Zápisnica č. 3

Dátum: 2.10.2018

Prítomní:

- Bc. Juraj Karásek, Bc. Matej Ohradzanský, Bc. Peter Radvan a Bc. Lukáš Štrba
- Mgr. Tomáš Fabšič, PhD. a Ing. Viliam Hromada, PhD.

Chýbajúci:

- Bc. Nikoleta Furičková (*ospravedlnené)*

Program stretnutia:

- Pokračovali sme tam, kde sme skončili naposledy. Vysvetlili sme si spôsob dešifrovania v kryptosystéme McEliece.
- Nasledoval popis kvázi-cyklických matíc (QC) a stretnutie sme ukončili tvorbou kontrolnej matice H v kryptosystéme QC-MDPC McEliece.

Úlohy:

- V DP *Implementácia QC-MDPC McEliecovho kryptosystému* si máme preštudovať 1. kapitolu.

Poznámka:

Zapisovateľ: Bc. Lukáš Štrba **Overovateľ:** Bc. Peter Radvan