



Final project proposal

| | |
|---|--|
| Type | Master |
| Title | <i>Authenticated ciphers</i> |
| Supervisor | Prof. Smile Markovski |
| e-mail | smile.markovski@finki.ukim.mk |
| Department / Group | |
| Theoretical foundation of informatics | |
| Topic(s) | |
| Cryptography | |
| Project can start from | 01.04.2014 |
| Project duration | 4 months |
| Short description | |
| Authenticated ciphers are devices that simultaneously provide security and authentication of transmitted messages. The student should (1) make a survey of several publications considering the authenticated ciphering and (2) to design a new or modified authenticated cipher. The first part is an individual activity of the student; the second part should be a joint work with the supervisor. | |
| Results and assessment | |
| A written master thesis and publication(s) of the new results with a presentation. | |
| Other (additional) information | |
| | |