Tinpro01-8 Practicumopdracht 3

W. Oele

30 mei 2016

Inleiding

In deze opdracht ga je een tekstbestand versleutelen middels het algoritme van Vernam (ook wel bekend als de one time pad). Uiteraard moet een versleuteld bestand ook weer ontsleuteld kunnen worden. We schrijven daarom twee programma' s:

encrypt.hs

Dit programma:

- leest het te versleutelen tekstbestand in.
- genereert op basis van een randomgenerator een sleutel.
- versleutelt het bestand en schrijft de versleutelde tekst weg naar een nieuw bestand.
- schrijft de sleutel weg in een apart `.key` bestand.

decrypt.hs

Dit programma:

- leest het versleutelde bestand in.
- leest de sleutel in.
- ontsleutelt de versleutelde tekst.
- schrijft het resultaat weg naar een apart bestand.

Aanwijzingen

Hanteer bij het maken van deze opdracht een stelselmatige manier van denken: benoem de individuele onderdelen van het programma en concentreer je op het volledig werkend hebben van dat onderdeel. Zo zitten er in het programma `encrypt.hs` de volgende "onderdelen":

Randomgeneratie Gebruik hiervoor de library `System.Random` en denk eraan dat voor random generatie aan i/o gedaan moet worden. Een randomwaarde zit derhalve per definitie in het `IO` datatype.

Bestand inlezen Gebruik hiervoor functies uit de library `System.IO`. Ook hier geldt dat het inlezen van een bestand een i/o actie is en je de inhoud van een bestand in een `IO` datatype krijgt aangeboden.

Versleutelen Versleutelen is bij het Vernam algoritme een eenvoudige bitsgewijze operatie. De library `Data.Bits` heeft daarvoor geschikte functies.

Opbouw

Verdeel het versleutelprogramma in losse onderdelen:

- Een functie die een bestand inleest en derhalve monadisch van aard is.
- Een functie die een lijst randomwaarden van een bepaalde lengte genereert en derhalve monadisch van aard is.
- Een functie die voor de feitelijke versleuteling zorgt. Deze is *niet* monadisch.
- Een functie die bovenstaande drie functies combineert.