**TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI**

**VIỆN ĐIỆN TỬ - VIỄN THÔNG**



**LÍ THUYẾT MẬT MÃ**

**ĐỀ TÀI: ỨNG DỤNG CHỮ KÍ SỐ SỬ DỤNG HỆ MẬT RSA VÀO THU THUẾ**

**Nhóm thực hiện:**

**Nguyễn Nguyên Bách (20150239) – Điện tử 08 K60**

**Trương Công Chính (20130422) – KT ĐT-TT 08 K58**

**Mai Văn Hải (20141365) – Điện tử 03 K60**

**Nguyễn Minh Hiếu (20151336) – Điện tử 03 K60**

**Giảng viên hướng dẫn: TS. Hán Trọng Thanh**

**Hà Nội, tháng 5/2018**

**NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN**

…………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

# LỜI MỞ ĐẦU

Ngành điện tử - viễn thông hiện nay là ngành mũi nhọn, được ứng dụng rộng rãi, đóng vai trò quan trọng trong sản xuất và đời sống. Với mục tiêu công nghiệp hóa, hiện đại hóa đất nước, các hệ thống máy móc ngày càng phải nhỏ gọn, tinh vi, hiệu năng tốt. Vì vậy, các ứng dụng công nghệ kỹ thuật điện tử ngày càng được mở rộng, là một phần không thể thiếu trong nền công nghiệp hiện đại.

Bản thân chúng em là sinh viên ngành điện tử - viễn thông, cần nâng cao trình độ, khả năng thực hành và ứng dụng kiến thức đã học vào thực tế. Học phần Lí thuyết mật mã đã giúp chúng em làm quen với lĩnh vực bảo mật và tìm hiểu một số ứng dụng của mật mã trong cuộc sống như bảo mật emai, tin nhắn sms, bảo mật trong ngân hàng quan đội, thông tin vệ tinh,…

Với vốn kiến thức học được trên giảng đường và tài liệu trên mạng, nhóm chúng em quyết định đưa ra đề tài “ứng dụng chữ kí số sử dụng hệ mật RSA vào thu thuế”.

Mục tiêu của đề tài là bước đầu giúp nhóm làm quen với hệ mật RSA và chữ kí số, cải thiện kĩ năng lập trình và biến kiến thức thành thực tế qua phần mềm. Trong quá trình thực hiện khó tránh khỏi những sai sót nhất định, rất mong nhận được những ý kiến đóng góp từ thầy giáo cũng như các bạn để nhóm rút kinh nghiệm, giúp các lần làm đề tài sau được hoàn thiện hơn.

Chúng em xin cảm ơn Ban lãnh đạo Viện Điện tử - Viễn thông và thầy Hán Trọng Thanh đã tạo điều kiện và hướng dẫn tận tình giúp nhóm chúng em hoàn thành đề tài này.

# Tóm tắt đề tài

Đề tài của nhóm là ứng dụng chữ kí số sử dụng hệ mật RSA vào thu thuế. Phần mềm được viết bằng ngôn ngữ C# và chạy bằng trình biên dịch Visual Studio trên nền Windows.

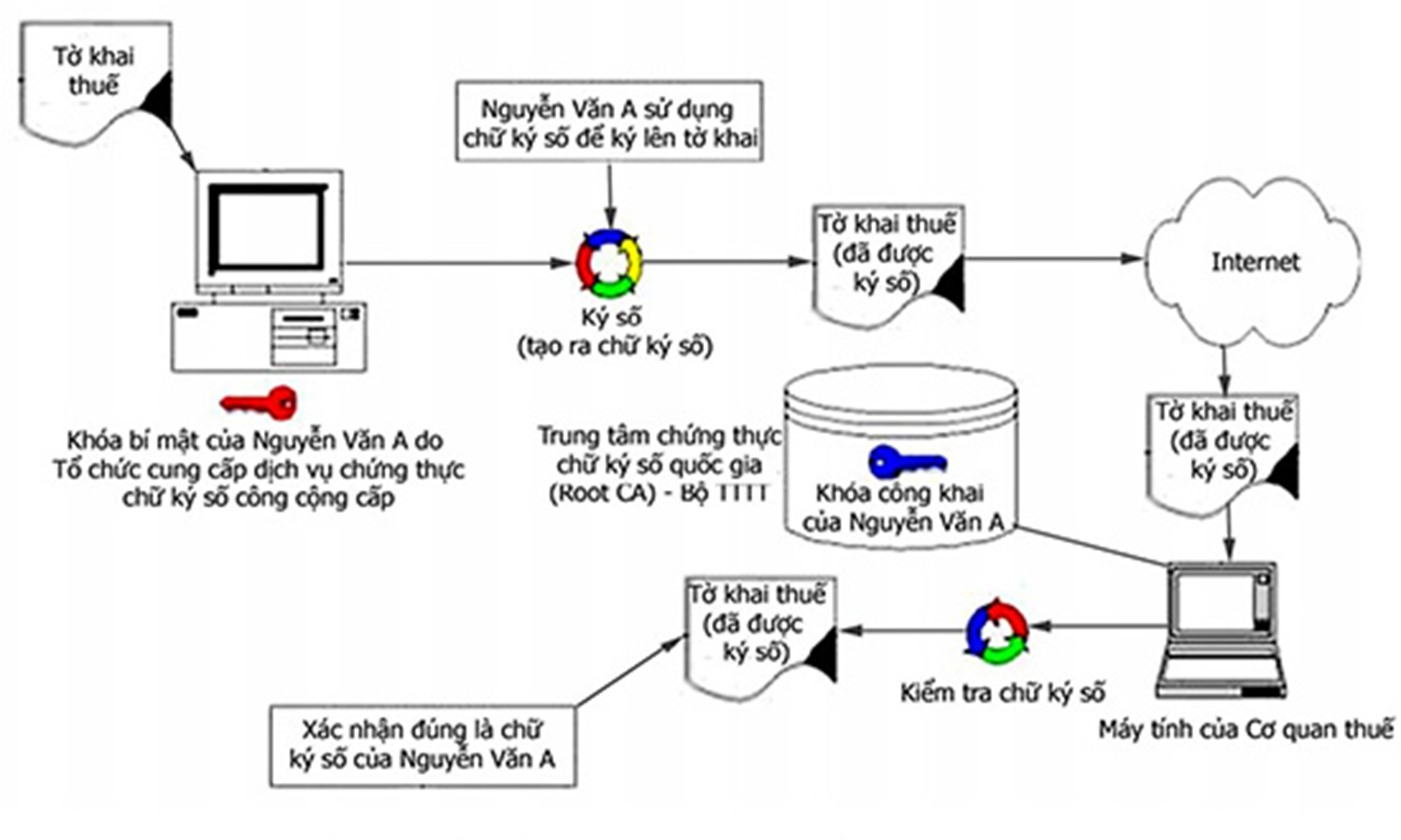
**Summary of project**

Our subject is application of digital signature using RSA cryptosystems in tax collection. Our software was written by programming language C# and run by the Visual Studio compiler on Windows.

# Ứng dụng thu thuế bằng chữ kí số

## Sơ đồ thu thuế bằng chữ kí số

Sơ đồ thu thuế bằng chữ kí số được thể hiện ở hình 3.1.



Hình Sơ đồ thu thuế bằng chữ kí số

Giả sử Nguyễn Văn A là người đi nộp thuế sử dụng chữ kí số. Nguyễn Văn A sử dụng khóa bí mật do trung tâm chứng thực chữ kí số quốc gia cấp để kí lên tờ khai thuế. Sau đó tờ khai thuế được gửi đến máy tính của cơ quan thuế.

Cơ quan thuế sử dụng khóa công khai của trung tâm chứng thực chữ kí số quốc gia để kiểm tra chữ kí số, xác nhận xem chữ kí số đúng của Nguyễn Văn A không.

**HƯỚNG DẪN SỬ DỤNG PHẦN MỀM**

Mở file Thuthue.sln

1. **Gửi file giữa client và server trong cùng 1 mạng**

Cần có 2 máy trở lên dùng chung 1 mạng

1. Gõ “Windows+R”, nhập “cmd”, nhập “ipconfig” để xem IP mạng
2. Nhập IP mạng vào ô “Nhập IP mạng”, giả sử IP mạng là 192.168.1.105
3. 1 máy chọn “Server”, các máy còn lại chọn “Client”,
4. Có thể gửi file từ server đến client hoặc ngược lại bằng các chọn “Chọn file gửi”
5. File được lưu trong thư mục “ThuThue/bin/Debug”
6. Nơi xác nhận cần nhận được tờ khai thuế cùng chữ kí và khóa công khai để thực hiện xác nhận như hướng dẫn ở mục III
7. **Tạo khóa và mã hóa thử**
8. Tạo các file cipher.txt, public.txt, private.txt để lưu bản mã hóa, khóa công khai và khóa bí mật
9. Chọn “Tạo khóa và mã hóa”
10. Chọn “Kích thước khóa”, giả sử nhập kích thước khóa là 512
11. Chọn “Tạo khóa”, sẽ có 1 cặp khóa công khai và bí mật được sinh ra
12. Chọn “Mã hóa”

* Đầu tiên, chọn 1 file cần mã hóa, giả sử chọn file SHA.txt có nội dung là “SHA-2 is a hash functions”
* Chọn file cipher.txt dể lưu bản mã hóa
* Chọn file public.txt để lưu khóa công khai
* Chọn file private.txt để lưu khóa bí mật

1. Chọn “Giải mã”

* Đầu tiên, chọn file cipher.txt chứa bản mã hóa
* Chọn file private.txt chứa khóa bí mật, bản rõ sẽ được hiển thị

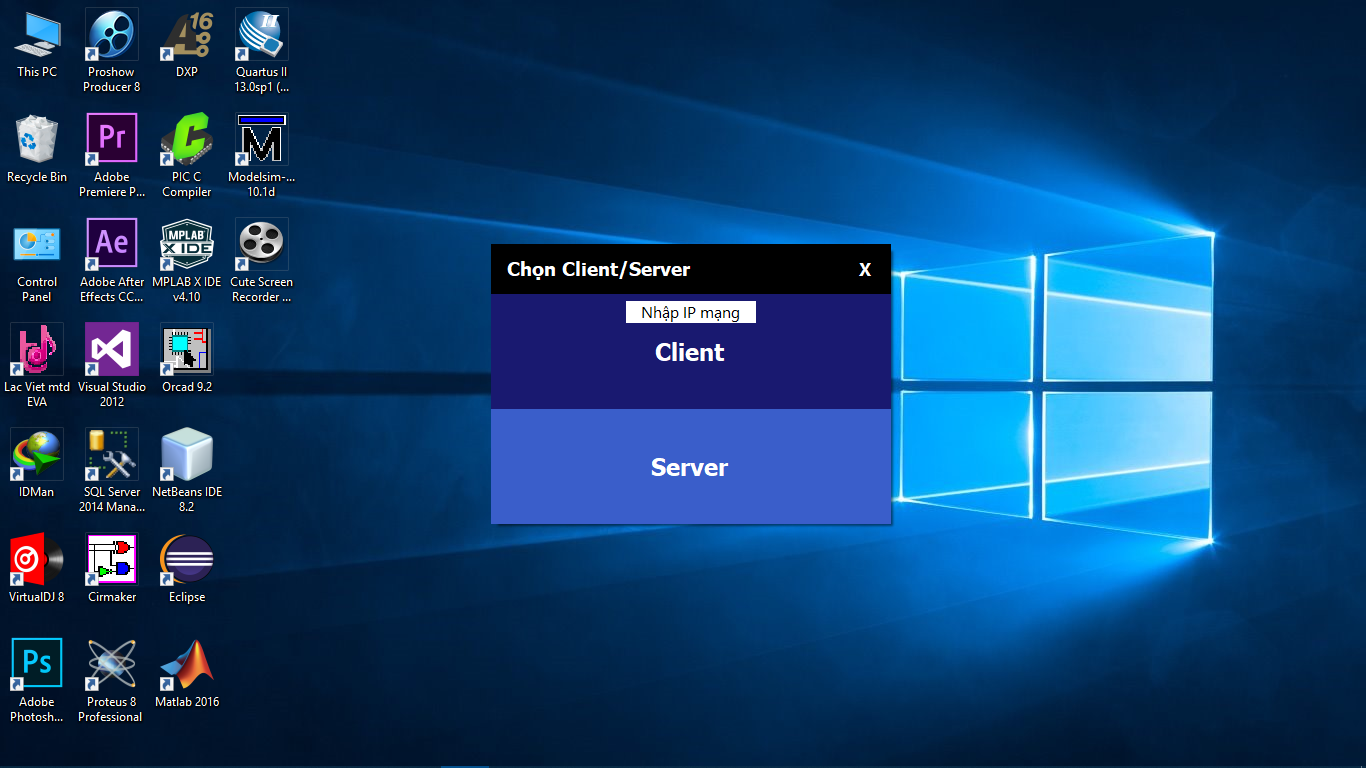
1. Chọn “Làm lại” nếu muốn làm lại từ đầu
2. **Tạo và kiểm tra chữ kí**
3. Tạo file Tờ khai thuế.docx để kí thử
4. Chọn “Ký và xác nhận”
5. Chọn “Nhập tờ khai thuế”, giả sử chọn file Tờ khai thuế.docx
6. Chọn “Chọn khóa bí mật”, chọn file private.txt
7. Chọn “Tạo chữ kí”, chữ kí được sinh ra
8. Chọn “Lưu chữ kí”, chữ kí được lưu dưới tên Tờ khai thuế.vsdx.sig.txt
9. Chọn “Chọn tờ khai thuế đã kí”, chọn file Tờ khai thuế.docx
10. Chọn file chứa chữ kí Tờ khai thuế.vsdx.sig.txt
11. Chọn “Chọn khóa công khai”, chọn file public.txt
12. Chọn “Xác nhận”, thông báo “Chữ kí hợp lệ” sẽ được hiển thị

## Phần mềm mô phỏng

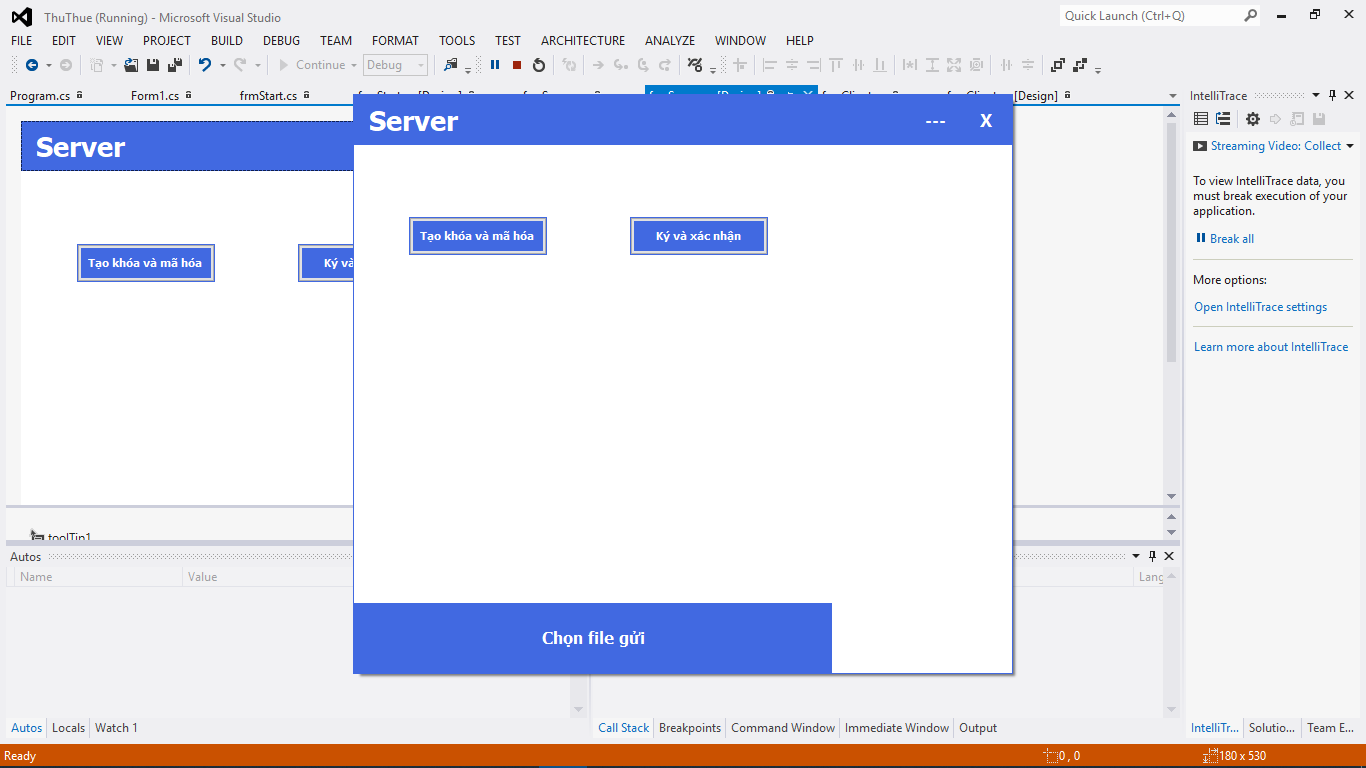
Phần mềm gồm có 3 phần chính:

* Phần gửi file giữu server và client
* Phần tạo khóa và mã hóa thử
* Phần tạo chữ kí và kiểm tra chữ kí

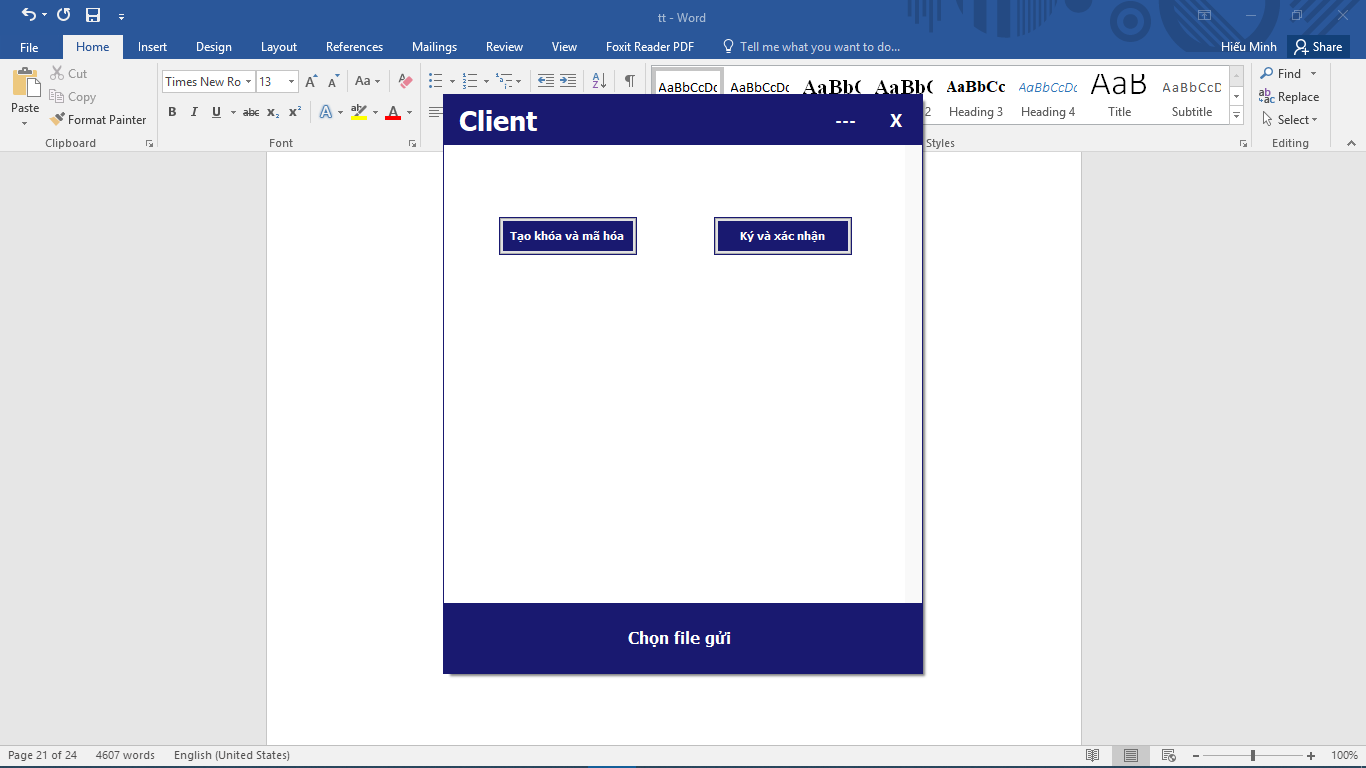
Phần mềm có chú thích đi kèm code và hướng dẫn cụ thể sử dụng phần mềm có trong file hướng dẫn.docx đi kèm.



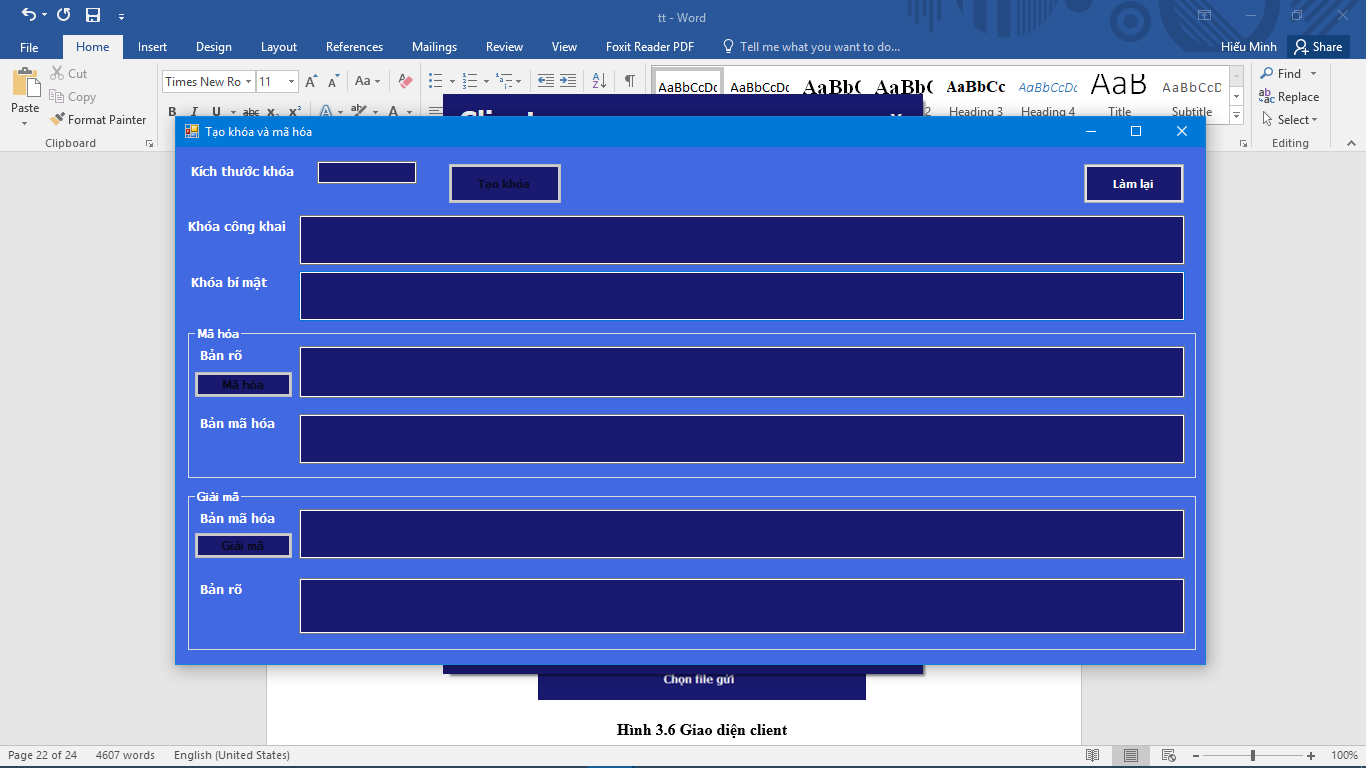
Hình Giao diện phần chọn client/server



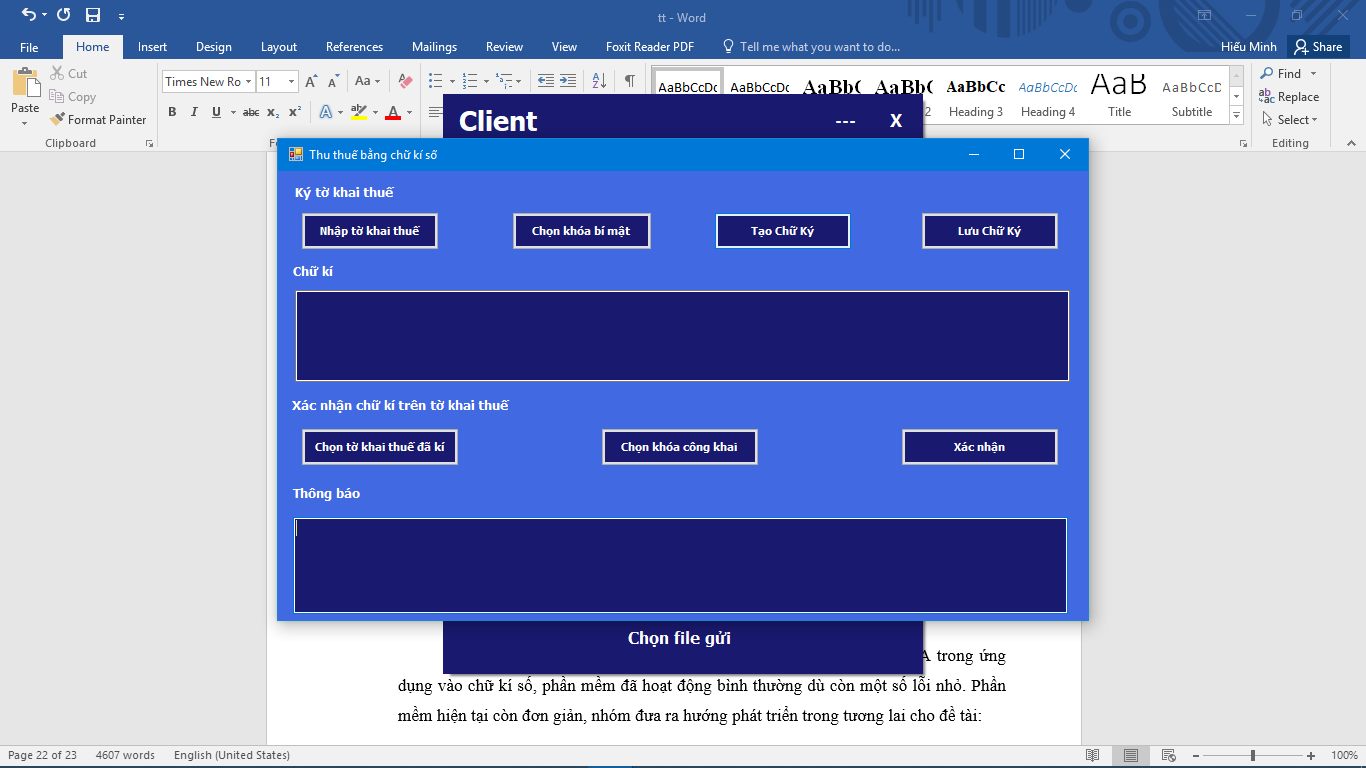
Hình Giao diện server



Hình Giao diện client



Hình Giao diện tạo khóa và mã hóa



Hình Giao diện ký và xác nhận

# KẾT LUẬN

Trong đề tài này, nhóm đã kiểm tra sự hoạt động của hệ mật RSA trong ứng dụng vào chữ kí số, phần mềm đã hoạt động bình thường dù còn một số lỗi nhỏ. Phần mềm hiện tại còn đơn giản, nhóm đưa ra hướng phát triển trong tương lai cho đề tài:

* Sửa các lỗi nhỏ, cải thiện hiệu năng phần mềm.
* Làm đẹp giao diện, dễ sử dụng hơn cho người dùng.
* Cố gắng ứng dụng thu thuế qua web.

Một lần nữa, nhóm xin cảm ơn thầy Hán Trọng Thanh đã giảng dạy và giúp chúng em hiểu rõ hơn về ngành mật mã – ngành học còn mới và chưa phổ biến trong chương trình đào tạo Điện tử - Viễn thông của trường.

# TÀI LIỆU THAM KHẢO

Nhóm sử dụng tài liệu tham khảo ở một số nguồn sau:

[1] <https://en.wikipedia.org/wiki/RSA_(cryptosystem)>

[2] <https://en.wikipedia.org/wiki/Digital_signature>

[3] <https://chukysovnpt-ca.com/gioi-thieu-ve-chu-ky-so>

[4] <https://en.wikipedia.org/wiki/Secure_Hash_Algorithms>