giá Luận sau khi Luận văn đã được sửa chữa (nếu có).

Chủ tịch Hội đồng đánh giá LV

TRƯỜNG ĐH CÔNG NGHỆ TP. HCM

PHÒNG QLKH – ĐTSĐH

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

Độc lập – Tự do – Hạnh phúc

TP.HCM, Ngày……tháng……năm 2016

NHIỆM VỤ LUẬN VĂN THẠC SĨ

Họ tên học viên: PHẠM PHI HÙNG Giới tính: Nam

Ngày, tháng, năm sinh: 20-07-1990 Nơi sinh: TP.HCM

Chuyên ngành: Công nghệ thông tin MSHV: 1441860047

I.- Tên đề tài:

NGHIÊN CỨU MÃ HÓA KHÓA BÍ MẬT SỬ DỤNG GIẢI THUẬT DI TRUYỀN VÀ ỨNG DỤNG BẢO MẬT NGÂN HÀNG ĐỀ THI

II.- Nhiệm vụ và nội dung:

- Nghiên cứu và tìm hiểu về Giải thuật di truyền.
- Tìm hiểu về các thuật toán trao đổi khóa, mã hóa, giải mã bằng khóa bí mật.
- Từ đó xây dựng chương trình bảo mật ngân hàng đề thi.

III.- Ngày giao nhiệm vụ: *23/1/2016*

IV.- Ngày hoàn thành nhiệm vụ: 20/7/2016

V.- Cán bộ hướng dẫn: TS LƯ NHẬT VINH

CÁN BỘ HƯỚNG DẪN
(Họ tên và chữ ký)

TS Lư Nhật Vinh

KHOA QUẢN LÝ CHUYÊN NGÀNH
(Họ tên và chữ ký)

LỜI CAM ĐOAN

Tôi xin cam đoan đây là công trình nghiên cứu của riêng tôi. Các số liệu, kết quả nêu trong Luận văn là trung thực và chưa từng được ai công bố trong bất kỳ công trình nào khác.

Tôi xin cam đoan rằng mọi sự giúp đỡ cho việc thực hiện Luận văn này đã được cảm ơn và các thông tin trích dẫn trong Luận văn đã được chỉ rõ nguồn gốc.

Học viên thực hiện Luận văn

(Ký và ghi rõ họ tên)

Phạm Phi Hùng

LỜI CẢM ƠN

Trước tiên, tôi xin được gửi lời cảm ơn đến Ban Giám Hiệu, toàn thể cán bộ nhân viên, giảng viên trường Đại Học HUTECH, Ban lãnh đạo Phòng Quản Lý Khoa Học và Đào Tạo Sau Đại Học, khoa Công Nghệ Thông Tin đã tạo điều kiện thuận lợi cho chúng tôi học tập và nghiên cứu trong suốt học trình cao học. Xin được gửi lời cảm ơn đến tất cả quý thầy cô đã giảng dạy trong chương trình Đào tạo thạc sĩ chuyên ngành Công nghệ thông tin, khóa 2, lớp 14SCT21 - Trường Đại học Công Nghệ TPHCM, những người đã truyền đạt cho tôi những kiến thức hữu ích để làm cơ sở cho tôi thực hiện tốt luận văn này.

Với lòng kính trọng và biết ơn, tôi xin bày tỏ lời cảm ơn đến TS Lư Nhật Vinh đã tận tình hướng dẫn cho tôi trong thời gian thực hiện luận văn, những gì thầy đã hướng dẫn, chỉ bảo đã cho tôi nhiều kinh nghiệm trong thời gian thực hiện luận văn.

Sau cùng tôi xin gửi lời biết ơn sâu sắc đến bạn bè, gia đình, các anh chị trong tập thể lớp 14SCT21 đã luôn tạo điều kiện tốt nhất cho tôi trong suốt quá trình học cũng như thực hiện luận văn.

Do thời gian có hạn và kinh nghiệm nghiên cứu khoa học chưa nhiều nên luận văn còn nhiều thiếu sót, rất mong nhận được ý kiến góp ý của Thầy/Cô và các anh chị học viên.

TÓM TẮT

Mật mã cung cấp các dịch vụ cơ bản như là khả năng gửi thông tin giữa các thành viên tham gia, nhưng phải đảm bảo an toàn có thể ngăn chặn người khác đọc nó. Để bảo vệ nội dung chống lại một kẻ tấn công, người gửi mã hóa thông điệp của mình bằng cách sử dụng một thuật toán mã hóa đối xứng hoặc bất đối xứng. Nhưng người nhận cần phải biết được khóa của người gửi để có thể giải mã và đọc được thông điệp đó, vấn đề này thì ta có thể đạt được bằng cách sử dụng một giao thức trao đổi khóa. Diffie-Hellman là giao thức trao đổi khóa được giới thiệu, và là giao thức trao đổi khóa phổ biến.

Ngày nay với sự phát triển như vũ bão của xã hội nói chung cũng như của nền giáo dục nước nhà nói riêng, việc bảo mật đề thi để tránh bị lọt vào tay kẻ xấu để trục lợi là rất đáng quan tâm.

Với những lý do trên tôi chọn đề tài "Nghiên cứu mã hóa khóa bí mật sử dụng giải thuật di truyền và ứng dụng bảo mật ngân hàng đề thi". Nghiên cứu này với mục đích bảo mật hơn trong quá trình mã hóa, chọn lọc đề thi để đảm bảo đề thi được an toàn trước ngày công bố.

ABSTRACT

Cryptography is the art of mangling information into apparent unintelligibility in a manner allowing a secret method of unmangling. The basic service provided by cryptography is the ability to send information between participants in a way that prevents others from reading it. In order to protect the content against an opponent, sender encrypts her message using a fast symmetric encryption algorithm. But receiver needs to know sender's key for reading her message, one can achieve this by using a key-exchange protocol. Diffie Hellman key exchange protocol was introduced for key exchange protocol.

Nowaday, with the development of society by storm in general and of education in particular country, the security of examination questions to avoid being caught in the wrong hands in order to profit as much concern.

From all reasons above I would like to choose the topic “Research secret key encryption uses Genetic algorithms and construction of bank security application exam”. This research with the aim of better privacy during exams encryption to ensure safe exam before the date of publication.

MỤC LỤC

DANH MỤC CÁC TỪ VIẾT TẮT

Kí hiệu		
GAs	Genetic Algorithm	Giải thuật di truyền
AES	Advanced Encryption Standard	Tiêu chuẩn mã hóa tiên tiến
DES	Data Encryption Standard	Tiêu chuẩn mã hoá dữ liệu
GAs	Genetic Algorithm	Giải thuật di truyền
AES	Advanced Encryption Standard	Tiêu chuẩn mã hóa tiên tiến
RSA		Tên của thuật toán lấy từ 3 chữ cái của 3 tác giả Ron Rivest, Adi Shamir và Len Adleman
NIST	National Institute of Standards and Technology	Viện Tiêu chuẩn và Kỹ thuật Quốc gia (Hoa Kỳ)
SSL	Secure Sockets Layer	Tiêu chuẩn của công nghệ bảo mật, truyền thông mã hoá giữa máy chủ Web server và trình duyệt (browser)
PGP	Pretty Good Privacy	Bảo mật rất mạnh

DANH MỤC CÁC BẢNG

DANH MỤC CÁC HÌNH

PHẦN MỞ ĐẦU

1. Lý do chọn đề tài

Hiện nay sự lệ thuộc ngày càng tăng nhu cầu xử lý thông tin và truyền tải trên hệ thống mạng kết nối phát triển mạnh đã làm tăng theo nhu cầu về an ninh thông tin. Mã hóa theo tập hợp các kỹ thuật toán học để cung cấp, bảo mật thông tin, bảo mật toàn vẹn dữ liệu, xác thực. Mã hóa và giải mã là các khái niệm chính của mật mã.

Trong khi gửi một dữ liệu đến người nhận, sự riêng tư của dữ liệu được bảo vệ bởi việc mã hóa tức là chuyển đổi dữ liệu thành một dạng không thể đọc được bằng phương pháp thường. Về phía người nhận sẽ được giải mã về hình thức ban đầu của nó.

Khi công nghệ thông tin và các ngành điện tử phát triển như vũ bão thì mọi hoạt động của xã hội đều có thể số hóa. Số hóa các công việc không chỉ đảm bảo hiệu quả công việc mà còn an toàn hơn rất nhiều so với những hoạt động do con người thực hiện. Một hoạt động to lớn và quan trọng hàng đầu trong xã hội hiện nay là làm thế nào để đảm bảo được tính an toàn bí mật cho các đề thi trước khi được công bố. Các vấn đề nói trên phần nào còn mới mẻ với nước ta, xuất phát từ đó tôi đã lựa chọn việc "Nghiên cứu mã hóa khóa bí mật sử dụng giải thuật di truyền và ứng dụng bảo mật ngân hàng đề thi" là chủ đề chính cho luận văn.

2. Tính cấp thiết của đề tài

Thông tin luôn là một tài sản vô giá của tổ chức, doanh nghiệp và cần được bảo vệ bằng mọi giá. Tuy nhiên, với những đòi hỏi ngày càng gắt gao của môi trường năng động chia sẻ thông tin qua Internet, việc bảo vệ thông tin trở nên ngày càng quan trọng và khó khăn hơn bao giờ hết. Hầu hết các tổ chức, doanh nghiệp ngày nay đều sử dụng các hệ quản trị cơ sở dữ liệu (CSDL) để lưu trữ tập trung tất cả các thông tin quý giá của mình. Hiển nhiên hệ thống sẽ là tiêu điểm tấn công của những kẻ xấu. Ở mức độ nhẹ, các cuộc tấn công sẽ làm hệ thống CSDL bị hỏng hóc, hoạt động không ổn định, mất mát dữ liệu làm cho các giao dịch hàng ngày của tổ chức, doanh nghiệp bị đình trệ. Nghiêm trọng hơn, các thông tin sống còn của tổ chức, doanh

nghiệp bị tiết lộ (như đề thi, thông tin sinh viên, học sinh, các thông tin về khách hàng, nhà cung cấp, tài chính, mức lương nhân viên) và được đem bán cho các những kẻ có ý đồ xấu. Có thể nói là thiệt hại của việc thông tin bị rò rỉ là vô cùng kinh khủng. Đó sẽ là một đòn chí mạng đối với uy tín của tổ chức, doanh nghiệp cũng như uy tín của toàn xã hội.

3. Mục tiêu, nội dung và phương pháp nghiên cứu

- *Mục tiêu tổng quát:*

+ Đảm bảo sự an toàn trong việc tạo và sử dụng khóa bí mật.

+ Ứng dụng bảo mật ngân hàng đề thi.

- *Mục tiêu cụ thể:*

+ Xây dựng được chương trình tạo khóa bí mật ứng dụng giải thuật di truyền để bảo mật ngân hàng đề thi và bước đầu cho phép thi online.

- *Phương pháp nghiên cứu lý thuyết*

+ Tiến hành thu thập và nghiên cứu các tài liệu liên quan đến đề tài.

+ Nghiên cứu Thuật toán tạo khóa bí mật, Giải thuật di truyền.

+ Nghiên cứu ứng dụng của Giải thuật di truyền vào việc mã hóa văn bản bằng khóa bí mật.

- *Phương pháp nghiên cứu thực nghiệm:*

+ Nghiên cứu cách xây dựng chương trình mã hóa các loại văn bản, tài liệu dựa trên việc ứng dụng mã hóa khóa bí mật kết hợp với Giải thuật di truyền.

+ Ngôn ngữ sử dụng: C# trong bộ Visual studio 2013.

+ Thử nghiệm trong nội bộ Trường THCS Nguyễn Đức Ứng.

+ Đánh giá kết quả đạt được.

CHƯƠNG 1
TỔNG QUAN VỀ GIẢI THUẬT DI TRUYỀN VÀ THUẬT TOÁN TẠO KHÓA BÍ MẬT

CHƯƠNG 2
ỨNG DỤNG MÃ HÓA KHÓA BÍ MẬT SỬ DỤNG GIẢI THUẬT DI TRUYỀN

2.1 Tổng quan

Mật mã học là một kỹ thuật cơ bản để bảo vệ thông tin. Trong bài nghiên cứu này, tôi sử dụng một thuật toán di truyền (GAs) dựa trên hệ thống mật mã khóa đối xứng để mã hóa và giải mã. Ở đây, các văn bản đơn giản và người dùng nhập vào (key) được chuyển thành ma trận văn bản và ma trận trọng tương ứng. Một ma trận phụ được tạo ra bằng cách thêm vào ma trận văn bản và ma trận chính. Một chức năng thay thế tuyến tính được áp dụng trên các ma trận phụ để sản xuất các thuật toán mã hóa trung gian. Sau đó, các chức năng GAs (chéo và đột biến) được áp dụng trên các thuật toán mã hóa trung gian để tạo ra các văn bản mật mã. Các thuật toán đề xuất có hai bước cơ bản đó là: ***chéo và đột biến***.

2.2 Phát biểu bài toán

Sự phụ thuộc ngày càng tăng trên các máy tính để xử lý thông tin và truyền tải nó trên hệ thống kết nối hầu như đã làm tăng nhu cầu về an ninh. Mã hoá theo một tập hợp các kỹ thuật toán học để cung cấp an ninh thông tin, bảo mật, toàn vẹn dữ liệu, xác thực. Mã hóa và giải mã là những khái niệm chính của mật mã [5].

Trong khi gửi một dữ liệu từ người gửi đến người nhận, sự riêng tư của dữ liệu được bảo vệ bởi mã hóa nó (nghĩa là) chuyển đổi dữ liệu trong một số hình thức không đọc được bằng cách thông thường. Về phía người nhận, dữ liệu có thể được

giải mã đến hình thức ban đầu của nó. Quá trình mã hóa và giải mã yêu cầu một khoá mật mã và khóa giải mã.

Mã hóa và giải mã có thể sử dụng các khóa giống nhau được gọi là khóa đối xứng / mã hóa khóa bí mật. Có hai loại kỹ thuật mã hóa cụ thể là thay thế và chuyển vị. Thay thế mỗi ký hiệu rõ với biểu tượng khác, các kỹ thuật chuyển vị biểu tượng trong bản rõ để tạo ra các văn bản mật mã.

Các thuật toán di truyền được phát triển dựa trên thuật toán tiến hóa về các khái niệm về chọn lọc tự nhiên. Thuật toán di truyền đã được chứng minh là đáng tin cậy và mạnh mẽ, tối ưu hóa trong một loạt các ứng dụng. Nó có thể được áp dụng cho cả văn bản và hình ảnh. Thuật toán di truyền là an toàn vì nó không sử dụng các số tự nhiên trực tiếp. Các kết quả thu được để tạo ra các khóa sử dụng thuật toán di truyền nên được tốt về hệ số tương quan. Nói chung thuật toán di truyền có hai chức năng cơ bản: *chéo và đột biến.*

Trong bài nghiên cứu này tôi sử dụng chức năng chéo và đột biến để áp dụng cho việc mã hóa và giải mã. Trong chức năng chéo, nhiễm sắc thể con được tạo ra bằng cách tham gia nhiều hơn một nhiễm sắc thể cha mẹ. Có rất nhiều loại kỹ thuật chéo như đơn điểm, hai điểm chéo, chéo đồng nhất và chéo cha mẹ.

Trong bài nghiên cứu này tôi sử dụng kỹ thuật hai điểm chéo. Trong kỹ thuật hai điểm chéo, hai điểm ngẫu nhiên được chọn từ hai cha mẹ và các bits giữa hai điểm được trao đổi để sản xuất các nhiễm sắc thể con.

0	**1**	**0**	**0**	**1**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**1**

1	**0**	**0**	**0**	**1**	**1**	**0**	**1**	**1**	**1**	**0**	**0**	**1**	**1**	**0**	**1**

Hình 2.1: Chéo hai điểm (trước khi chéo)

0	**1**	**0**	**0**	**1**	**1**	**0**	**1**	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**1**

1	**0**	**0**	**0**	**1**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**1**	**1**	**0**	**1**

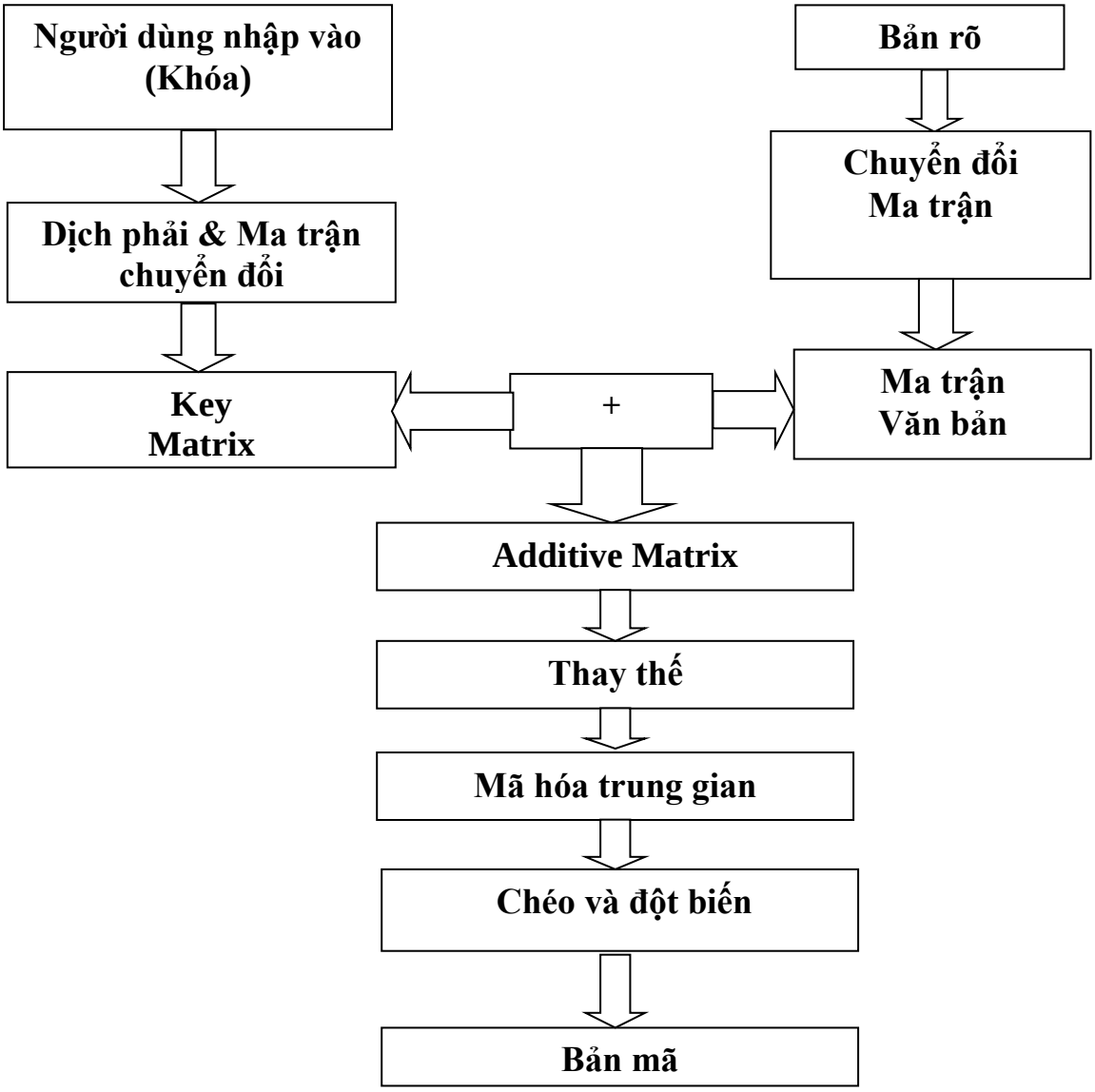
Hình 2.2: Chéo hai điểm (sau khi chéo)

Sau kỹ thuật chéo, chức năng đột biến được áp dụng. Có rất nhiều loại đột biến như lật bits, ranh giới đột biến, đột biến không đồng nhất, đột biến đồng nhất và đột biến Gaussian. Trong bài nghiên cứu này tôi sử dụng các kỹ thuật lật bits.

Nó liên quan đến việc lựa chọn một hoặc nhiều bits của nhiễm sắc thể và đột biến thành bù của nó có nghĩa là '0' sẽ biến đổi thành "1" và ngược lại.

2.2.1 Các thuật toán đề xuất

- Ma trận bổ sung (Matrix Addition)
- Thay thế (Substitution)
- Chéo Gen và đột biến (Genetic crossover and mutation)



Hình 2.3: Sơ đồ mã hóa từng bước

2.2.2 Tiến trình mã hóa

2.2.2.1 Khóa Thuật toán di truyền

- Chọn kích thước khối *n*.

- Chia key cho kích thước *n* và thêm các ký tự z vào cuối nếu nó không bằng *n*.

- Người dùng nhập vào ký tự bảng mã ASCII và thực hiện chuyển đổi trên hệ nhị phân của nó để có được ma trận mà trật tự là *nxn*.

2.2.2.2 Thuật toán thay thế

- Các thuật toán thay thế có dạng $C(x) = (ax + b)MOD\ 26$, ở đây *x* là tương đương số lượng của 26 chữ cái trong bảng chữ cái và *a,b* là số nguyên.

- Quá trình giải mã có dạng $C^{-1}(y) = a^{-1}\ (y - b)MOD\ 26$, ở đây *y* được xét là x tức là: $y = C(x) = (ax + b)MODE\ 26$. Chúng ta xem xét bảng chuyển đổi sau đây cho bảng chữ cái tiếng anh để thực hiện thay thế.

Bảng 2.1: Bảng chuyển đổi

0	1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M
13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Ví dụ: ta sẽ mã hóa từng bước một sử dụng Thuật toán Thay thế để áp dụng cho từ “Beach” với key mã hóa là (3,1).

+ *Bước 1*: Sử dụng bảng trên, ta có thể thấy các ký tự trong từ “Beach” lần lượt xuất hiên trong bảng với các số: 1 4 0 2 7.

+ *Bước 2*: Nhân mỗi số tìm được trên bước 1 với key mã hóa (là 3 trong ví dụ này) ta được: 3 12 0 6 21.

+ *Bước 3*: Cộng thêm số thứ hai trong key mã hóa (là 1 trong ví dụ này) với kết quả tìm được ở bước 2 ta được: 4 13 1 7 22.

+ *Bước 4*: Lấy kết quả tìm được ở bước 3 dò lên trên bảng chuyển đổi ta được chuỗi đã mã hóa là: ENBHW.

2.2.2.3 Thuật toán mã hóa

+ Bước 1: Lấy bản rõ và chuyển vào ma trận văn bản

+ Bước 2: Tạo 1 ma trận phụ bằng cách thêm khóa ma trận vào văn bản rõ

+ Bước 3: Áp dụng Thuật toán Thay thế trên ma trận vừa tạo để tạo ra mã hóa trung gian.

+ Bước 4: Một hàm tổng quát (Chéo, đột biến) được áp dụng trên các thuật toán mã hóa trung gian để tạo ra các bản mã.

+ Bước 5: Các văn bản mật mã được người dùng nhập vào khóa, kích thước, khóa thay thế, và chéo 2 điểm được gửi đến người nhận để lấy lại bản rõ.

2.2.2.4 Tạo khóa ma trận

- Người dùng sẽ nhập vào chuỗi "NETWORK".

- Đặt Size n=3; Chuyển chuỗi sang mã ASCII với size là n ta được:

78 69 84 87 79 82 75 90 90

- Giờ ta chuyển từ ASCII sang mã nhị phân ta được:

01001110 01000101 01010100 01010111 01001111 01010010 01001011 01011010 01011010

Dịch chuyển phải 2bits trên chuỗi nhị phân

00010011 00010001 00010101 00010101 00010011 00010100 00010010 00010110 00010110

Ma trận có được là:

19	17	21
21	19	20
18	22	22

2.2.2.5 Tạo ma trận văn bản

Đặt ***plain text*** là SECURITY.

Ma trận tương đương sau khi chuyển đổi các văn bản tương đương vào block size *n* như bên dưới:

83	69	67

85	82	73
84	89	90

2.2.2.6 Tạo ma trận phụ

Thêm các key ma trận và ma trận văn bản để tạo ma trận phụ.

102	86	88
106	101	93
102	111	112

2.2.2.7 *Thay thế*

Áp dụng các thuật toán thay thế vào các ma trận phụ để có được mật mã trung gian.

O G U Q H D 0 Z G

Mã ASCII tương đương cho các thuật toán mã hóa trung gian

79 71 85 81 72 68 79 90 71

2.2.2.8 Chéo Gen và đột biến

Chuyển dãy sang hệ nhị phân:

01001111 01000111 01010101 01010001 01001000 01000100 01001111 01011010 01000111

Chia chuỗi nhị phân làm 2 phần:

010011110100011101010101010100010100

100001000100010011110101101001000111

Áp dụng chéo hai điểm (như hình 1)

0100111**01000100**0101010101010100010100

1000010**01110100**1111010110100100011 1

Áp dụng ***Chức năng Đột biến:*** (đổi 0 thành 1 và ngược lại)

10110000 10111011 10101010 10101110 1011

01111011 10111000 00001010 01011011 1000

Chia 8 bit và chuyển về hệ HEX → Bước cuối cùng

B0, BB, AA, AE, B7, 5B, 80, A5, B8

Ta có văn bản mật mã là {B0, BB, AA, AE, B7, 5B, 80, A5, B8} kèm theo là chuỗi NETWORK372916 được gửi cho người nhận để giải mã. Từ NETWORK là người dùng nhập vào, 3 là block size, 7 & 2 là số nguyên tố sử dụng trong thuật toán Thay Thế, 9 & 16 là hai điểm chéo.

2.2.2.9 Độ phức tạp của thuật toán

Các hoạt động chính của thuật toán đề xuất là con trỏ phải, cộng ma trận, hoạt động theo modulo và các chức năng di truyền. Trong số các hoạt động quan trọng của chức năng modulo tăng trưởng có thứ tự lớn hơn. Nó được dự kiến và được phân tích rằng, nếu dữ liệu được mã hóa bằng các phương pháp đề xuất để tăng trưởng thì độ phức tạp của thuật toán ở điều kiện tốt nhất sẽ là **O (n^2).**

Tốc độ mã hóa và giải mã trong thực tế: Do thời gian thực hiện luận văn có hạn nên việc tính toán đo đạc thời gian mã hóa và giải mã một cách chính xác nhất vẫn chưa được thực hiện một cách triệt để. Cần thêm nhiều thời gian trong thực nghiệm và CSDL lớn hơn mới có thể tính toán một cách chính xác nhất.

Ưu điểm:

Các thuật toán đề xuất thực hiện trong bài viết này là đơn giản và dễ thực hiện trong hệ thống mật mã. Quá trình tạo khóa và thuật toán mật mã trung gian cung cấp bảo mật tốt để truyền dữ liệu. Ở đây thuật toán đối xứng, thay thế key được sử dụng để đảm bảo bảo mật trong mạng, thực hiện với sự giúp đỡ của các chức năng di truyền để cung cấp tăng cường tính bảo mật.

Ngoài ra, thay cho một kỹ thuật thay thế tuyến tính, một khả năng sử dụng kỹ thuật thay thế có thể được sử dụng trong các thuật toán thay thế nhằm đạt được mức độ tốt về an ninh.

2.3 Các nghiên cứu liên quan

Công việc đề xuất sử dụng thuật toán di truyền trong lĩnh vực mã hóa khóa bí mật là một thành phần thiết yếu trong an ninh thông tin ngày nay. Nỗ lực khám phá ra việc tạo khóa cho mã hóa khóa bí mật khai thác thuật toán di truyền để làm cho việc mã hóa khóa bí mật an toàn hơn giống như là DES và RSA.

Để có được ý tưởng trong lĩnh vực này, các bài nghiên cứu trước đó đã được nghiên cứu và phân tích.

Goyat trình bày phương pháp, các văn bản thô được chuyển đổi thành văn bản mật mã sử dụng XOR bản rõ nhị phân với một chìa khóa nhị phân. Văn bản mã hóa được chuyển qua một kênh và khi người nhận nhận được các văn bản mật mã và XORs nó với cùng khóa đó sẽ nhận được bản rõ [2].

Delman tạo ra một số so sánh hiệu năng giữa các phương pháp phân tích mật mã truyền thống và phương pháp sử dụng thuật toán di truyền, để xác định tính phù hợp của các phương mã hóa truyền thống và phương pháp sử dụng thuật toán di truyền trong lĩnh vực giải mã [3].

Sindhuja K, Pramela Devi S và các đồng sự đã trình bày phương pháp tạo khóa bí mật ứng dụng các kỹ thuật của giải thuật di truyền điển hình như đột biến gen nhằm tăng cường tính bảo mật cho khóa bí mật được tạo ra [5].

Công bố dữ liệu bảo mật tính riêng tư (PPDP): Ý tưởng là dữ liệu đó được công bố bởi một chủ sở hữu vì lợi ích chung cho phép các nhà phân tích khai thác các mô hình từ đó. Dữ liệu được công bố với sự hạn chế, sự khái quát hóa, sự biến dạng hoặc sự phân tách thích hợp sao cho sự bí mật cá nhân không bị ảnh hưởng. Rõ ràng, cách tiếp cận này có thể bảo vệ bí mật cá nhân nhưng không phải là bí mật của doanh nghiệp, nghĩa là, sự bí mật của cơ sở dữ liệu giao dịch và các luật kết hợp được khai thác [7].

2.4 Hạn chế của những nghiên cứu trước và những vấn đề được tiếp tục nghiên cứu:

Hạn chế của các thuật toán khóa đối xứng bắt nguồn từ yêu cầu về sự phân hưởng chìa khóa bí mật, mỗi bên phải có một bản sao của chìa khóa. Do khả năng các chìa khóa có thể bị phát hiện bởi đối thủ mật mã, chúng thường phải được bảo

đảm an toàn trong khi phân phối và trong khi dùng. Hậu quả của yêu cầu về việc lựa chọn, phân phối và lưu trữ các chìa khóa một cách không có lỗi, không bị mất mát là một việc làm khó khăn, khó có thể đạt được một cách đáng tin cậy.

Để đảm bảo giao thông liên lạc an toàn cho tất cả mọi người trong một nhóm gồm n người, tổng số lượng chìa khóa cần phải có là $\frac{n(n-1)}{2}$

Vì vậy nghiên cứu này sẽ ứng dụng giải thuật di truyền để tạo ra khoá bí mật với mục đích bảo mật trong quá trình trao đổi khóa và ứng dụng vào thực tiễn.

CHƯƠNG 3
CÀI ĐẶT CHƯƠNG TRÌNH THỬ NGHIỆM

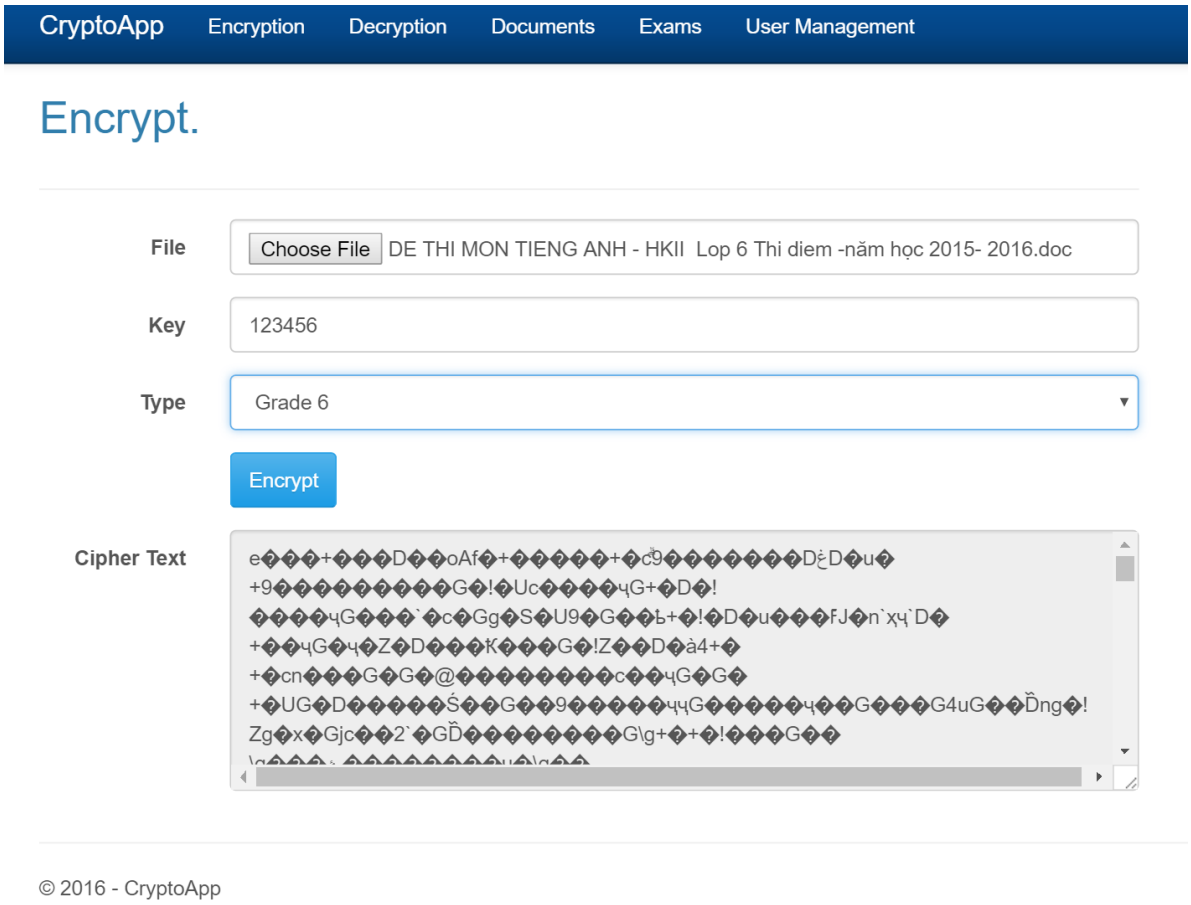
Trong báo cáo này tôi xây dựng mô hình bảo mật ngân hàng đề thi và thi online ứng dụng mã hóa khóa bí mật sử dụng Giải thuật di truyền. Sử dụng ngôn ngữ: C# trong bộ Visual studio 2013.Thử nghiệm trên mô hình hệ thống mạng nội bộ tại Trường THCS Nguyễn Đức Ứng.

3.1 Cài đặt chương trình

3.1.1 Giao diện chính:

*** Trang Admin gồm có 5 tab với 5 chức năng xử lý:**

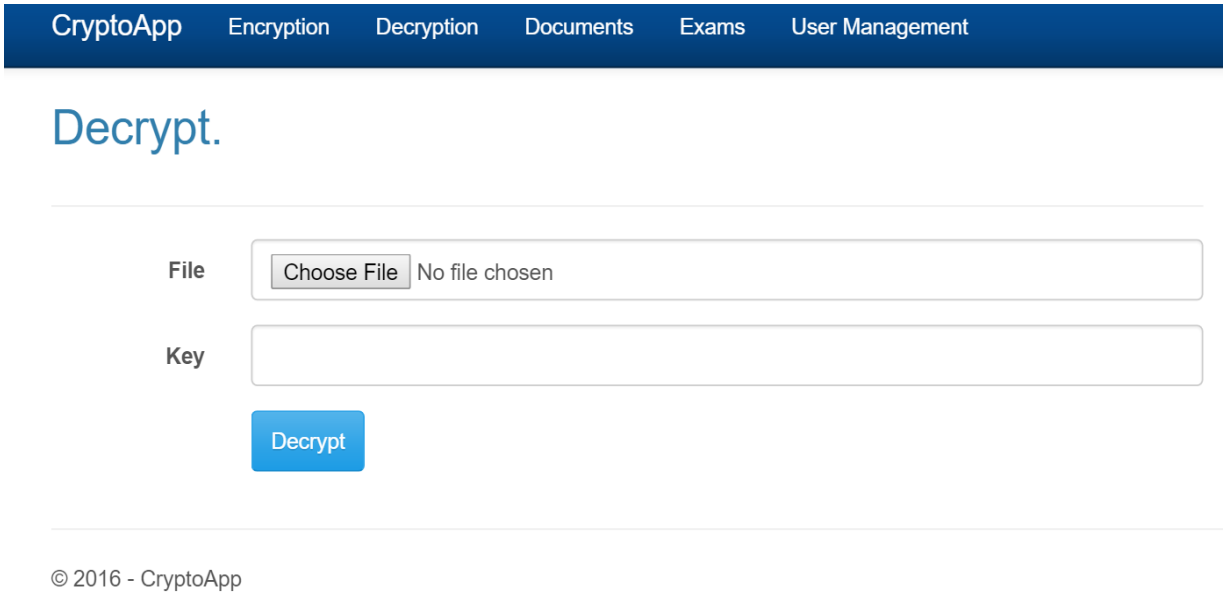
3.1.1.1 Encryption: Mã hóa file được tải lên và hiển thị nội dung mã hóa.



Hình 3.1: Đọc file và mã hóa với khóa chỉ định

- Chức năng: chọn file cần mã hóa, nhập key, chọn thư viện cần lưu, bấm Encrypt để xử lý.

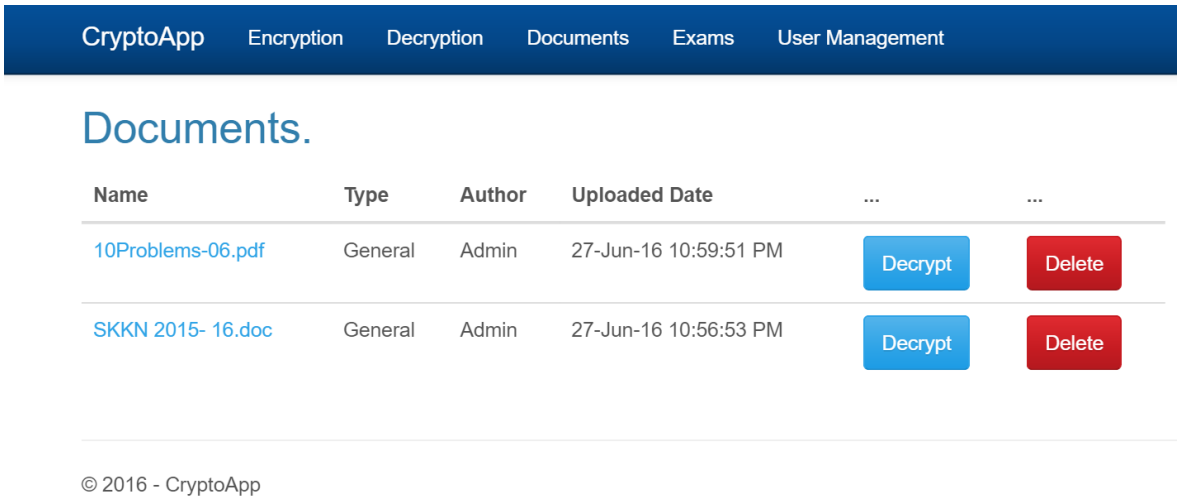
3.1.1.2 Decryption: Giải mã file



Hình 3.2: Upload file và giải mã với khóa

Chức năng: Chọn file cần giải mã, nhập key, bấm Decrypt để giải mã.

3.1.1.3 Documents: Ngân hàng dữ liệu dùng chung

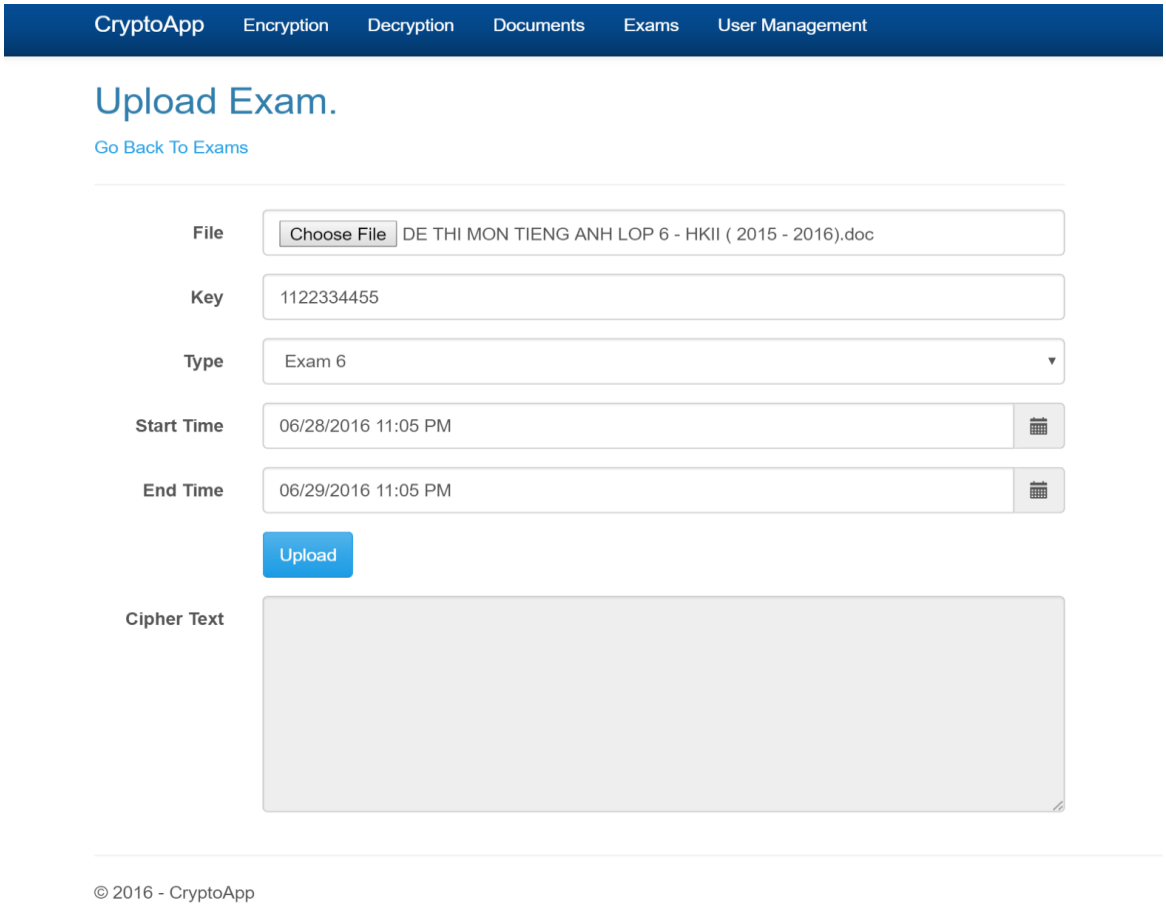


Hình 3.3: Quản lý kho tài liệu dùng chung

Chức năng: mọi người có thể chia sẽ tài liệu của mình trên đây, nhưng chỉ những người có key mới giải mã được tài liệu. Chỉ Admin có quyền xóa file.

3.1.1.4 Exam: Quản lý đề thi và upload đề thi

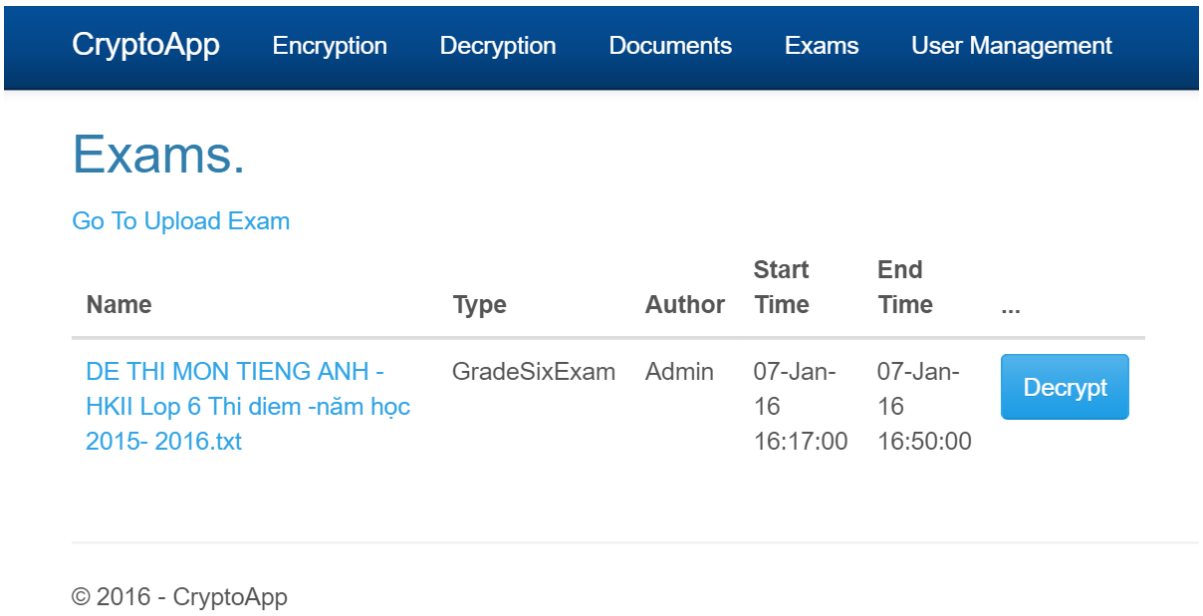
*** Upload đề thi:**



Hình 3.4: Upload bài thi với khóa và chọn khối khi, ngày giờ thi

Chức năng: Upload đề thi, chọn lớp thi, chọn thời gian bắt đầu và kết thúc. Đến thời gian hẹn sẵn học sinh mới được bắt đầu làm bài.

*** Quản lý đề thi:**



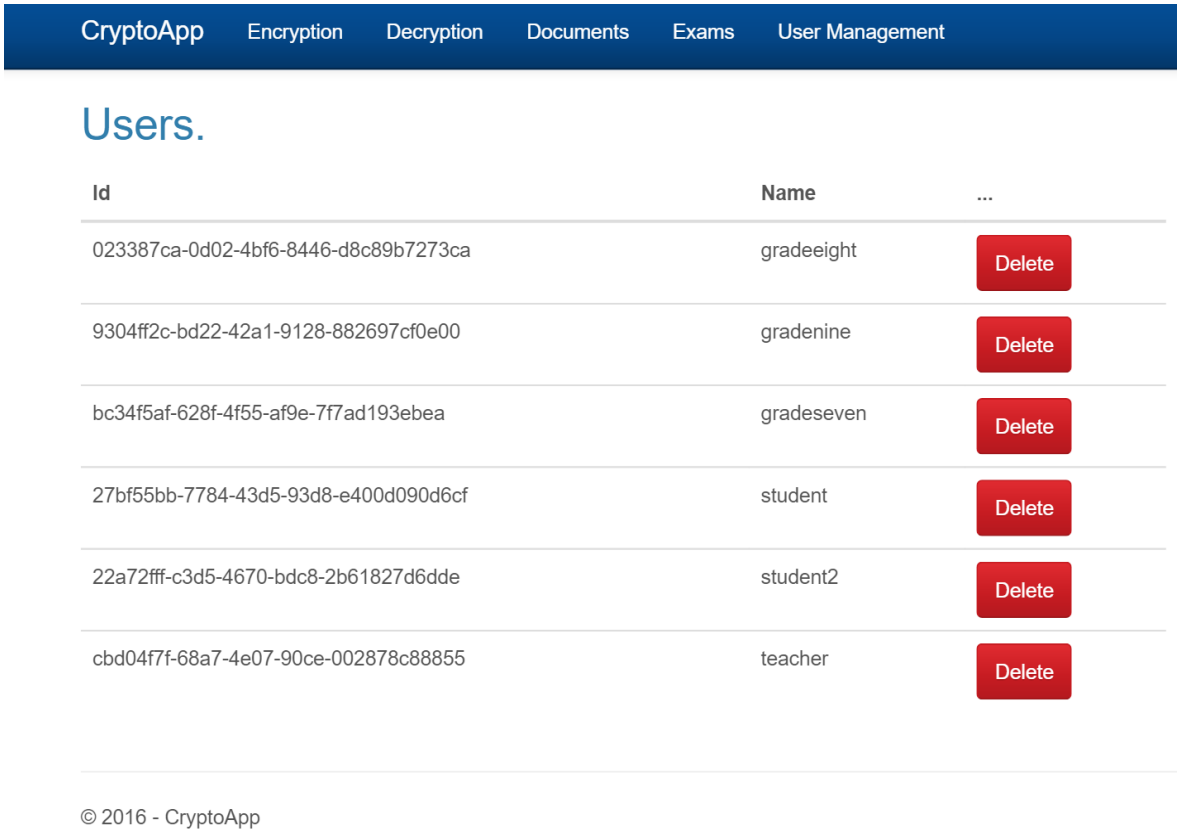
Hình 3.5: Admin quản lý đề thi

- Admin có thể tải lên đề thi hoặc tải về bài thi.

3.1.2 Các tính năng chính

3.1.2.1 Usermanager: Quản lý user

Chức năng: Admin có thể thêm, xóa user thường, học sinh hoặc giáo viên.

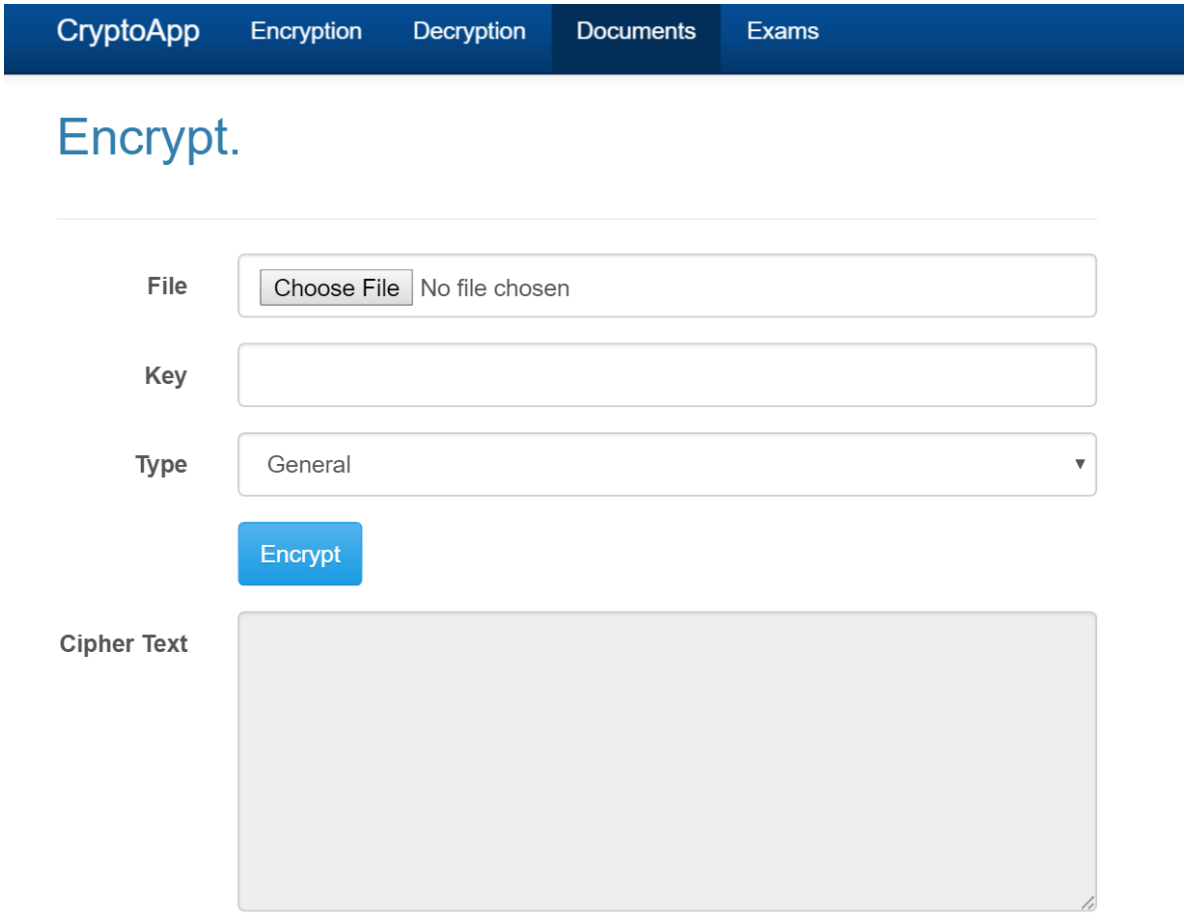


Hình 3.6: Quản lý User

3.1.2.2 Trang Login của Giáo viên gồm có 4 tab:

- Tab Encryption

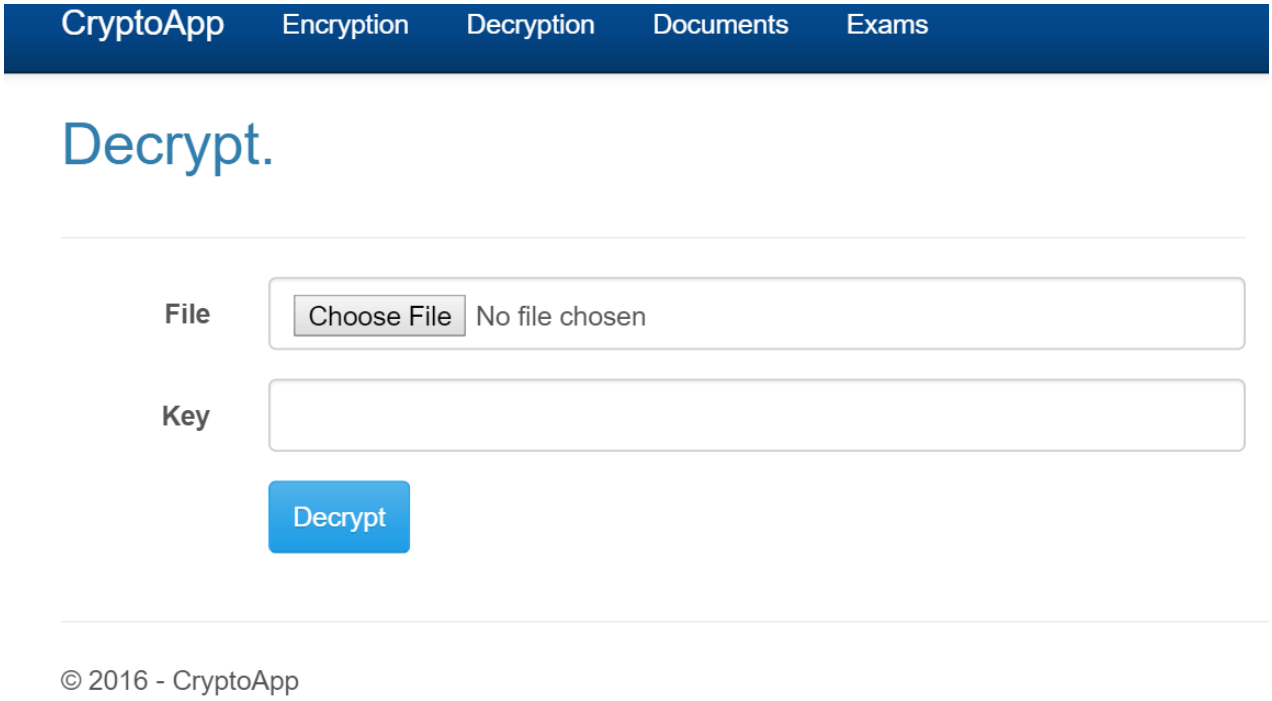
Chức năng: Upload bài thi cho từng khối và upload tài liệu dùng chung.



Hình 3.7: Trang Login của Giáo viên

- **Tab Decryption**

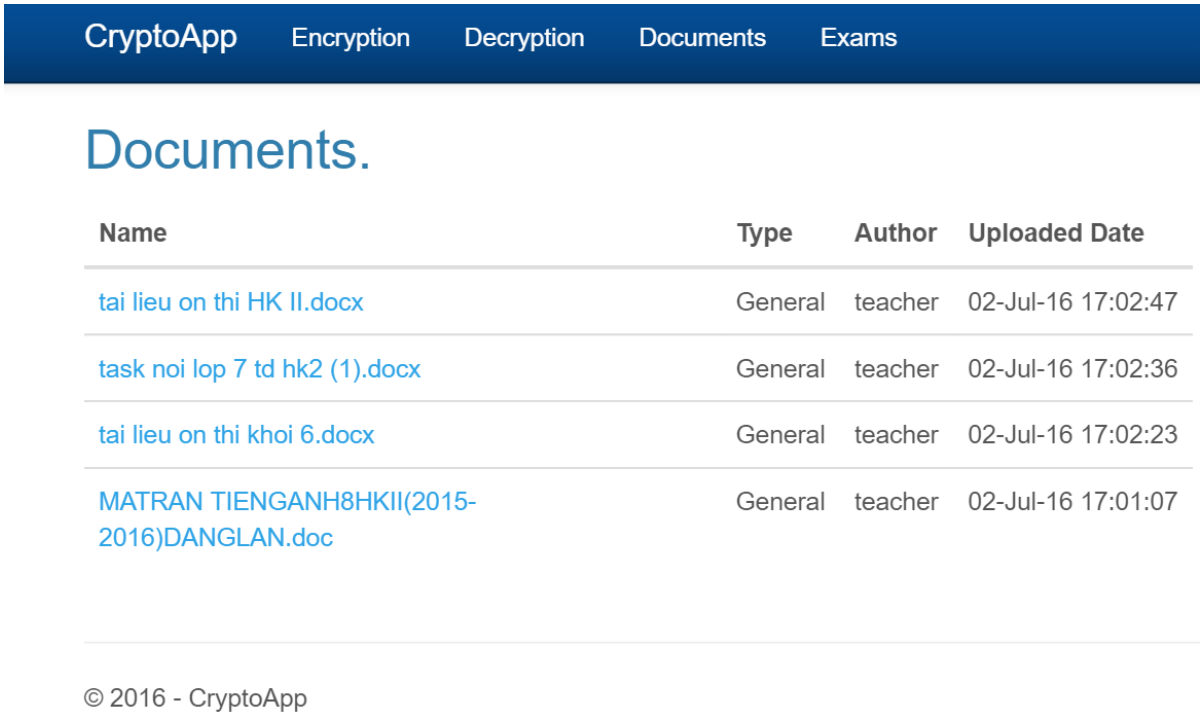
Chức năng: Giải mã tài liệu được mã hóa với khóa cho trước.



Hình 3.8: Chức năng Upload của giáo viên

- Tab Documents

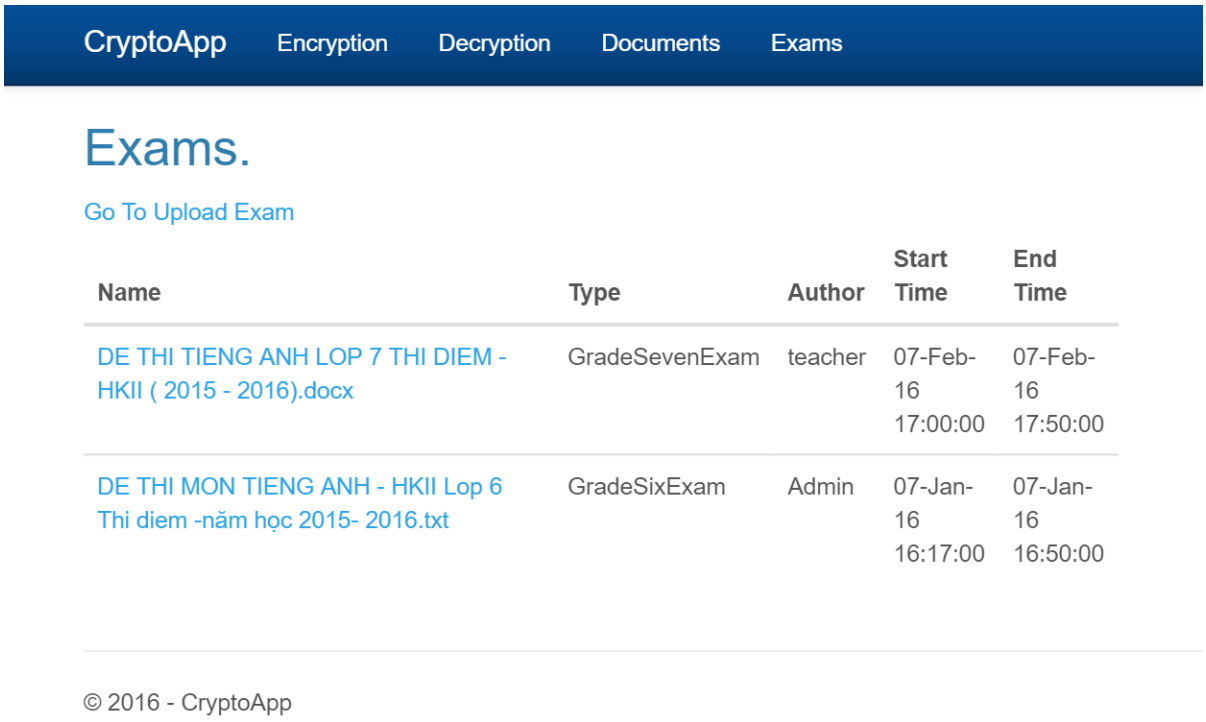
Chức năng: Ngân hàng tài liệu dùng chung được chia sẽ mã hóa.



Hình 3.9: Ngân hàng đề thi, tài liệu

- Tab Exams

Chức năng: Quản lý bài thi mình đã upload.

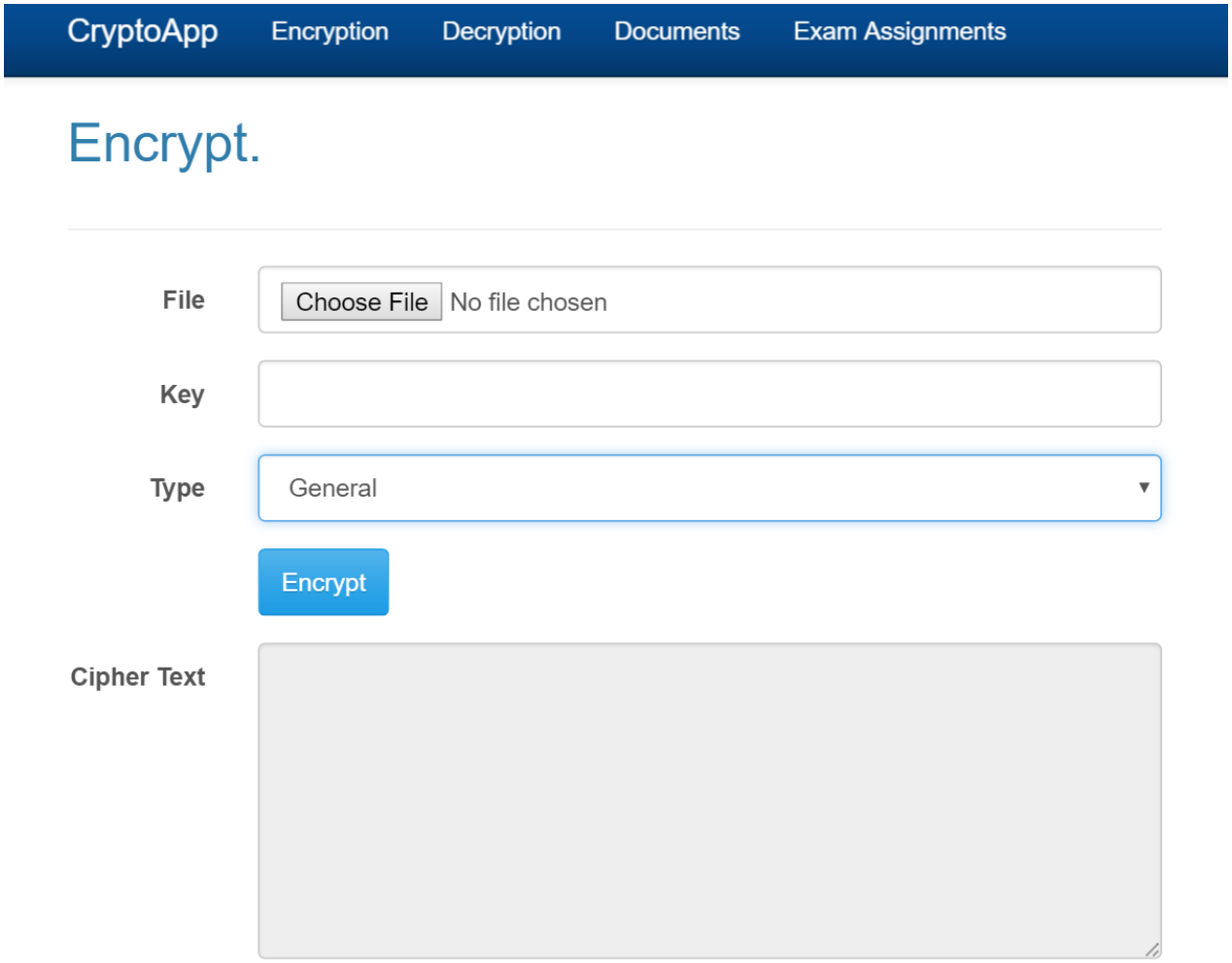


Hình 3.10: Quản lý bài thi mình đã Upload

3.1.2.3 Trang Login của Học sinh gồm có 4 tab:

- **Tab Encryption**

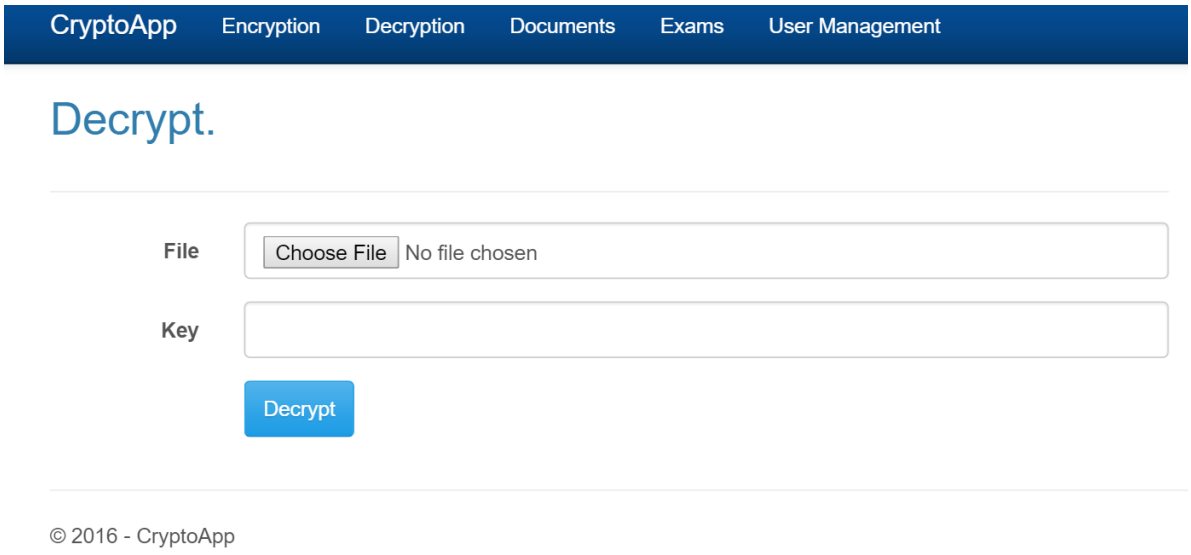
Chức năng: Upload tài liệu mã hóa (học sinh chỉ có quyền upload tài liệu vào Documents và khối lớp mình đang học).



Hình 3.11: Trang Login của học sinh

- **Tab Decryption**

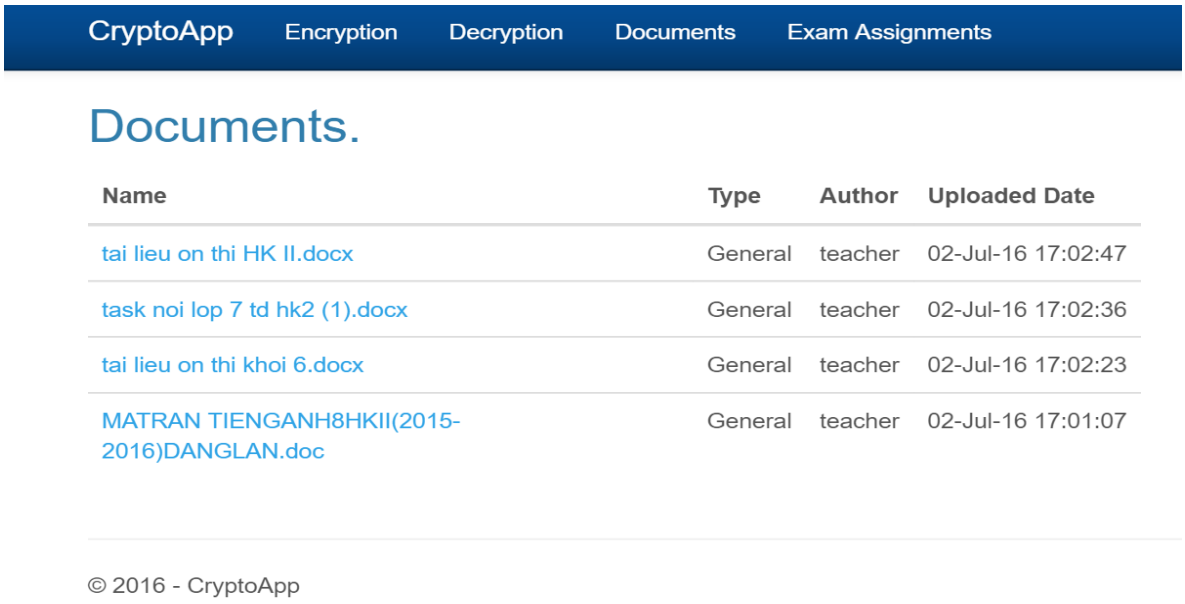
Chức năng: Giải mã tài liệu mã hóa với khóa cho trước



Hình 3.12: Chức năng Upload của học sinh

- **Tab Documents**

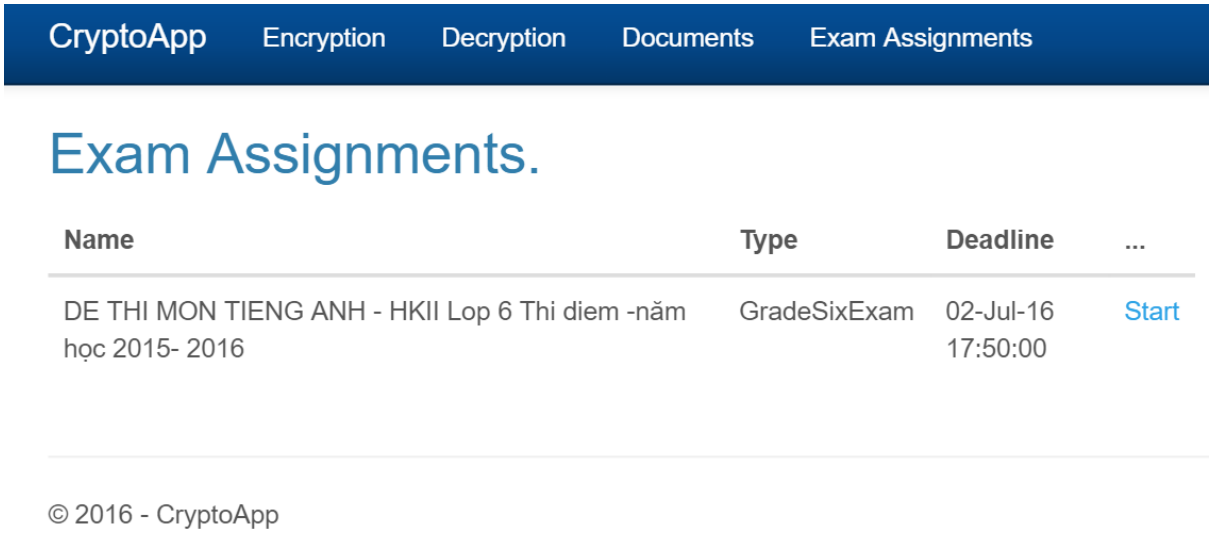
Chức năng: Kho tài liệu mã hóa được chia sẽ dùng chung (học sinh chỉ thấy được tài liệu mục Documents và khối lớp mình đang học).



Hình 3.13: Chức năng quản lý tài liệu của học sinh

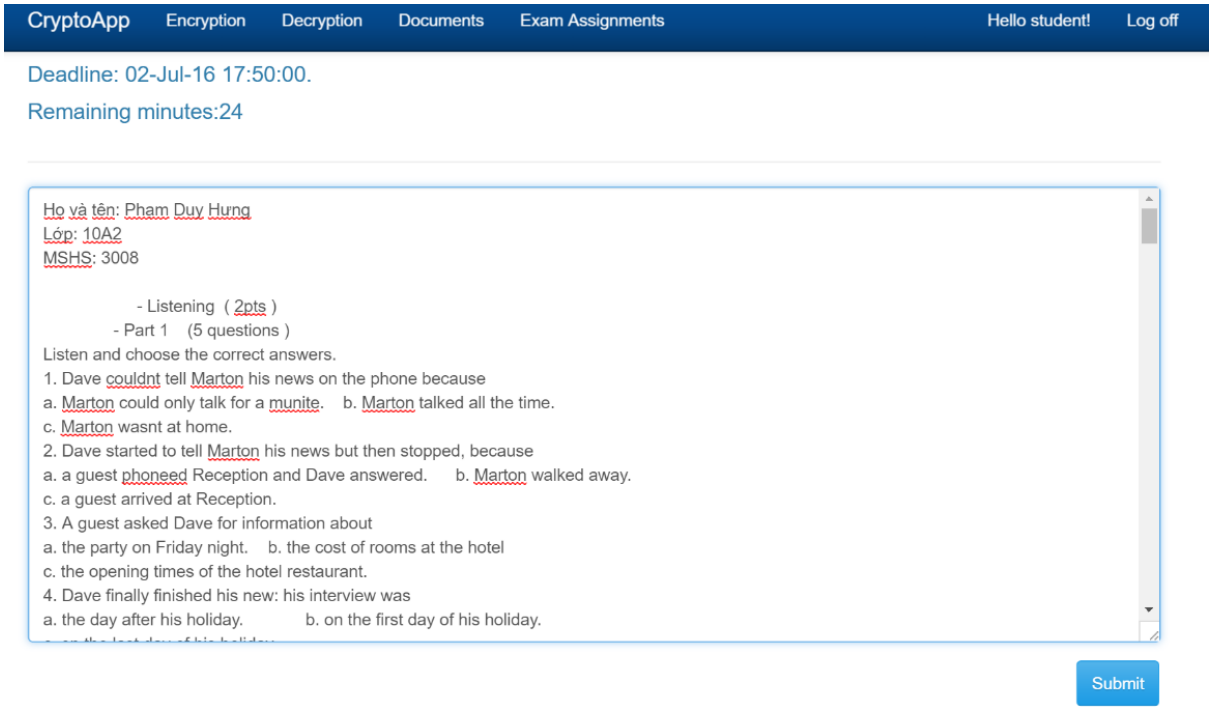
- **Tab Exam Assignments**

Chức năng: Thi online theo ngày giờ được định sẵn (học sinh chỉ thấy được bài thi của khối mình đang học và đến đúng ngày giờ bài thi mới xuất hiện).



Hình 3.14: Chức năng thi Online của học sinh

Học sinh sẽ click nút Start để bắt đầu thi, bài thi được tự động giải mã và hiển thị cho học sinh làm. Thời gian sẽ bắt đầu đếm ngược.



Hình 3.15: Chức năng làm bài thi Online của học sinh

Trước khi thời gian làm bài kết thúc, học sinh phải bấm nút Submit để nộp bài, nếu quá thời gian nộp bài Server sẽ đóng lại không thể nộp bài.

Bài thi sẽ được mã hóa với khóa sinh ngẫu nhiên và gửi về server.

Phòng đào tạo sẽ lấy bài thi, giải mã và chuyển cho giáo viên chấm điểm.

PHẦN KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

Kết luận:

Các thuật toán đề xuất thực hiện trong bài này là đơn giản và dễ dàng triển khai trong hệ thống mật mã. Quá trình tạo khóa và Thuật toán mã trung gian cung cấp bảo mật tốt để truyền tải dữ liệu trên mạng. Ở đây thuật toán thay thế khóa được sử dụng để đảm bảo tính bí mật, kết hợp và thực hiện với sự giúp đỡ của các chức năng di truyền để cung cấp gia tăng thêm biện pháp an ninh.

Luận văn cũng trình bày một số lý thuyết và một số thuật toán về mã hóa dữ liệu bảo toàn tính riêng tư của các tác giả khác đã được công bố.

Kết quả thực nghiệm cho thấy rằng thuật toán mã hóa và giải mã là an toàn. Điều quan trọng ở đây là, cho dù người ngoài có thể lấy được đề thi nhưng không có khóa giải mã thì cũng không thể nào tấn công và phát hiện ra bản gốc (bản rõ) được.

Kết quả đạt được:

- Nghiên cứu lịch sử phát triển của Giải thuật di truyền, các cơ chế mã hóa ứng dụng Giải thuật di truyền.

- Các khái niệm về giải thuật di truyền, nhiễm sắc thể, các toán tử lai ghép, ghép chéo, đột biến.

- Tổng quan về Mật mã học, cơ chế mã hóa và giải mã. Lập bảng biểu so sánh giữa Mã hóa khóa bí mật và mã hóa khóa công khai.

- Tìm hiểu về thuật toán tạo khóa bí mật, các thuận toán Triple DES, AES, RSA …

- Đã ứng dụng được cơ bản mã hóa khóa bí mật sử dụng Giải thuật di truyền vào thực tiễn tại Trường THCS Nguyễn Đức Ứng.

Hướng phát triển:

Trong tương lai, tôi đang có kế hoạch để thay đổi thuật toán để hỗ trợ cả mã hóa hình ảnh, thêm nhiều định dạng hơn hỗ trợ tốt hơn trong ứng dụng thi Online.

Cần phân tích độ phức tạp về không gian và thời gian chạy trong chương trình mã hóa/giải mã để hiểu rõ hơn khả năng áp dụng vào thực tế, cũng như cải tiến thời gian khai thác bằng các thuật toán khai thác có độ phức tạp tốt hơn.

Thực nghiệm trên CSDL lớn và có tính thực tế cao hơn.

TÀI LIỆU THAM KHẢO

[1] William Stallings, “Cryptography and Network Security”, 4rd Edition, Nov 2005.

[2] Goyat, S., “Cryptography Using Genetic Algorithms (GAs).” IOSR Journal of Computer Engineering (IOSRJCE), Volume 1, Issue 5, Volume 1, Issue 5, June 2012.

[3] Delman, B., “Genetic Algorithms in Cryptography.” Master of Science in Computer Engineering, Rochester Institute of Technology, Rochester, New York, July 2004

[4] Subhranil Som, Niladri Shekhar Chatergee, J.K Mandal, “Key Based Bit Level Cryptographic Technique(KBGCT)”, 7th International Conference on Information Assurance and Security, 2011.

[5] Sindhuja K et al, “A Symmetric Key Encryption Technique Using Genetic Algorithm” (IJCSIT) International Journal of Computer Science and information Technologies, Vol. 5 (1), 2014, 414-416

[6] Harsha Bhasin, Ramesh Kumr, Neha Kathuria, “Cryptography using Cellular Automata”. Iternational Journal of Computer Science and Information Technology, Vol. 4(2), 355-357, 2013.

[7] Xiao, X.K. and Tao, Y.F.,” Utility-Based Anonymization Using Generalization Boundaries to Protect Sensitive Attributes”, Journal of Information Security, Vol.6 No.3, June 15, 2015

[8] https://vi.wikipedia.org/wiki/Thuật_toán_khóa_đối_xứng.

[9] https://vi.wikipedia.org/wiki/Giải_thuật_di_truyền