MUNI

Příloha č. 12 směrnice MU Habilitační řízení a řízení ke jmenování profesorem

HODNOCENÍ PŘEDNÁŠKY PRO ODBORNOU VEŘEJNOST

Masarykova univerzita	
Fakulta	Fakulta informatiky
Obor řízení	Informatika
Uchazeč	RNDr. Petr Švenda, Ph.D.
Datum přednášky	26. 3. 2019
Téma přednášky	Analysis and use of RSA keypair generation bias
Přítomno posluchačů (počet)	42 (viz prezenční listinu v příloze)
Pověření hodnotitelé (členové komise)	prof. RNDr. Antonín Kučera, Ph.D. prof. RNDr. Otokar Grošek, PhD doc. Dr. Ing. Petr Hanáček doc. Mgr. Jan Obdržálek, PhD.

Uchazeč vysvětlil roli generátorů náhodných čísel z pohledu syntézy šifrovacích klíčů a jejich důležitost pro prevenci útoků. Následně se zaměřil na problematiku testování kvality náhodnostních generátorů a kvality RSA klíčů. Vysvětlil použitou metodologii i získané výsledky.

Přednáška jasně prokázala skvělé pedagogické schopnosti uchazeče a také jeho vysokou odbornou erudici.

Závěr

Přednáška Petra Švendy „Analysis and use of RSA keypair generation bias“, přednesená v rámci habilitačního řízení ***prokázala*** – ~~***neprokázala***~~ dostatečnou vědeckou kvalifikaci a pedagogickou způsobilost uchazeče, standardně požadovanou v rámci habilitačních řízení v oboru Informatika.

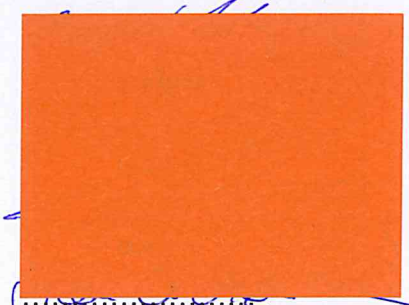
Brno dne 26. 3. 2019

Antonín Kučera

Otokar Grošek

Petr Hanáček

Jan Obdržálek



podpis