KRY
RSA

Tomáš Willaschek
xwilla00

Implementace

Ze všech bodů zadání bylo splněno:
- generování klíče,
- šifrování,
- dešifrování.

Lámání klíče implementováno není.

Veškerá implementační logika se nalézá v třídě RSA, rozdělená do patřičných metod. Pro generování klíče je použit generátor náhodných čísel z knihovny GMP. Použité algoritmy jsou implementovány většinou podle manuálu, výjimku tvoří jen Lehmannův algoritmus pro detekci prvočísla, jehož popis nebyl v manuálu dostatečný.
Veřejný exponent je generován od počáteční hodnoty 0x3, jelikož se jedná pouze o testovací implementaci RSA a vysoká bezpečnost šifrování není třeba. Zvětšíme-li však počáteční hodnotu veřejného exponentu, algoritmus lze reálně používat.
Program je schopen generovat použitelné RSA klíčet v řádu jednotek sekund.