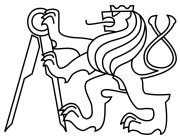
CZECH TECHNICAL UNIVERSITY IN PRAGUE
FACULTY OF INFORMATION TECHNOLOGY



# ASSIGNMENT OF BACHELOR'S THESIS

| | |
|---|---|
| **Title:** | Timing Attack on the RSA Cipher |
| **Student:** | Martin Andrýsek |
| **Supervisor:** | Ing. Jiří Buček |
| **Study Programme:** | Informatics |
| **Study Branch:** | Information Technology |
| **Department:** | Department of Computer Systems |
| **Validity:** | Until the end of winter semester 2018/19 |

## Instructions

Review known timing side channel attacks on RSA decryption and signing operations. Create a demonstration application that will perform timing attack on RSA in order to determine the private key. The application will be used in courses on cryptology and computer security as a part of laboratory exercises. Consider an attack on a local computer or over the network and evaluate its time complexity.

## References

Will be provided by the supervisor.

prof. Ing. Róbert Lórencz, CSc.
Head of Department

prof. Ing. Pavel Tvrdík, CSc.
Dean

Prague March 7, 2017