Zadání maturiní práce z informatiky

Štěpán Kovačič

Leden 2024

Maturitní projekt - program na šifrování a dešifrování podle RSA algoritmu

1 Motivace

Existuje mnoho funkčních kódů zabývajících se RSA, které se dají v praxi použít. Jsou rychlé, komplikované a využívají různých triků jak být co nejvíce efektivní a elegantní.

Problém s těmito kódy je ten, že není lehké pochopit jejich základní logiku, matematiku v pozadí a princip o který se všechny tyto kódy opírají.

Cílem této práce je vytvořit program, který bude dobře dokumentovaný, komentovaný a vysvětlený. Nebude využito žádných zásadních programátorských kliček. Hlavní je pochopit jak kód funguje a proč.

2 Hlavní myšlenka

RSA (iniciály autorů Rivest, Shamir, Adleman) je šifra s veřejným klíčem, jedná se o první algoritmus, který je vhodný jak pro podepisování, tak šifrování. Používá se i dnes, přičemž při dostatečné délce klíče je považován za bezpečný. [Wikipedie]

Vytvořím kód, který bude šifrovat a dešifrovat pomocí RSA.