**Assignment: Chapter 3 Encryptie Tool**

Algemene werking van het document “assignment”:

* De grijze tekst maakt geen deel uit van het eindverslag! Deze tekst is enkel ter verduidelijking van de opdracht. Vervolledig het gevraagde en verwijder de grijze tekst voor het inleveren van het rapport!
* Groene tekst moet ingevuld worden door jouw persoonlijke data of oplossing.

|  |  |
| --- | --- |
| Team nummer:  *2 PRO\_A\_10* | Teamleden:   * Achternaam Naam 1 PRO X * Achternaam Naam 2 PRO X * Achternaam Naam 3 PRO X * Milan Posman 2PROF |

→ Vul teamnummer en teamleden aan in deze tabel.

Tijdsraming Chapter 3 protecting a secret

Vul onderstaande tijdsraming in als controle van je teamwerk. Elk teamlid noteert hoe lang hij/zij aan elke deelopdracht heeft gewerkt.   
Zorg dat het werk evenredig verdeeld wordt! Let ook op dat niet steeds dezelfde teamleden dezelfde type deelopdrachten maken. Niet elke deelopdracht is even moeilijk!

De tabel pas je aan naargelang de opdracht. Dit kan gebruikt worden als basis.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Teamlid | AES | RSA | Layout | Totaal |
| Teamlid 1 | ... min | ... min |  | ... min |
| Teamlid 2 | ... min | ... min |  | ... min |
| Teamlid 3 | ... min | ... min |  | ... min |
| Milan Posman | 9 h | 5 h | 30 min | 14 h 30 min |

Indien van toepassing → Reden van onevenwichtige verdeling:

Evaluatie en feedback

* Onder dit item wordt mogelijks door de lectoren feedback geplaatst (via een opmerking in blackboard).
* Indien nodig noteer je hier zelf opmerkingen.
* Deze opdracht is verplicht en telt mee voor het eindcijfer PE
* Beide delen in 1 document indienen op blackboard (pdf formaat)

1. **Encryptie Tool**

Maak een WPF applicatie dat AES en RSA encryptie kan uitvoeren. Gebruik hiervoor de namespace System.Security.Cryptography van Microsoft.

Het doel is om de tool sleutels te laten genereren om er vervolgens tekst en afbeeldingen mee te encrypteren en decrypteren.

* 1. **AES encryptie**

Opdracht gemaakt door: Naam teamlid/leden

1.1.1 Als gebruiker kan je een symmetrische sleutel genereren voor het AES algoritme. De  
 sleutel voor het AES algoritme is tweeledig: er is een sleutel en een initialisatievector.   
 Beide worden opgeslagen als een base64 string in een bestand.

Welke rol speelt de initialisatievector ?

1.1.2 Als gebruiker kan ik een sleutel selecteren om een encryptie mee uit te voeren.

1.1.3 Als gebruiker kan ik een sleutel selecteren om een decryptie mee uit te voeren.

1.1.4 Als gebruiker kan ik tekst ingeven in een TextBox om later te encrypteren.

1.1.5 Als gebruiker kan ik een txt document selecteren om later te encrypteren.

1.1.6 Als gebruiker kan ik een txt document selecteren om te decrypteren.

1.1.8 Als gebruiker kan ik op een encrypteer-knop klikken om het encryptie proces te   
 starten.

1.1.9 Als gebruiker kan ik op een decrypteer-knop klikken om een decryptie proces te   
 starten.

1.1.10 Als gebruiker kan ik een titel en een pad kiezen om de ciphertext in op te slaan die   
 geproduceerd is na encryptie. De ciphertext wordt als een base64 string opgeslagen   
 in het bestand.

1.1.11 Als gebruiker kan ik een titel en bestand kiezen om de nieuwe plain text in op te slaan   
 die geproduceerd is na decryptie.

1.1.12 Behandel CryptographicExceptions en waarschuw de gebruiker bij het gebruik van   
 verkeerde keys.

**Extra**

1.1.12 Als gebruiker kan ik een afbeelding selecteren van een bepaalde extensie om te   
 encrypteren.

Welke afbeelding extensie hebben jullie gekozen voor jullie applicatie?

1.1.13 Als gebruiker kan ik een keuze maken om een ciphertext te decrypteren als een   
 afbeelding van de gekozen extensie.

* 1. **RSA encryptie**

Opdracht gemaakt door: Naam teamlid/leden

1.2.1 Als gebruiker kan je asymmetrische sleutels genereren voor het RSA algoritme.   
 De sleutels voor het RSA algoritme mogen opgeslagen worden als XML files.

1.2.2 Als gebruiker kan ik een public key selecteren om een encryptie mee uit te voeren.

1.2.3 Als gebruiker kan ik een private key selecteren om een decryptie mee uit te voeren.

1.2.4 Als gebruiker kan ik tekst ingeven in een TextBox om later te encrypteren.

1.2.5 Als gebruiker kan ik een txt document selecteren om later te encrypteren.

1.2.6 Als gebruiker kan ik een txt document selecteren om te decrypteren.

1.2.8 Als gebruiker kan ik op een encrypteer-knop klikken om het encryptie proces te   
 starten.

1.2.9 Als gebruiker kan ik op een decrypteer-knop klikken om een decryptie proces te   
 starten.

1.2.10 Als gebruiker kan ik een titel en een pad kiezen om de ciphertext in op te slaan die   
 geproduceerd is na encryptie. De ciphertext wordt als een base64 string opgeslagen   
 in het bestand.

1.2.11 Als gebruiker kan ik een titel en bestand kiezen om de nieuwe plain text in op te slaan   
 die geproduceerd is na decryptie.

1.2.12 Behandel CryptographicExceptions en waarschuw de gebruiker bij het gebruik van   
 verkeerde keys.

**Extra**

1.2.12 Als gebruiker kan ik een afbeelding selecteren van een bepaalde extensie om te   
 encrypteren.

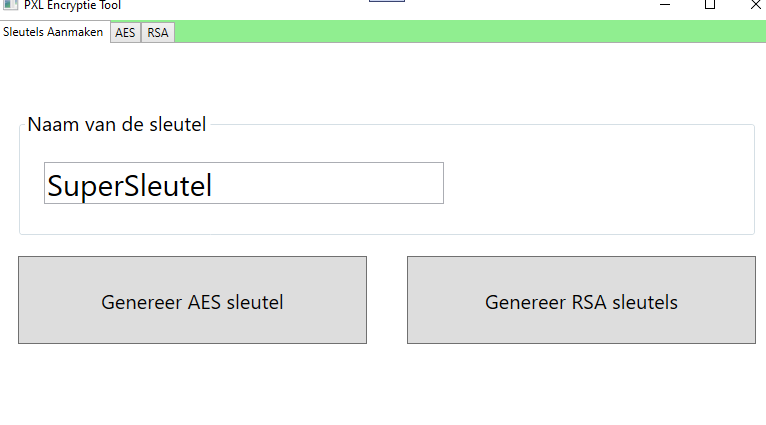
Welke afbeelding extensie hebben jullie gekozen voor jullie applicatie?

1.2.13 Als gebruiker kan ik een keuze maken om een ciphertext te decrypteren als een   
 afbeelding van de gekozen extensie.

1. **Layout**

Maak het programma gebruiksvriendelijk. Je kan via een dialoogvenster afbeeldingen of tekstbestanden inladen ofwel via een drag en drop functionaliteit.

De layout en de gebruikersinterface kunnen het encryptie- en decryptie proces verduidelijken naar de eindgebruiker toe. Zorg er voor dat het proces intuïtief is om te volgen.



*De afbeelding van het voorbeeld mogen jullie verwijderen in jullie uiteindelijke verslag. Jullie eigen layout mag uiteraard gedocumenteerd worden in het verslag.*

* 1. **User interface**

Opdracht gemaakt door: Naam teamlid/leden

2.1.1 Zorg er voor dat de gebruikersinterface duidelijk communiceert hoe een gebruiker de   
 verschillende functionaliteiten van het programma kan benutten. Je kan hiervoor  
 gebruik maken van tabs, meerdere vensters, meerdere layouts, een duidelijke   
 opdeling in een grid.

Voor welk design hebben jullie gekozen en waarom?

* 1. **Gebruiksvriendelijkheid**

Opdracht gemaakt door: Naam teamlid/leden

2.2.1 Let er op dat de applicatie een eenvoudige manier heeft om bestanden te encrypteren en decrypteren. Je kan hiervoor gebruik maken door een ingebouwde file picker, een dialoogvenster of een drag en drop functionaliteit.  
  
 Voor welke functionaliteit hebben jullie gekozen en waarom?