Fakulta riadenia a informatiky

**SEMESTRÁLNA PRÁCA**

Pokročilé objektové technológie

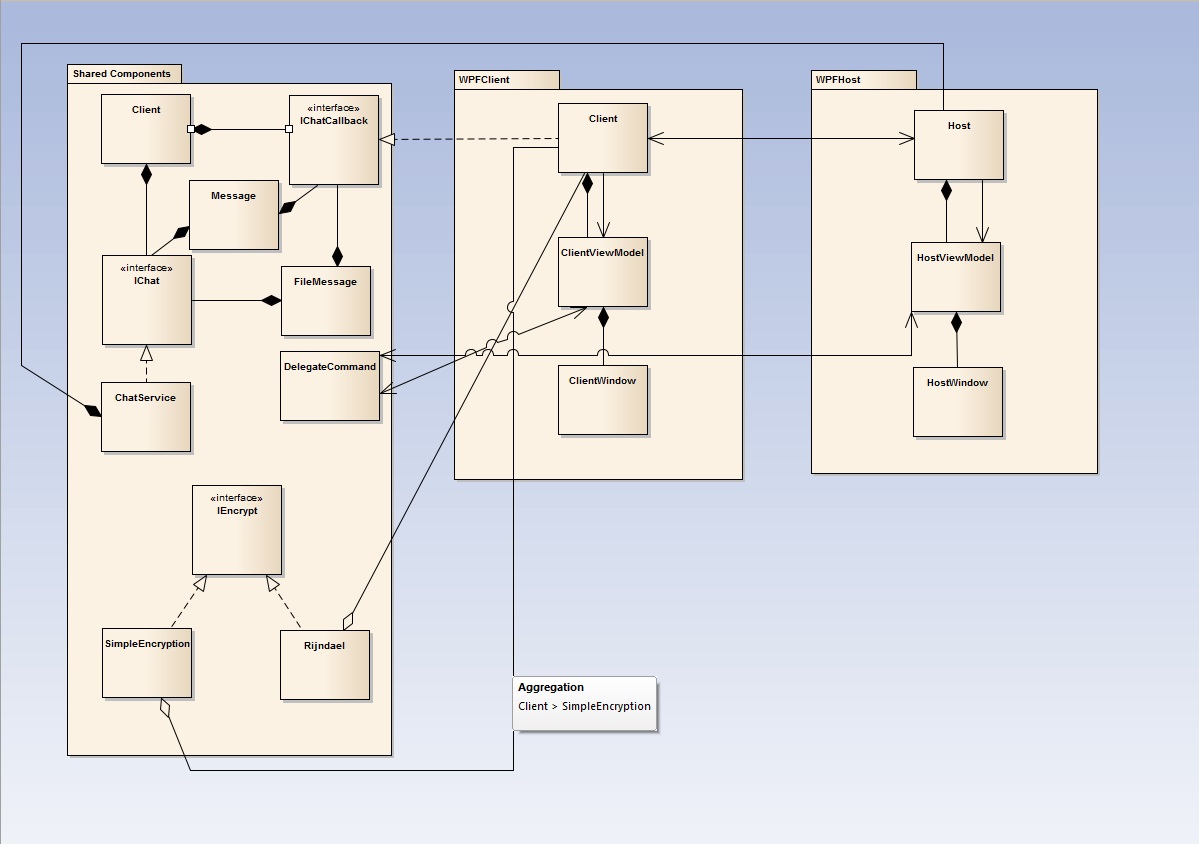
Encrypted Chat

František Kajánek, 5ZZS15

# Zadanie

Ako zadanie som si zvolil realizáciu chatu(p2p alebo client-server), ktorý by poskytoval ochranu proti odchytávaniu. Toto som chcel dosiahnuť šifrovaním správ medzi osobami v chate. GUI knižnica, ktorú som zvolil pre túto úlohu bola WPF s MVVM. Správy sa budú ukladať do SQL databázy.

# UML diagram



Tento UML diagram tried znázorňuje základné vzťahy medzi použitými triedami.

# Použité technológie

* Implementácia chatu cez internet zo stránky <http://www.codeproject.com/Articles/25261/A-WCF-WPF-Chat-Application>
* MS SQL Databáza prostredníctvom Entity Framework 6
* .Net Framework 4.6.1
* WPF s MVVM
* Rijndael algoritmus na šifrovanie z Window.System.Cryptography, http://stackoverflow.com/questions/1629828/how-to-encrypt-a-string-in-net

# Požiadavky na systém

* .Net Framework 4.6.1
* Sieťové pripojenie medzi klientom a serverom
* Microsoft Windows

# Problémy a riešenia

Jeden z prvých problémov riešenia tohto zadania bolo nájdenie dobrého úvodu do WCF komunikácie. Zistil som, aké všetky rôzne stavy môžu nastať pri komunikácií na sieti a zistil som, že ako začiatočníkovi bude potrebný nejaký obsiahly príklad. Preto som sa rozhodol začať pracovať s už fungujúcim chatom zo stránky Codeproject, kde boli pokryté všetky základy komunikácie po sieti.

Keď som mal tento Codebase, bolo treba prepísať úplne celé GUI správanie aby bolo konformné s MVVM patternom. Tu som narazil na niekoľko limitácií Bindingov vo WPF. Napríklad nie je možné mimo codebehind dať Focus na daný prvok alebo registrovať stlačenie tlačidiel počas písania v TextBoxe bez použitia rozšírení, napr. MVVM Light. Obišiel som to poslaním Action objektov z codebehindu (inštalácia frameworkov vs. 5 riadkov kódu).

Následne som implementoval šifrovanie stringov, nadizajnoval som interface, a podľa neho naimplementoval svoju symetrickú šifru a jedno z .net frameworku. Jediný problém bol správne transformovanie stringu na byte array, + bolo treba dodržať aby vstupný kľuč pre Rijndael je násobok 16ky.

Ako databázu na implementovanie som pôvodne zvolil Mysql, keďže ju doma bežne používam. Problém nastal keď update Connectoru a Mysql for Visual Studio pre Entity framework corruptol inštaláciu VS2013, znemožnil správnu reinštaláciu a iné. Preto som pokračoval v VS2015 a použil MS SQL cez Entity framework 6.

Veľmi zaujímavý bug bol, keď som používal SelectedIndex aj SelectedItem z ComboBoxu vo WPFku. Na každý z nich bol nabindovaný property. Keďže som v spracovávaní indexu používal aj item, zistil som že tieto properties sa neupdatujú naraz ale postupne, a prvý sa spracúva SelectedIndex. Race Conditions tam kde to človek nečaká.

# Záver

Výsledná implementácia je funkčná aj použiteľná na bežné chatovanie. Až na databázu funguje program tak ako som mal v úmysle. Jedna z vecí, ktorá sa ale nedostala do finálnej verzie je kombinovanie šifier. Ako možné rozšírenia by bolo teda použitie rôznych šifier v rôznych poradiach (konfigurovateľné v GUI). Taktiež pridanie emotikonov a ich vizualizácia. Nakoniec by bolo taktiež možné pridanie hesla k pripojeniu na server a umožniť aby na jednom servri bolo viac chatovacích miestností (na to by bolo ale taktiež treba prispôsobiť ukladanie do databázy).