



MATEMATICKO-FYZIKÁLNÍ  
FAKULTA  
Univerzita Karlova

## Zápis o části státní závěrečné zkoušky Obhajoba diplomové práce

Akademický rok: 2020/2021

**Jméno a příjmení studenta:** Bc. Sára Vyhnalová  
**Identifikační číslo studenta:** 75926964

**Typ studijního programu:** navazující magisterský  
**Studijní program:** Matematika  
**Studijní obor:** Matematika pro informační technologie  
**ID studia:** 627527

**Název práce:** Ideal lattices in cryptography  
**Pracoviště práce:** Katedra algebry (301. • 32-KA)  
**Jazyk práce:** angličtina  
**Jazyk obhajoby:** čeština  
**Vedoucí:** Mgr. Vítězslav Kala, Ph.D.  
**Oponent(i):** doc. Mgr. Pavel Příhoda, Ph.D.

**Datum obhajoby:** 14.09.2021      **Místo obhajoby:** Praha  
**Termín:** řádný

**Průběh obhajoby:** Studentka seznámila komisi s obsahem své diplomové práce formou počítačové prezentace. Přítomný vedoucí i oponent přednesli svůj posudek. Oponent požádal studentku o vyjasnění konkrétního bodu práce, kde se používá čínská věta o zbytku. Studentka byla na tento dotaz připravena a částečně ho zodpověděla pomocí počítačové prezentace. Diskuse se dále týkala současné role kryptografie založené na mřížích a důvodů volby článku, který diplomovou práci motivoval.

**Výsledek obhajoby:** velmi dobře (2)

**Předseda komise:** prof. RNDr. Aleš Drápal, CSc., DSc. ....

**Členové komise:** doc. RNDr. Iveta Hnětynková, Ph.D. ....  
doc. Mgr. Štěpán Holub, Ph.D. ....  
doc. RNDr. Přemysl Jedlička, Ph.D. ....  
prof. RNDr. Ing. Petr Němec, DrSc. ....  
doc. Mgr. Pavel Příhoda, Ph.D. ....

doc. RNDr. Petr Somberg, Ph.D.

.....

doc. Mgr. et Mgr. Jan Žemlička, Ph.D.

.....