



ZADÁNÍ DIPLOMOVÉ PRÁCE

Název: Asymetrický šifrovací algoritmus McEliece
Student: Bc. Vojtěch Myslivec
Vedoucí: prof. Ing. Róbert Lórencz, CSc.
Studijní program: Informatika
Studijní obor: Počítačová bezpečnost
Katedra: Katedra počítačových systémů
Platnost zadání: Do konce letního semestru 2016/17

Pokyny pro vypracování

Prostudujte asymetrický šifrovací algoritmus McEliece založený na binárních Goppa kódech. Proveďte rešerši existujících kryptoanalýz algoritmu McEliece a jeho variant. Zvažte metody zabývající se zkrácením velikosti klíče. Implementujte šifrovací a dešifrovací algoritmy a změřte jejich výpočetní časovou a prostorovou náročnost v závislosti na velikosti klíče.

Seznam odborné literatury

Dodá vedoucí práce.

L.S.

prof. Ing. Róbert Lórencz, CSc.
vedoucí katedry

prof. Ing. Pavel Tvrdík, CSc.
děkan

V Praze dne 2. února 2016