Kryptografie (KRY)
Implementace a prolomení RSA

Daniel Konečný (xkonec75)
Vysoké učení technické v Brně
Fakulta informačních technologií

28. dubna 2022

1 Nalezení prvočísel p a q

Je využito postupu generování vysokého čísla a následné testování, zda se jedná o prvočíslo. U generovaného čísla je zajištěno, že jeho nejvýznamější bit má hodnotu 1, nastavením tohoto bitu. K otestování prvočíselnosti je využit Solovay-Strassen test s pevně nastaveným počtem iterací na 50. Tím je zajištěno, že se bude jednat o prvočíslo s velmi vysokou pravděpodobností.

2 Další implementační detaily

Jak pro hledání největšího společného dělitele (GCD), tak pro výpočet modulárního inverzu byla zvolena iterativní metoda místo rekurzivní, aby nedošlo k problémům u velmi vysokých čísel.

3 Prolomení šifry – faktorizace

Tato část projektu není implementována.