Název práce: Diffie a Hellman si vyměňují matice nad grupovým okruhem

Autor: Romana Linkeová

Katedra: Katedra algebry

Vedoucí bakalářské práce: Mgr. Pavel Příhoda, Ph.D., Katedra algebry

Abstrakt: Diffieho-Hellmanův protokol pro výměnu klíčů není při počítání nad grupou $\mathbb{Z}_p^*$ (kde počet cifer p je alespoň 300) vykonatelný na strojích s menší výpočetní silou. Tento fakt vedl ke snaze pracovat nad jinými algebraickými strukturami s cílem snížit výpočetní a paměťovou náročnost výpočtů. D. Kahrobaei a spol. publikoval v roce 2013 návrh na pracování nad strukturou malých matic s tím, že tato modifikace nesníží bezpečnost daného protokolu. V této práci se pokusíme napadnout takto modifikovaný Diffieho-Hellmanův protokol pomocí teorie reprezentací symetrických grup.
Nejprve připomeneme základy teorie reprezentací a uvedeme obě varianty Diffieho-Hellmanova protokolu. Dále rozebereme celý útok krok po kroku a doplníme některé kroky o příklady. Později prozkoumáme bezpečnost modifikovaného protokolu proti známému útoku baby-step giant-step.

Klíčová slova: kryptografie s veřejným klíčem, reprezentace symetrických grup, Diffieho-Hellmanův protokol