Croitoru Alexandru-Razvan
Anul III, Ingineria Sistemelor, Grupa 1.2

Criptare mesaj folosind ASP.NET MVC4 (Rijndael + RSA)

I. INTRODUCERE

ASP.NET prin MVC4 a devenit una dintre cele mai raspandite modalitati de a crea aplicatii WEB in Cloud.

Tehnologia ASP.NET foloseste urmatoarea structura “model-view-controller” pentru a implementa cat mai eficace atat front-end-ul , cat si back-end-ul unei aplicatii WEB de top.

Fisierul in care se afla informatia necriptata se numeste ***"Message.txt"***, iar fisierul in care se va cripta informatia dorita se numeste ***"Message.enc"***. Fisierul care va contine cheia publica RSA se numeste ***"PublicKey.txt"***.

II. IMPLEMENTARE

Programul a fost creat cu ajutorul softului Microsoft Visual Studio 2017 și a fost realizat în C#.

Au fost implementate 3 metode importante: crearea unui mesaj , criptarea acestui mesaj insotita de decriptarea acestuia. Daca se accesează aplicația, puteți vedea că se va deschide o pagina web interactiva, unde se vor putea vizualiza aspectele prezentate anterior!

Explicarea codului: In spatele acestui program scris in C# exista urmatoarea structura:

Se iau datele introduse in `textarea` si se transmit unui Response, care impreuna cu aceste „string-uri” formeaza mesajul „ .txt ”, `Message.txt`. Acesta din urma, va fi criptat prin modalitatea RijndaelManaged.

Aceasta modalitate foloseste o cheie asimetrica prin care se cripteaza si se decripteaza informatia. In acest program, s-a folosit doar modalitatea de criptare.

Informatia criptata, cheia si IV sunt toate salvate intr-un FileStream, la care ne vom referi prin pachetul de criptare.

Acest pachet are urmatorul format:

- Lungimea Key , bytes: 0 – 3
- Lungimea IV, bytes: 4 – 7
- Cheia criptata
- IV
- Textul criptat

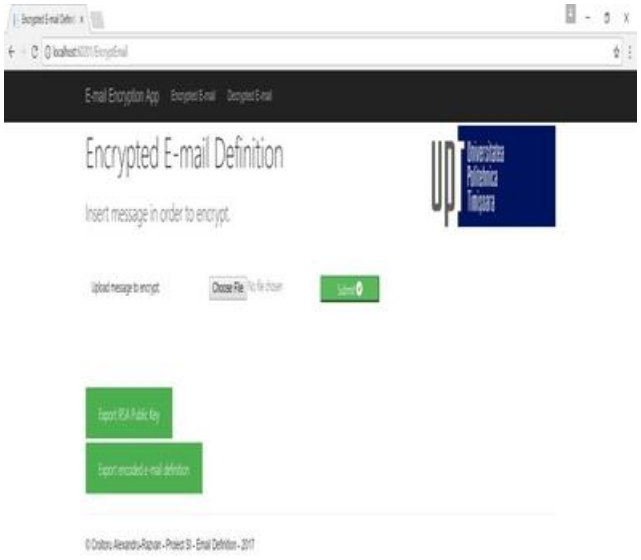
A. *Criptarea textului*

1. Se creeaza un algoritm simetric RijndaelManaged pentru a cripta informatia
2. Se creeaza un RSACryptoServiceProvider pentru criptarea cheii RijndaelManaged
3. Se foloseste un CryptoStream pentru citirea si criptarea FileStream-ului al fisierului sursa, in blocuri de bytes, catre o destinatie tip FileStream, pentru mesajul criptat.
4. Se determina lungimea cheii criptate si a IV si se creeaza vectori byte cu lungimea acestora.
5. Se scriu cheia, IV si lungimea acestora in pachetul de criptare.

B. Exportarea si importarea cheii publice si a celei private.

Exportarea cheii publice este folosita pentru a permite si altor utilizatori sa poata cripta in continuare mesaje catre destinatarul care are cheia privata. Acesta cheie este de fapt cheia publica de RSA. Cheia privata va fi trecuta in back-end, unde va fi transmisa utilizatorului care doreste sa observe procesul complet de criptare si decriptare. Un exemplu de criptare este cel in care un utilizator ofera cheia publica unui altuia pentru a putea cripta fisiere pentru ei, urmand ca doar ei apoi sa poata decripta, deoarece au cheia privata. Utilizatorii care au cheia privata pot doar cripta, nu si decripta, deoarece acestia nu au toti parametrii RSA!

Modalitatea cea mai buna in ASP.NET MVC4 pentru a schimba cheia privata este accea de File Sharing prin Azure. Aceasta modalitate implica salvarea fiecarei chei private intr-o baza de date, in care se vor face query-uri pentru a verifica care cheie privata corespunde carui destinatar, cu ajutorul cheii publice.



III. INTERFAȚĂ ȘI MOD DE UTLIZARE

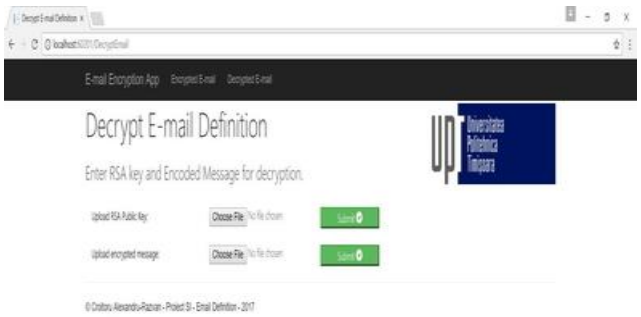
Se poate observa că are o interfață foarte ușoară de utilizat.

Se deschide tabul de E-mail Encryption App in care se introduc datele pentru criptare in campurile Head, Content si Footer.

Se apasa apui pe creearea mesajului txt „ Message.txt”, de asemenea se poate previzualiza e-mail-ul in format PDF, prin apasarea butonului Preview PDF E-mail.

Urmatorul pas este acela de Encrypted E-mail. In acest pas se introduce fisierul creat anterior „Message.txt” in campul pentru Upload message to be encrypted. Apoi se va descarca cheia publica RSA cu ajutorul butonului Export RSA Public Key. Nu in ultimul, rand se va apasa pe butonul de Export Encoded Message, pentru a descarca mesajul criptat.

Ultimul pas este acela de Decrypted E-mail, in care se urmareste decriptarea fisierului creat mai sus. Acest lucru se va putea face prin incarcarea cheii publice RSA, impreuna cu mesajul codat anterior. Rezultatul va fi acela de a descarca mesajul decriptat cu ajutorul cheii publice si a celei private, deoarece scopul este acela de a putea previzualiza cum se desfasoara acest proces de criptare/decriptare.



Bibliografie

[1] https://en.wikipedia.org/wiki/ASP.NET_MVC
[2] https://msdn.microsoft.com/en-us/library/bb397867(v=vs.110).aspx
[3] http://security.ittoolbox.com/documents/aes-vs-rsa-13016
[4] http://www.securitatea-informatiilor.ro/solutii-de-securitate-it/algoritmul-de-criptografie-rsa/