

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Jiří VÁVRA**
Osobní číslo: **A09663**
Studijní program: **B 3902 Inženýrská informatika**
Studijní obor: **Informační a řídicí technologie**

Téma práce: **Off-the-record protokol pro výměnu textových zpráv**

Zásady pro vypracování:

1. Vypracujte literární rešerši na dané téma.
2. Popište principy šifrování pomocí OTR.
3. Zjistěte současný stav užívání OTR.
4. Napište knihovnu, případně aplikaci OTR protokolu v C++ nebo JavaScriptu.

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **VONDRUŠKA, Pavel. Kryptologie, šifrování a tajná písma. Albatros, 2006. ISBN 8000018888.**
2. **MOLDOVYAN Nick, MOLDOVYAN Alex. Innovative Cryptography, Second Edition. Cengage Charles River Media, 2007. ISBN 9781584504672.**
3. **DENIS, Tom St. Cryptography for Developers. Syngress Publishing. 2007. ISBN 9781597491044.**
4. **PRATA, Stephen, Mistrovství v C++, 3., aktualiz. vyd., Computer press, 2007, ISBN 9788025117491.**
5. **GOLDBERD, Ian et al. Off-the-Record Messaging [online]. [cit. 2012-06-02]. Dostupné z: <http://www.cypherpunks.ca/otr/>**

Vedoucí bakalářské práce:

Ing. Roman Šenkeřík, Ph.D.

Ústav informatiky a umělé inteligence

Datum zadání bakalářské práce:

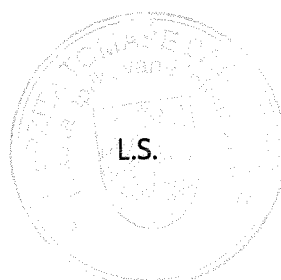
24. února 2012

Termín odevzdání bakalářské práce:

8. června 2012

Ve Zlíně dne 24. února 2012

prof. Ing. Vladimír Vašek, CSc.
děkan



prof. Ing. Vladimír Vašek, CSc.
ředitel ústavu