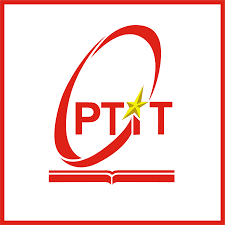
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

**KHOA CÔNG NGHỆ THÔNG TIN 2**

----------**🙠🙣✪🙡🙣**----------



**BÀI BÁO CÁO TIỂU LUẬN CUỐI KỲ**

**MÔN HỌC: CÁC HỆ THỐNG PHÂN TÁN**

**NHÓM: 15**

**Giảng viên: Lê Ngọc Bảo**

**Sinh Viên: Ung Nguyễn Trường Luân**

**MSSV: N18DCCN120**

**Lớp: D18CQCP01-N**

**Năm học: 2021-2022**

Mục lục

**Phần 1: Bài tập cá nhân3**

1. Câu 223

2. Câu 1113

3. Câu 2004

**Phần 2: Bài tập nhóm4**

1. Tổng quan về ứng dụng4
2. Hoạt động của server5
3. Hoạt động của client5
4. Thuật toán DES7

4.1 Quy trình mã hóa7

4.2 Quy trình giải mã7

1. Giải thích code8
2. Tài liệu tham khảo13

**Phần 1: Bài tập cá nhân**

1. ***Câu 22:***

**Q:** Consider an unstructured overlay network in which each node randomly chooses *c* neighbors. If *P* and *Q* are both neighbors of *R*, what is the probability that they are also neighbors of each other?

**A:** Consider a network of *N* nodes. If each node chooses *c* neighbors at ran- dom, then the probability that *P* will choose *Q*, or *Q* chooses *P* is roughly 2*c* / (*N* - 1).

**Trả lời:**

Hệ thống P2P không có cấu trúc dựa vào các thuật toán ngẫu nhiên để xây dựng một mang lớp phủ (Overlay network):

* Thuật toán ngẫu nhiên để xây dựng mạng overlay gọi chung là random graph
* Mỗi node duy trì một danh sách hàng xóm còn gọi là partial view
* Dữ liệu sẽ được đưa vào hệ thống một cách ngẫu nhiên

Dữ kiện bài toàn: Một mạng có N node và mỗi node chọn ngẫu nhiên c hàng xóm thì xác xuất P chọn Q là c/(N-1) và P chọn Q cũng là c/(N-1)

Giải thích: c/(N-1) là chọn ngẫu nhiên c Node trong N-1 Node còn lại.

Xác xuất để R không chọn cả P và Q là: c/(N-3)

Xác xuất để R không chọn P là: c/(N-2) – c/(N-3)

Xác xuất để R không chọn Q là: c/(N-2) – c/(N-3)

* Xác xuất R chọn cả P và Q : là phần bù của **không chọn P**, **không chọn Q** và **không chọn cả P và Q**
* Xác xuất R chọn cả P và Q = 1 – c/(N-3) – 2( c/(N-2) – c/(N-3) )

= **1 – 2c/(N-2) + c/(N-3)**

1. ***Câu 111:***

**Q:** A distributed system may have multiple, independent resources. Imagine that process 0 wants to access resource *A* and process 1 wants to access resource *B*. Can Ricart and Agrawala’s algorithm lead to deadlocks? Explain your answer.

**Trả lời:**

* Thuật toánRicart and Agrawala không dẫn đến bế tắc vì mỗi tài nguyên được sử lý độc lập với tất cả các tài nguyên khác vì:
* Nếu các tiến trình truy cập tài nguyên một cách tuần tự và nghiêm ngặt có nghĩa là một tiến trình đang nắm giữ một tài
* nguyên thì không thể truy cập vào 1 tài nguyên khác thì sẽ không có cách nào mà nó có thể chặn khi đang giữ một tài nguyên mà một số tiến trình khác muốn => Hệ thống không bị tắt nghẽn.
* Mặt khác nếu tiến trình 0 nắm giữ tài nguyên A và đang cố truy cập vào tài nguyên B, thì có thể xảy ra tắt nghẽn nếu một số tiến trình khác đang cố gắng lấy tài nguyên theo chiều ngược lại. Có nghĩa là các tiến trình này đang nắm giữ tài nguyên B và cố gắng truy cập vào tài nguyên A. => Điều này có thể làm hệ thông xảy ra tắt nghẽn.

1. ***Câu 200:***

**Q:** Using RPC2’s side effects is convenient for continuous data streams. Give another example in which it makes sense to use an application-specific proto- col next to RPC.

**Trả lời:**

- Thay vì sử dụng cơ chế RPC thuần túy, có thể hiệu quả hơn khi chuyển các tệp rất lớn bằng giao thức như FTP. FTP cho phép tất cả các máy tính kết nối với một mạng lưới có nền TCP/IP, xử lý tập tin trên một máy tính khác trên cùng một mạng lưới với mình, bất kể máy tính ấy dùng [hệ điều hành](https://vi.wikipedia.org/wiki/H%E1%BB%87_%C4%91i%E1%BB%81u_h%C3%A0nh) nào (nếu các máy tính ấy đều cho phép sự truy cập của các máy tính khác, dùng giao thức FTP).

-Và hiện này dịch vụ FTP của WEB đã ứng dụng trong việc xử lý một số thao tác về tập tin, như tải tập tin lên máy chủ, tải tập tin từ máy chủ xuống máy của mình, đổi tên của tập tin, hoặc xóa tập tin ở máy chủ v.v

**Phần 2: Bài tập Nhóm**

**Đề tài 15: Xây dựng ứng dụng mã háo chuỗi tin và giải mã thông tin truyền trên hệ thống Client Server**

1. **Tổng quan về ứng dụng**

* Ứng dụng gồm hai phần Client và Server:
* Công việc của Client:

1. Gửi tin nhắn được mã hóa và key lên cho server , tùy theo thuật toàn mình chọn mà sẽ có các loại key khác nhau.
2. Nhận phản hồi từ Server, tiếp tục dùng tin nhắn đã mã hóa và key do server gửi về để giải mã, sau đó hiện nội dung tin nhắn đã được giải mã lên trên màn hình.

* Công việc của Server:

1. Là nơi nhận tin nhắn được mã hóa cùng với key từ Client gửi lên.
2. Giải mã và show lên trên màn hình, Tiếp tục mã hóa và gửi đoạn tin đã hóa và key về cho Client

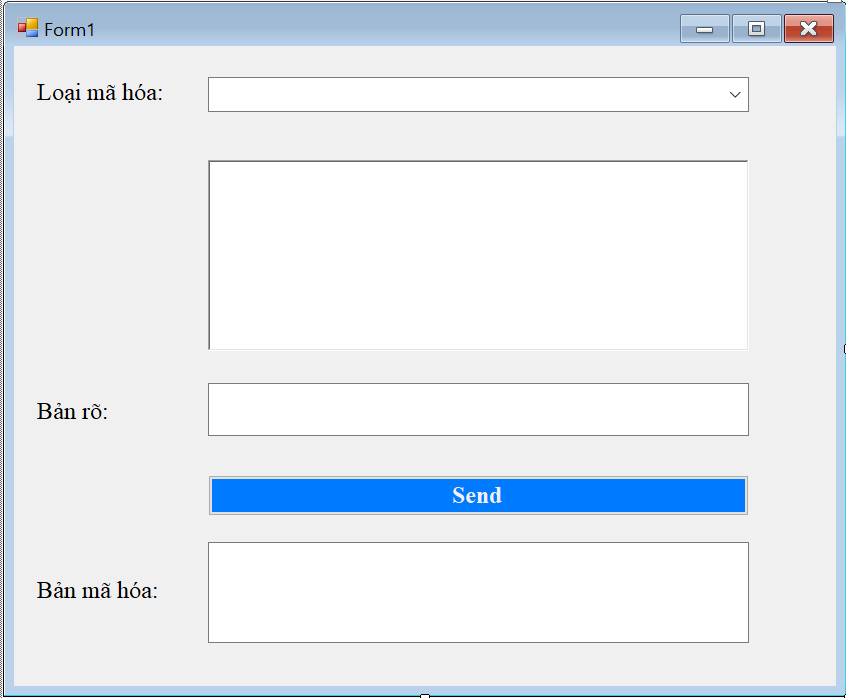
* Ứng dụng dùng phương thức TCP/IP để lắng nghe và gửi dữ liệu giữa server và client

**2. Hoạt động của Server**

* Đầu tiên ta cho khởi chạy Server, mỗi khi nào có Client kết nối tới thì ta tạo thêm 1 luồng mới cho Server và Client này nhằm mục đích nhận dữ liệu gửi và nhận giữa 2 bên. Trên Server sẽ hiện lên số Client hiện tại đang kết nối tới.
* Trong Server có các biến toàn cục được khai báo tương ứng với các thuật toán mã hóa mà chương trình cho phép. Hiện tại có 4 thuật toán (Mã hóa đối xứng: DES, 3DES, AES. Mã hóa bất đối xứng: RSA) . Dựa vào nội dung gửi từ Client lên mà server sẽ dùng các biến toàn cục để thực thi mã hóa và giải mã.
* Giải mã xong thì sẽ hiện lên màn hình của Server
* Mã hóa xong sẽ gọi hàm ECHO để gửi tin nhắn mã hóa và key về cho các Client đang kết nối tới.

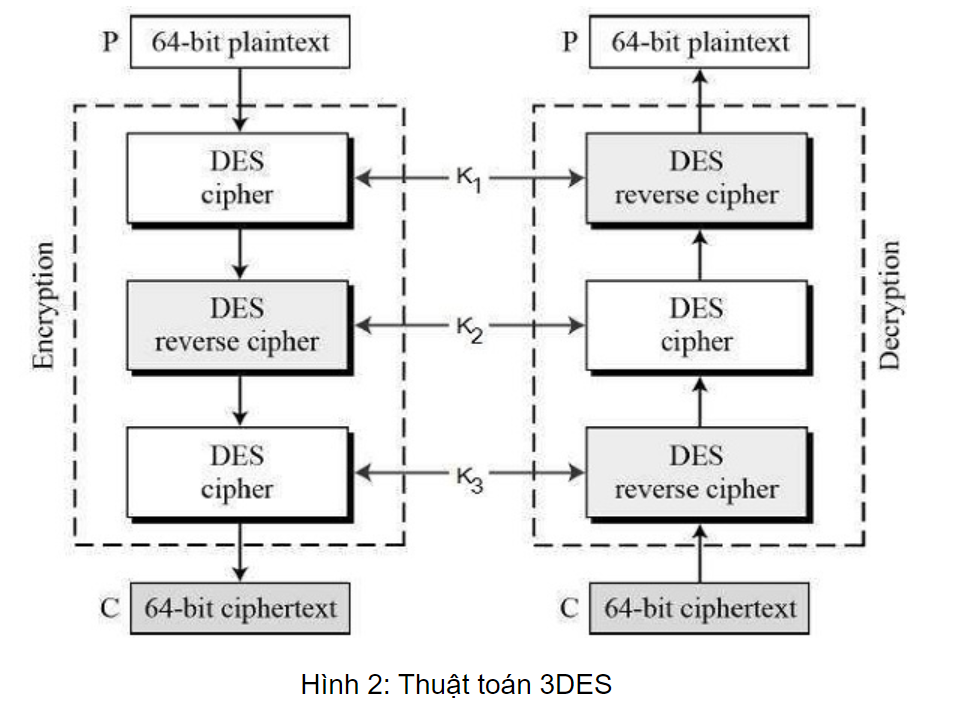
**3. Hoạt động Client**

* Cũng như Server thì Client cũng có các biến toàn cục là các thuật toàn nhằm thực hiện việc mã hóa gửi nội dung lên Server và giải mã nội dung nhận từ Server.



* + - 1. Combobox chứa danh sách các thuật toán (3DES, DES, AES, RSA).
      2. Đây là nơi hiện nội dung của chính Client gửi lên và Server gửi về.
      3. Đây là nơi ta nhập nội dung tin nhắn.
      4. Button Send sẽ gửi nội dung gồm “Thuật toán mã hóa” , “Nội dung đã đc mã hóa” , “Key”.
      5. Khi nhập nội dung tin nhắn thì đồng thời sẽ hiện ra nội dung đã mã hóa.
* Khi khởi chạy Client, trước hết kiểm tra có kết nối với Server thông qua địa chỉ IP và cổng , nếu không thể tìm thấy Server hiện ra một Message thông báo: “Không thể kết nối tới Server”.
* Hoạt động bình như giải thích ở trên
* Khi đóng Client Sẽ gửi nội dung “CLOSING” lên Server để Server gửi về các Client đang kết nối tới.

**4. Thuật Toán DES:**

Thuật toán 3DES sử dụng một nhóm khóa bao gồm 03 khóa DES là K1, K2 và K3, mỗi khóa có giá trị 56 bít. Thuật toán mã hóa thực hiện như sau:   
***4.1 Quy trình mã hóa***

**Bản mã= EK3(DK2(EK1(Bản rõ)))**

- Trước tiên, thực hiện mã hóa DES với khóa K1, tiếp tục giải mã DES với khóa K2 và cuối cùng mã hóa DES với khóa K3(E – Encryption: quá trình mã hóa; D - Decryption: quá trình giải mã; Bản rõ: Dữ liệu đầu vào của phép mã hóa hoặc dữ liệu đầu ra của phép giải mã; Bản mã: Dữ liệu đầu ra của phép mã hóa hoặc dữ liệu đầu vào của phép giải mã).

***4.2 Quy trình giải mã***

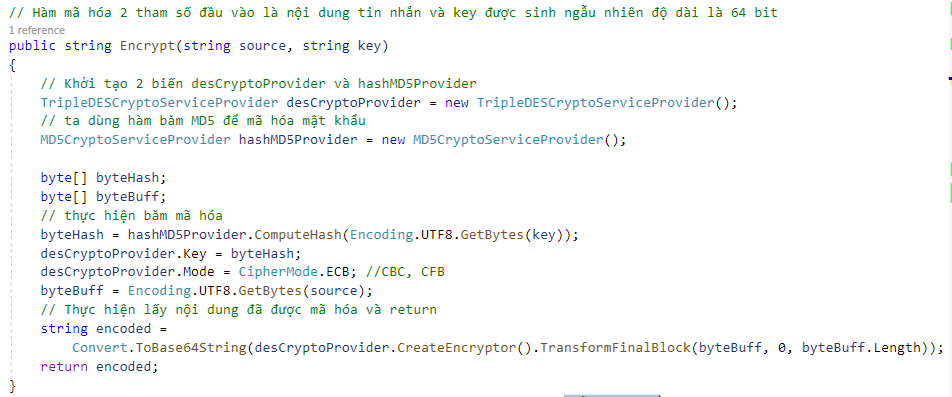
**Bản rõ = DK1(EK2(DK3(Bản mã))**

* Quá trình giải mã với việc giải mã với khóa K3, sau đó mã hóa với khóa K2,và cuối cùng giải mã với khóa K1

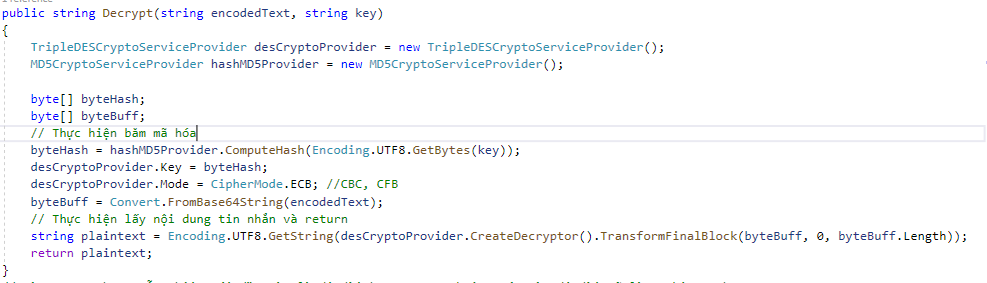
Để thuật toán mã hóa 3DES có độ an toàn cao nhất thì các khóa K1,K2,K3 phải khác nhau.

**5.Giải thích code:** Dưới đây là các đoạn code quan trọng của ứng dụng

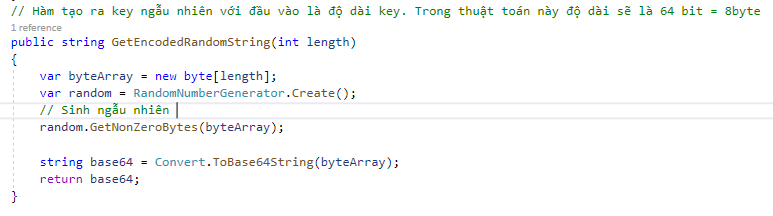
* Hàm mã hóa



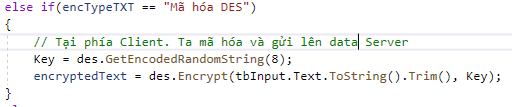
* Hàm giải mã



* Hàm tạo khóa ngẫu nhiên theo độ dài bất kỳ



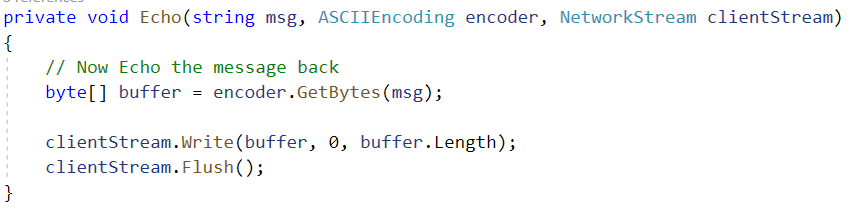
* Thực hiện gọi hàm mã hóa tại frmClient.cs



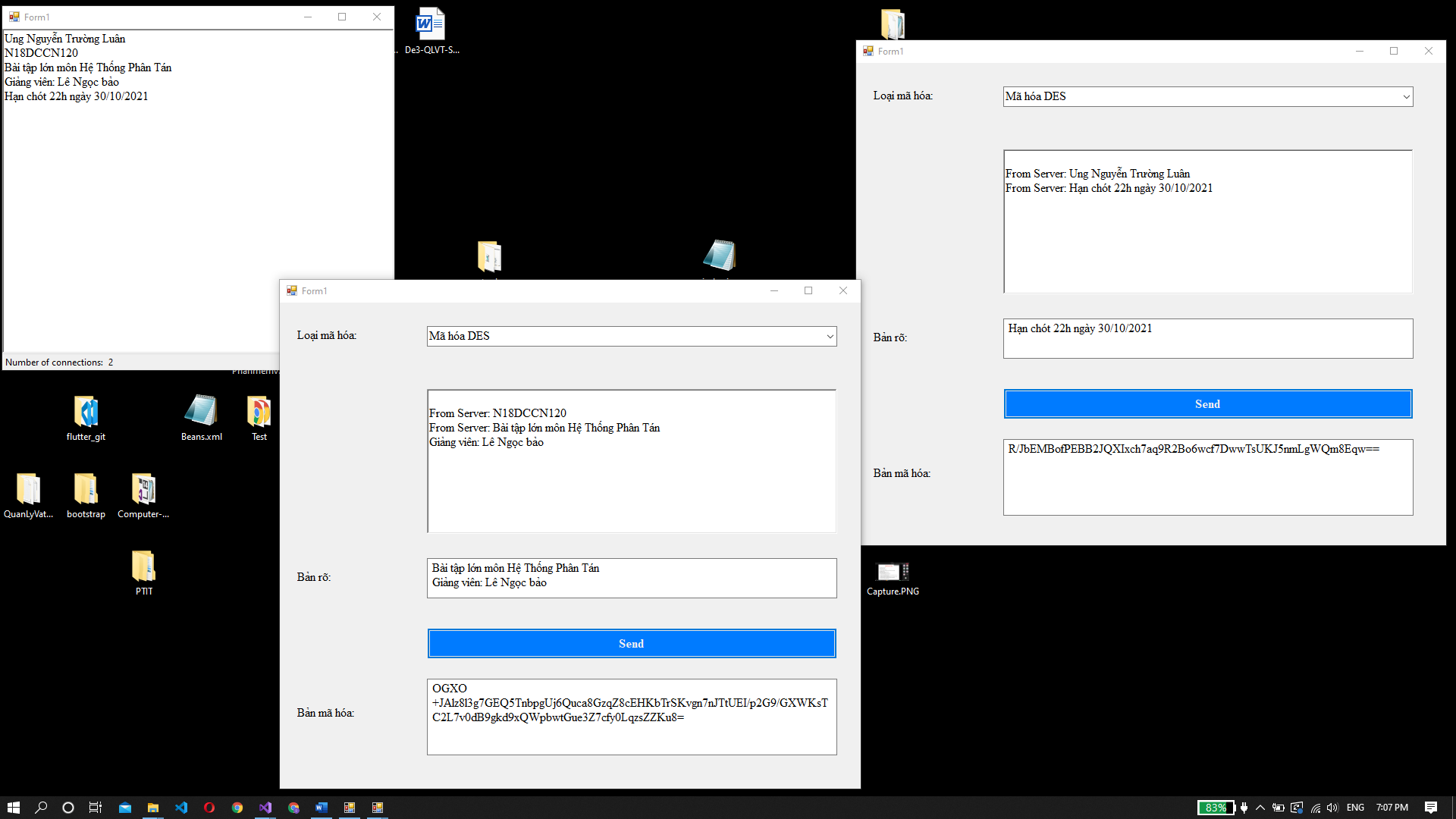
* Thực hiện gọi hàm giải mã và mã hóa tại Server



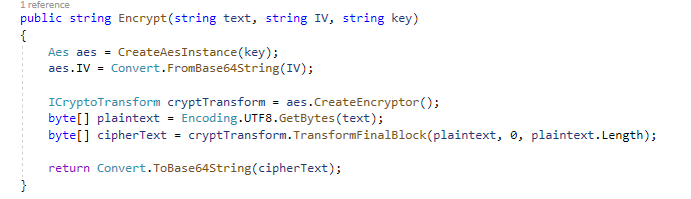
* Gửi dữ liệu từ Server về Client thông qua hàm Echo



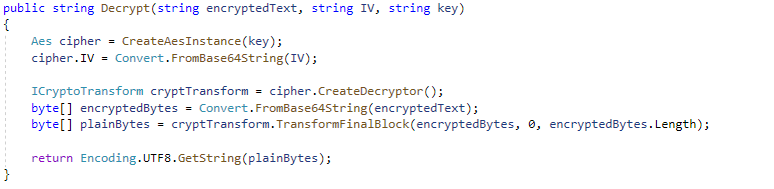
* Kết quả chạy demo mã hóa 3DES

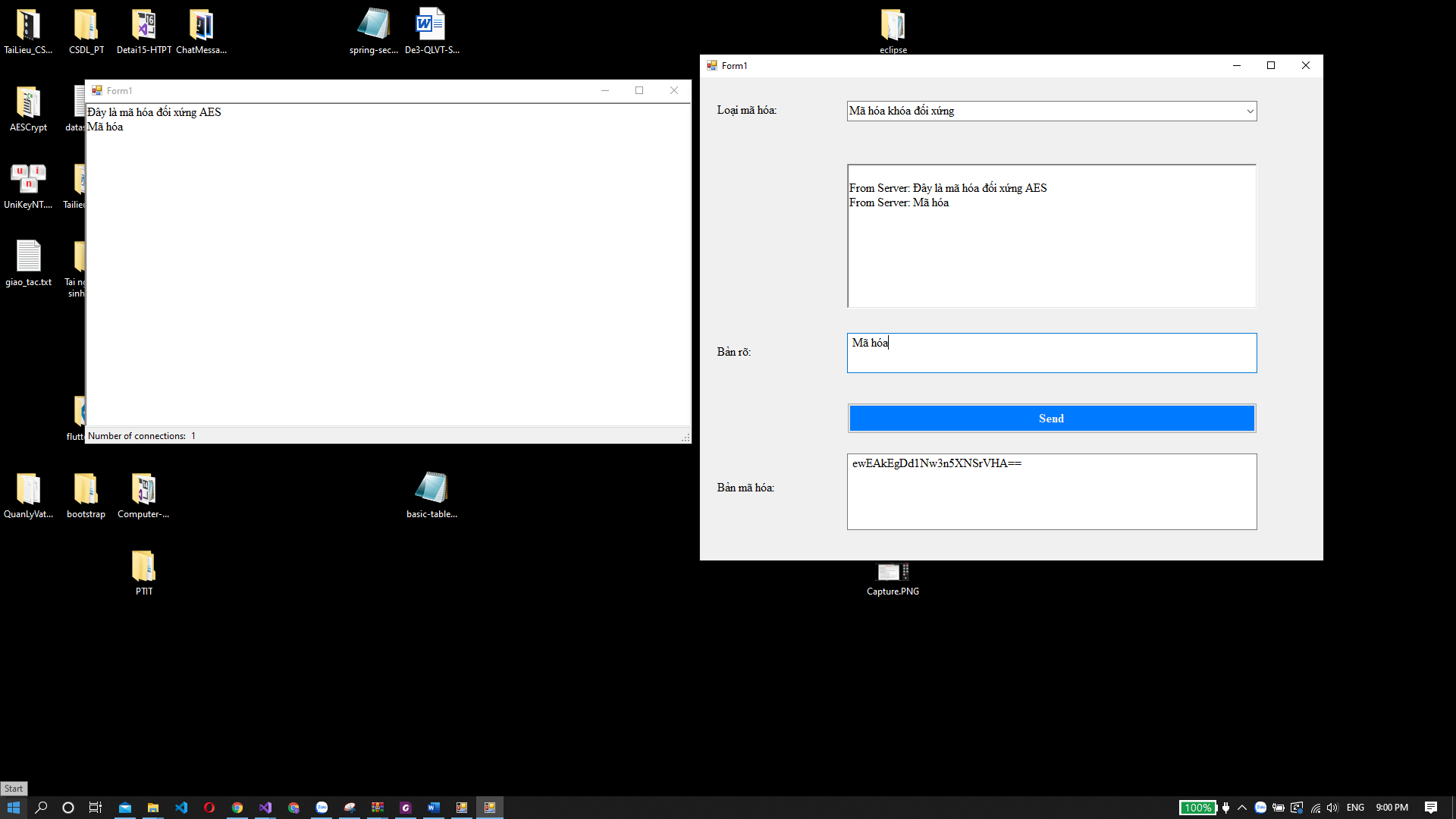


- Code mã hóa AES

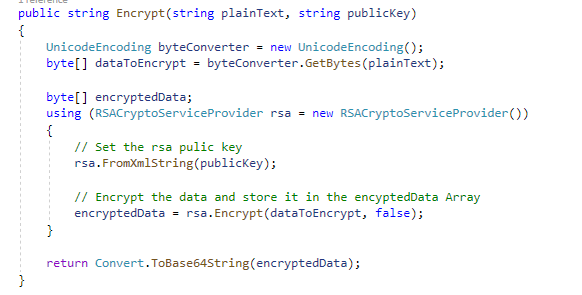


- Code giải mã AES

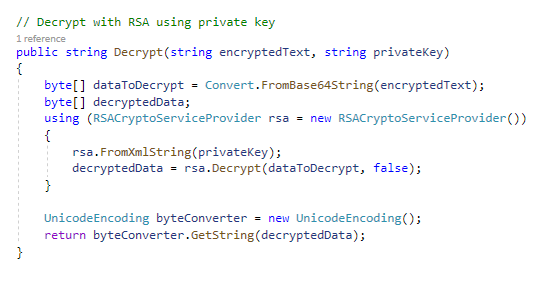


- Demo thuật toán mã hóa đối xứng AES

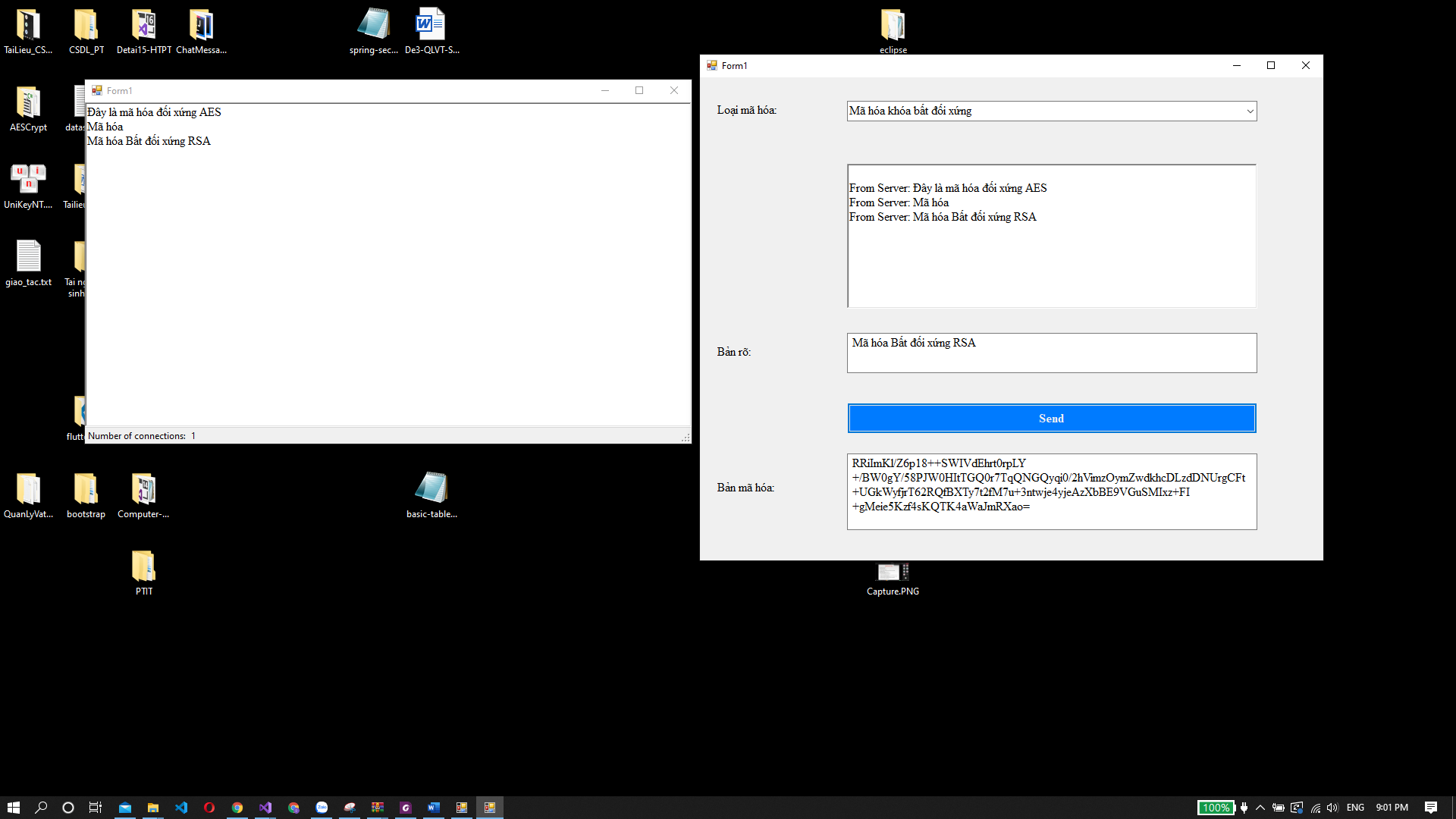
- Code mã hóa RSA



- Code giải mã RSA



- Demo thuật toán mã hóa bất đối xứng RSA



**6.Tài liệu tham khảo**

1) SnippetBank Net, C# Client/Server BroashCast Example 1, https://snippetbank.blogspot.com/2014/04/csharp-client-server-broadcast-example-1.html , truy cập ngày 20/10/2021.

2. Bảo mật thông tin, Mã hóa 3DES là gì và DES hoạt động như thế nào? <https://instagalleryapp.com/bo-mt-thong-tin/ma-hoa-3des-la-gi-va-des-hot-ng-nh-th-nao/>, truy cập ngày 22/10/2021.

3. Lê Ngọc Bảo (2021), Slide bài giảng môn học Các hệ thống phân tán, truy cập 22/10/2021.

4. Adrew S.Tanenbaum, Maarten Van Steen (2006), Book distributed systems principles and paradigms 2nd edition.

5. TS. Văn Thiên Hoàng (2021), Lập trình mạng.