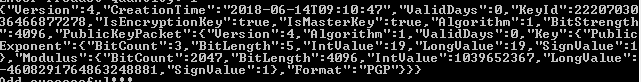
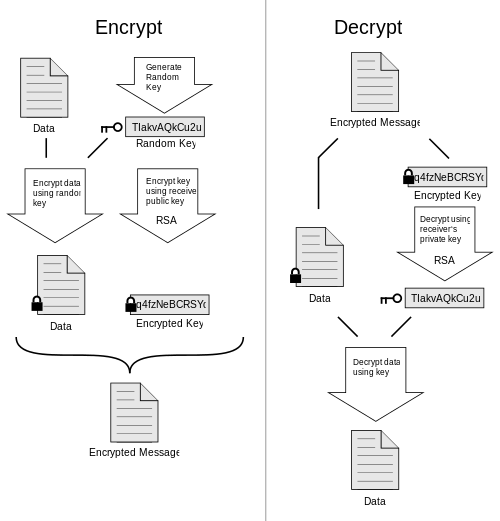
**Demo PGP (Pretty Good Privacy)**

1. Những thành phần bên trong thuật toán PGP
2. Public Key: Khóa công khai, dùng để trao đổi giữa các thành phần. AI cũng có thể nhìn thấy được public key. Dùng để mã hóa random key trước khi gửi về server

Một public khi được chuyển thành chuỗi string dưới dạng json object có dạng:



1. Private Key: Khóa bí mật, dùng để tạo ra public key và dùng để giải mã những dữ liệu bị khóa do public key.
2. PassPhare: kết hợp với Username và các thành phần khác để tạo ra private key và public key. Ngoài ra, còn được dùng trong việc xác nhận thông tin trước khi giải mã
3. Thuật toán TripleDES: mã hóa đối xứng (dùng key để mã hóa và dùng chính key đó để giải mã)
4. Thuật toán RSA: mã hóa bất đối xứng (dùng public key để mã hóa, dùng private key để giải mã)
5. Sơ đồ hoạt động:



1. Bên phía nhận dữ liệu sẽ tự tạo private key và public key khi Deploy và gửi public key sang phía gửi dữ liệu (hoặc dùng cặp key tĩnh)
2. Bên phía gửi dữ liệu sẽ tạo ra một random key và dùng key đó để mã hóa dữ liệu bằng thuật toán TripleDES
3. Tiếp theo, dùng public key để mã hóa random key bằng thuật toán RSA và gửi key đã được mã hóa cùng với gói dữ liệu đã được mã hóa sang phía nhận dữ liệu.
4. Phía nhận dữ liệu sẽ dùng private key để giải mả random key, sau đó dùng random key để giải mã dữ liệu.
5. Ví trí Key sau khi được tạo ra:

Vị trí: C:\Users\Thanh\AppData\Local\Temp\Temporary ASP.NET (hoặc tương tự)

* Search PGPPrivateKey.asc và PGPPublicKey.asc
* Được tạo mới mỗi khi run project server.

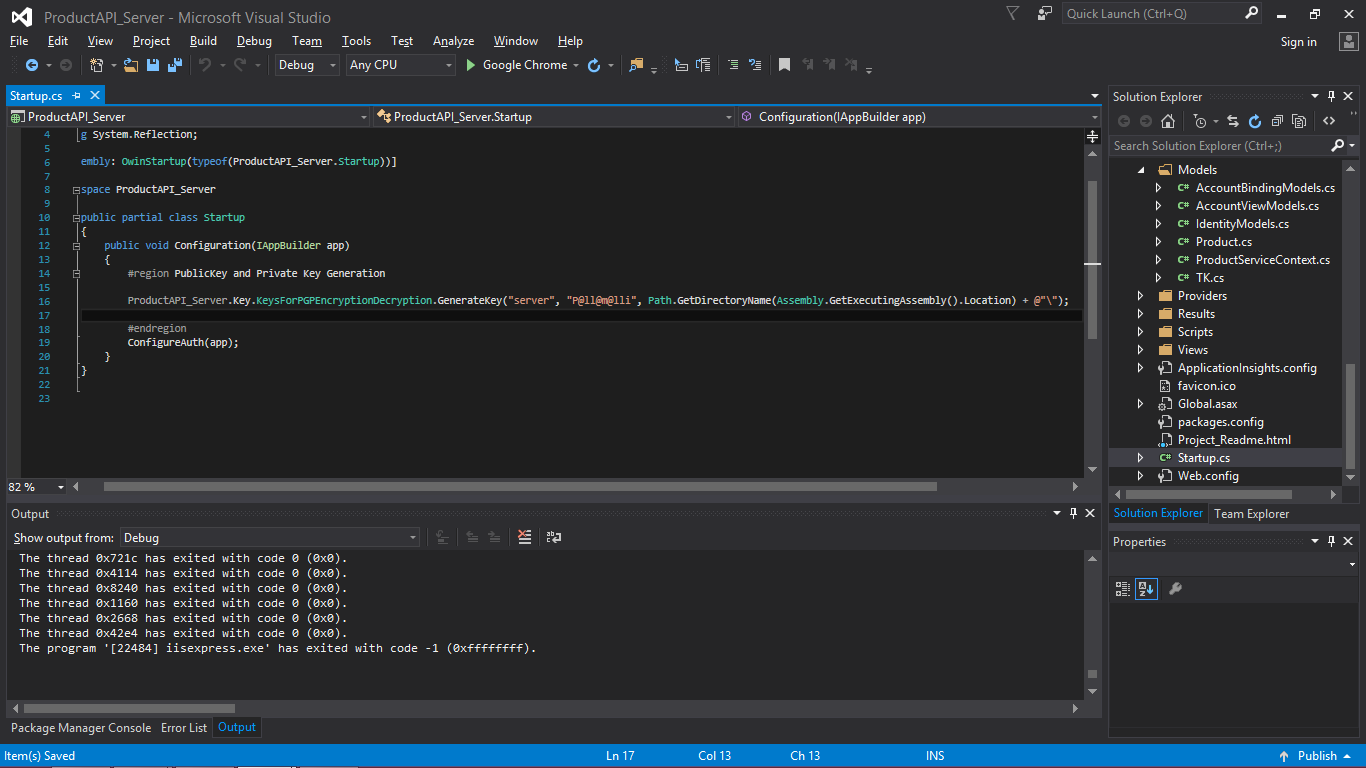
1. Mô tả demo.
2. Bao gồm 3 folder:

* ProductAPI\_Server: web project cung cấp các API để thực thi chương trình
* ProductAPI\_Client: Console app dùng để test các API
* Pretty Good Alg: => Old: PGP Project nguyên mẫu được lấy từ MSDN

=> New/Late: PGP Project đã qua chỉnh sửa + comment các tính năng. (chỉnh từ sơ đồ nguyên mẫu sang sơ đồ cải tiến)

1. Server: Khởi tạo key
2. Khởi tạo key:

* Được gọi ở file Startup.cs, khởi tạo key trước khi bắt đầu chạy app.

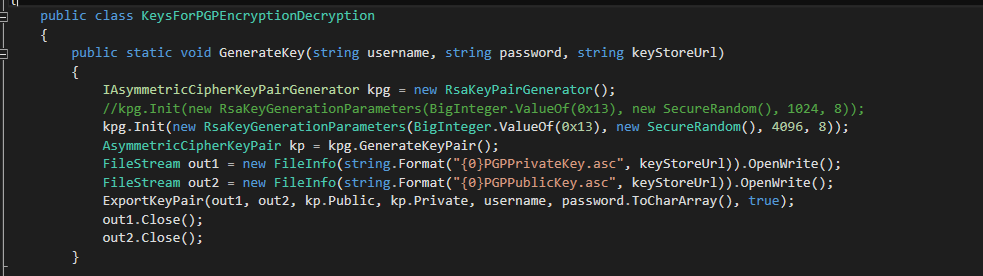


Call command: ProductAPI\_Server.Key.KeysForPGPEncryptionDecryption.GenerateKey("server", "P@ll@m@lli", Path.GetDirectoryName(Assembly.GetExecutingAssembly().Location) + @"\");

1. GenerateKey

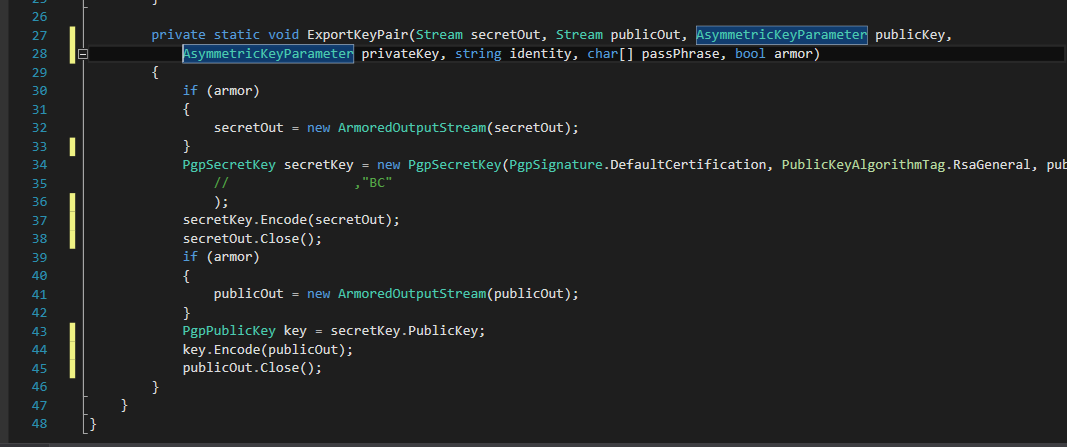
Các tham số được truyền vào: username, password, đường dẫn lưu file.

* Dùng tạo private key và public key dựa vào username và password và các thành phần random khác.
* Gọi hàm lưu chúng vào file.



Lưu ý: số 4096 là độ dài của chuỗi trong file private key. Nên truyền vào tham số la bội số của 1024. Và độ dài của private key cũng ảnh hưởng đến độ dài file của public key.

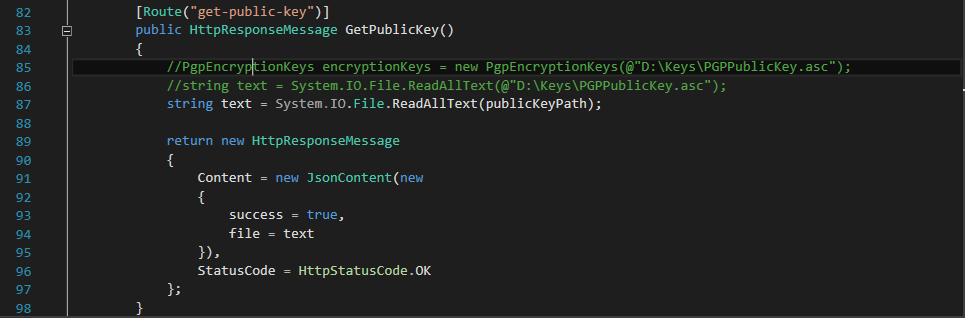
1. ExportKeyPair



* Được gọi từ GenerateKey
* Truyền về các tham số: stream của nơi save private key và public key, publickey và private key sau khi được tạo ra ở GenerateKey, username, password, và tham số phụ (armor?).
* Hàm này dùng để in private key và public key vào file nơi lưu trữ chúng.

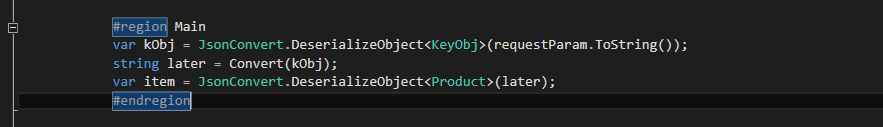
1. Server: API nhận public key

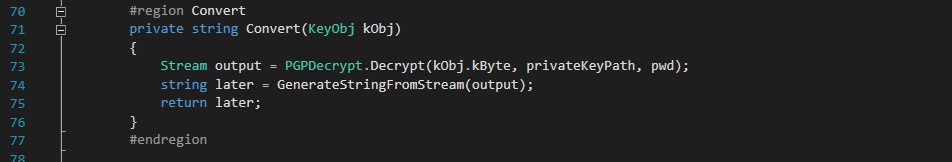
* Đường dẫn: api/acc/get-public-key
* (Năm ở file TksController.cs)



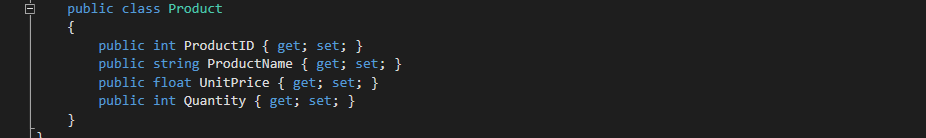
* Trả về chuổi string là thông tin của public key.
* Có thể thêm [Authorized] vào đầu hàm để chỉ có thể gọi được hàm này sau khi đã Authorized.

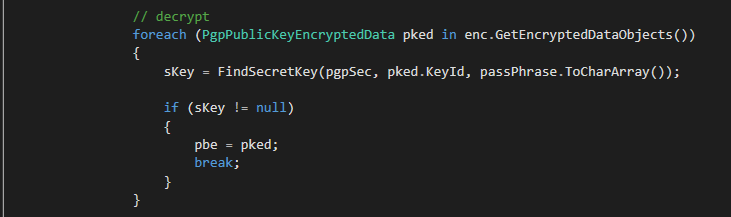
1. Server: Nhận dữ liệu sau khi mã hóa và giải mã (Nẳm ở file ProductController.cs





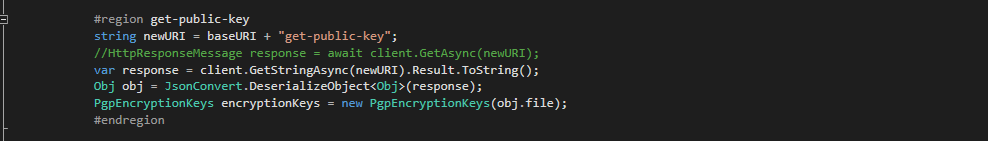




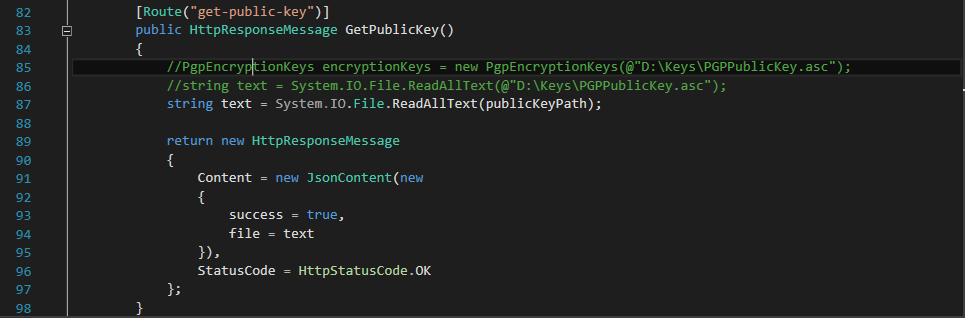


* Dữ liệu được chuyển từ client sang server dưới dạng 1 Json object KeyObj với giá trị byte[] được đặt trong parameter kByte.
* Sau đó phần data được giải mã sẽ được lưu trữ trong OutputStream output khi đưa đúng private key ứng với public key đã mã hóa và password tạo ra chính private key và public key đó.
* Quá trình giải mã: Dùng private key + password để tìm giải mã và tìm ra random key (secret key), sau đó sẽ dùng key đó để giải mã dữ liệu.
* Chuyển từ outputStream sang chuỗi Json để có thể chuyển nó về object ban đầu (quá trình mã hóa được viết ở dưới)

1. Client: get public key and encrypt data:

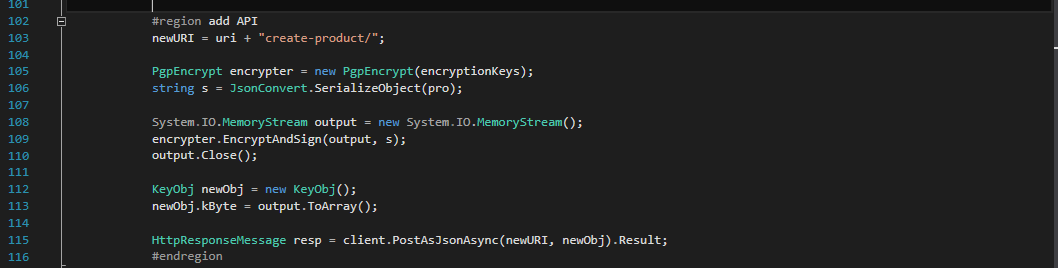


Gọi API để lấy public key dưới dạng một json.

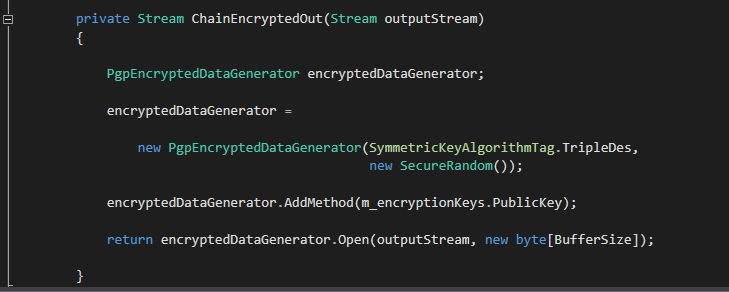




(dùng chuổi string ở trong parameter file đó để tạo public key)

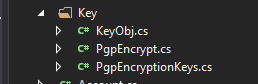






* Chuyển object sang chuỗi json => tạo random key => dùng random key mã hóa chuỗi json đó => Dùng public key mã hóa random key => Bỏ tất cả vào một object mới => gửi đi

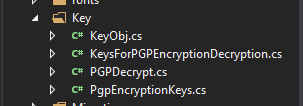
**Lưu ý:**



Object KeyObj: Chứa data trước khi giải mã dưới dạng byte[]

PgpEncrypt: mã hóa dữ liệu

PgpEncryptionKeys: Tạo public từ chuỗi string nhận được từ việc gọi api.



KeysForPGPEncryptionDecryption: Tạo 2 key.

Object KeyObj: Chứa data trước khi giải mã dưới dạng byte[]

PgpEncrypt: mã hóa dữ liệu

PgpEncryptionKeys: Tạo public từ chuỗi string nhận được từ việc gọi api.

**Các thành phần phụ cần lưu ý:**

