

Pro orientaci ve výuce připravili vyučující studentům interaktivní osnovu, která je rozdělena po jednotlivých týdnech výuky a odkazuje je na prezentace, slajdy z přednášek a k dispozici jsou i videozáznamy přednášek.

Studenty velmi ceněným elektronickým studijním materiálem jsou videopřednášky nahrané přes službu PolyMedia Technologies. Vyučující a jeho komentář jsou zaznamenávány na kameru a vedle toho je snímán i sešit, kam učitel zapisuje poznámky a výpočty. Demonstrovaný výpočet si díky tomuto řešení může student kdykoliv pozastavit, vrátit se k vybraným pasážím nebo přeskocit to, co se mu zdá zřejmé.

Během semestru studenti píšou dvě vnitrosestrální písemky a nakonec i závěrečnou zkoušku. Vše má formou rukou psaných odpovědí do skenovatelných odpovědních archů, kam opravující vepisují body a případné komentáře. Body mají studenti ihned po naskenování přístupné v poznámkových blocích a komentáře k nahlédnutí ve své Přijímačce.

Docházka do seminárních skupin je povinná a eviduje se elektronicky pomocí příslušné aplikace. Na cvičeních studenti mohou získat body navíc za tzv. minipísemky. Další body mohou získat za nalezení chyb ve zveřejněné učebnici.

Studenti...

(zkráceno)

## Náhledy e-learningu

**Týden 2**  
Učitel doporučuje studovat od 16. 2. 2015 do 22. 2. 2015

2. Minipísemka, kongruence  
Základní vlastnosti kongruence  
vhodné příklady: 10.11. - 10.12.

Praktická prezentace 2  
Slidy 2  
[/el/1433/jaro2015/MB104](#)

**Týden 3**  
Učitel doporučuje studovat od 2. 3. 2015 do 8. 3. 2015

3. Prvočísla, řád čísla  
Rozložení prvočísel, malá Fermatova věta  
vhodné příklady: 10.11. - 10.12.

Řešené příklady s komentářem vyučujícího jsou připravené na každý týden

Handwritten mathematical work on a scanned sheet, including calculations and a question: "máme nějaké příklady? (o jaké číslo?)".

Studenti v naskenovaných listech vidí zpětnou vazbu učitele a místa, kde chybovali

**Titulní strana předmětu MB104 Diskrétní matematika**

**Týden 1**  
Učitel doporučuje studovat od 16. 2. 2015 do 22. 2. 2015

1. Dělitelnost  
základní vlastnosti, největší společný dělitel  
vhodné příklady 10.1. - 10.10.

Praktická prezentace 1  
Slidy 1  
[/el/1433/jaro2015/MB104](#)

**Týden 2**  
Učitel doporučuje studovat od 16. 2. 2015 do 22. 2. 2015

2. Minipísemka, kongruence

**Týden 11**  
Učitel doporučuje studovat od 27. 4. 2015 do 3. 5. 2015

8. Vytvořující funkce, rekurence  
Základní způsoby řešení kombinatorických úloh: rekurence  
Vhodné příklady: 12.61 - 12.67

Praktická prezentace 8  
Slidy 8  
[/el/1433/jaro2015/MB104/um/m/IV-8.pdf](#)

Praktické videoprezentace a slajdy z přednášek mají studenti odkazovány z interaktivní osnovy

Princip digitálního podpisu

- Vygeneruje se otisk (hash)  $H_M$  zprávy pevně stanovené délky (např. 160 nebo 256 bitů).
- Podpis zprávy  $S_M(H_M)$  tohoto hashu s nutnou podepsujícího.
- Zpráva  $M$  (případně spolu s podpisem) odesílá.

Ověření podpisu

- K přijaté zprávě  $M$  se vygeneruje otisk  $H_M$ .
- S pomocí veřejného klíče odesílatele se rekonstruuje původní zpráva  $M$ .
- Oba otisky se porovnají.

Kryptografie s veřejným klíčem (PKC)

Dva hlavní úkoly pro PKC jsou zajistit

- šifrování, kdy zpráva zašifrovanou veřejným klíčem příjemce není schopen rozšifrovat nikdo kromě něj (resp. držitele jeho soukromého klíče)
- podepisování, kdy int. klíčem odesílatele můžeme veřejnému klíči odělat.

Nejčastěji používané systémy

- RSA (šifrování) a odě

**Příklad (Lidská příbůh algoritmu)**  
Vypočítáme  $2^{560} \pmod{561}$  (Protok 560 = (100011000)2, dostaneme uvedeným algoritmem

exponent	base	result	exp's last digit
560	2	1	0
280	4	1	0
140	16	1	0
70	256	1	0
35	460	1	1
17	103	460	1
8	511	256	0
4	256	256	0
2	460	256	0
1	103	256	1
0	511	1	0

Výukové prezentace mají studenti dostupné z interaktivní osnovy