

Základy kryptografie

Úvodné informácie

Vyučujúci

- Meno: Tomáš Fabšič (aj prednášky aj cvičenia)
- Email: tomas.fabsic@stuba.sk
- Konzultácie po dohode emailom.

Filozofia výučby

- **Verím, že počas vášho štúdia sú pre vás najprínosnejšie tie chvíle, kedy nad študovanou látkou samostatne rozmýšľate.**
- Budem vítať, ak mi počas prednášok a cvičení budete dávať otázky.
- Budem vám odporúčať, aby ste priebežne čítali odporúčanú literatúru.
- Budem vám dávať sady úloh na riešenie. Body za riešenie týchto úloh budú tvoriť polovicu všetkých bodov, ktoré je na predmete možné získať.

Podmienky absolvovania predmetu

- Výsledná známka bude určená podľa klasifikačnej stupnice uvedenej v študijnom poriadku STU.
- Hodnotenie pozostáva z:
 - bodov získaných za riešenie súb úloh počas výučbovej časti semestra (max. 50 bodov)
 - bodov získaných zo skúšky (max. 50 bodov)
- Na úspešné absolvovanie predmetu je potrebné:
 - Získať aspoň 25 bodov za riešenie súb úloh počas výučbovej časti semestra. Študenti, ktorí nezískajú aspoň 25 bodov nebudú pripustení ku skúške.
 - Získať aspoň 25 bodov zo skúšky.
 - Získať aspoň 50 bodov dokopy.

Odporúčaná literatúra

- Predmet je založený na druhom vydaní knihy Understanding Cryptography od autorov Paar, Pelzl a Güneysu.
- Z univerzitnej siete je kniha voľne dostupná na <https://link.springer.com/book/10.1007/978-3-662-69007-9>
- Veľmi vám odporúčam si túto knihu priebežne čítať. Myslím si, že kniha je pre študentov na vašej úrovni veľmi dobre čitateľná.
- Počas semestra plánujem prebrať (s malými obmenami) materiál z Curriculum 2, ktoré je popísané na strane x v knihe.

Doplňujúce materiály ku knihe

- Ku knihe zriadili jej autori aj webstránku
<https://www.cryptography-textbook.com/>
- Na tejto webstránke môžete nájsť:
 - Zoznam chýb, ktoré sa v knihe nachádzajú.
 - Riešenia nepárnych úloh z knihy.
 - Videá zo starších prednášok založených na prvom vydaní knihy. Pozor! My pôjdeme podľa druhého vydania, ktoré obsahuje aj témy, ktoré v prvom vydaní neboli. Preto tieto videá nepokrývajú celú látku, ktorú budeme preberať. Pokrývajú z nej ale významnú časť a myslím si, že pre vás budú užitočné.
 - Slajdy zo starších prednášok založených na prvom vydaní knihy. Pozor! Opäť platí, že tieto slajdy nepokrývajú celú látku, ktorú budeme preberať.

Prednášky a cvičenia

- Medzi prednáškami a cvičeniami nebudem rozlišovať. Znamená to, že cvičenia a prednášky budú vyzeráť rovnako – budem preberať novú látku a priebežne budem uvádzať príklady.
- Prednáška sa koná v čase Pondelok 10:00-12:00 v miestnosti ab35.
- Cvičenie sa koná v čase Štvrtok 15:00-17:00 v miestnosti ab35.

Sady úloh

- Počas výučbovej časti semestra dostanete 10 sád úloh.
- Každú z úloh odovzdáte do miesta odovzdania v AISe.
- Na prvej prednáške/cvičení po uplynutí termínu na odovzdanie aktuálnej sady úloh vygenerujem pseudonáhodné číslo, ktoré určí, ktorú úlohu z aktuálnej sady budem hodnotiť. Maximálny počet bodov, ktorý za vybranú úlohu budete môcť získať bude vždy 5. Hodnotenia vybraných úloh budem priebežne zadávať do miesta odovzdania v AISe.
- Na prvej prednáške/cvičení po uplynutí termínu na odovzdanie aktuálnej sady úloh budete mať možnosť pýtať sa na riešenia.
- Podobné úlohy sa môžu vyskytnúť aj na záverečnej skúške.

Webstránka predmetu

- Predmet má zriadenú vlastnú webovú stránku na stránke Ústavu informatiky a matematiky:

<https://uim.fei.stuba.sk/predmet/i-zkry/>

- Na webstránke budú priebežne zverejňované tieto materiály:
 - Prezentácie z prednášok a cvičení.
 - Sady úloh.

Ďalšie používané informačné nástroje

- Aktuálne informácie vám budem priebežne posielat' na vaše univerzitné emaily.

Kto absolvoval predmet ***Klasické šifry***?

Kto absolvoval predmet **Rýchle**
algoritmy?

Kto absolvoval predmet ***Algebraické
štruktúry?***