|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Algebra** | | | | |
| **Typ předmětu** | přednáška a cvičení  základní teoretický předmět profilujícího základu | | | **doporučený ročník / semestr** | 2LS |
| **Rozsah studijního předmětu** | 4/2 | **hod.** | 78 | **kreditů** | 8 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z+Zk | | **Forma výuky** | přednáška a cvičení | | |
| **Další požadavky na studenta** |  | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | doc. RNDr. David Stanovský, Ph.D. | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Abstraktní teorie dělitelnosti*  *Algebra polynomů*  *Grupy a symetrie*  *Tělesová rozšíření a Galoisova teorie* | | | | | |
|  | | | | | | |
| **Studijní literatura** | D. Stanovský, Základy algebry, Matfyzpress, Praha 2010.  J. Rotman, A First Course in Abstract Algebra  L. Rowen, Algebra: Groups, Rings, and Fields  S. Lang, Algebra, Revised 3rd ed., GTM 211, Springer, New York, 2002.  N. Lauritzen, Concrete Abstract Algebra, Cambridge Univ. Press, Cambridge 2003. | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Analýza maticových výpočtů 1** | | | | |
| **Typ předmětu** | přednáška a cvičení | | | **doporučený ročník / semestr** | 3ZS |
| **Rozsah studijního předmětu** | 2/2 | **hod.** | 52 | **kreditů** | 5 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z+Zk | | **Forma výuky** | přednáška a cvičení | | |
| **Další požadavky na studenta** | Předpokládají se znalosti v rozsahu základních kursů lineární algebry,  matematické analýzy a numerických metod. Při cvičeních bude využíván  MATLAB a veřejně přístupný software. | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | RNDr. Iveta Hnětynková, Ph.D. | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Opakování maticových rozkladů*  *Řešení lineárních aproximačních problémů*  *Krylovovy prostory, Arnoldiho a Lanczosova metoda pro výpočet báze*  *Krylovovské metody pro řešení soustav lineárních algebraických rovnic*  *Maticové funkce*  *Speciální matice* | | | | | |
|  | | | | | | |
| **Studijní literatura** | Duintjer Tebbens, J., Hnětynková, I., Plešinger, M., Strakoš, Z., Tichý, P., Analýza metod pro maticové výpočty: Základní metody, Matfyzpress, Praha, 2012.  Fiedler, M., Speciální matice a jejich použití v numerické matematice, SNTL, Praha, l981.  Golub, G..H., Van Loan, C.F., Matrix Computations, J. Hopkins Univ. Press, Baltimore, Third edition 1996.  Higham, N. J., Functions of Matrices: Theory and Computation, SIAM, 2008.  Watkins, D.S., Fundamentals of Matrix Computations, J. Wiley & Sons, New York, Third edition 2010. | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Anglický jazyk** | | | | |
| **Typ předmětu** | přednáška | | | **doporučený ročník / semestr** | 2LS |
| **Rozsah studijního předmětu** | 0/2 | **hod.** | 26 | **kreditů** | 1 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Zk | | **Forma výuky** | přednáška | | |
| **Další požadavky na studenta** | Pokročilá znalost anglického jazyka | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | KJP | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Výuka anglického jazyka pro středně pokročilé a pokročilé studenty.*  *Zkouška z všeobecného a odborného anglického jazyka (gramatika, poslech, četba s porozuměním, esej) na pokročilé úrovni.* | | | | | |
|  | | | | | | |
| **Studijní literatura** | M. Foley, D. Hall: Total English Elementary - Students' Book + Workbook with key (Pearson - Longman)  R. Acklam, A. Crace: Total English Pre-Intermediate - Students' Book + Workbook with key (Pearson - Longman)  A. Clare, J.J. Wilson: Total English Intermediate; Total English Upper Intermediate; Total English Advanced - Students'  Book + Workbook with key (Pearson - Longman)  R. Acklam, A. Crace: Total English Upper Intermediate - Students' Book + Workbook with key (Pearson - Longman)  J.J. Wilson, A. Clare: Total English Advanced - Students' Book + Workbook with key (Pearson - Longman)  A. Křepinská a kol.: Rozšiřující materiály pro výuku anglického jazyka (Matfyzpress).  Angličtina pro jazykové školy I - III. (E. Zábojová, J. Peprník, S. Nangonová; D. Sparling, nakl. Fortuna) | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Anglický jazyk pro středně pokročilé a pokročilé I** | | | | |
| **Typ předmětu** | přednáška | | | **doporučený ročník / semestr** | 1ZS |
| **Rozsah studijního předmětu** | 0/2 | **hod.** | 26 | **kreditů** | 1 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z | | **Forma výuky** | přednáška | | |
| **Další požadavky na studenta** | Základní znalost anglického jazyka | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | KJP | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Výuka anglického jazyka pro mírně pokročilé.* | | | | | |
|  | | | | | | |
| **Studijní literatura** | A. Crace, R. Acklam: New Total English Pre-Intermediate - Students' Book + Workbook with key (Pearson Longman);  A. Křepinská, M. Bubeníková, M. Mikuláš: Angličtina pro studenty MFF UK (Matfyzpress) | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Anglický jazyk pro středně pokročilé a pokročilé II** | | | | |
| **Typ předmětu** | přednáška | | | **doporučený ročník / semestr** | 1LS |
| **Rozsah studijního předmětu** | 0/2 | **hod.** | 26 | **kreditů** | 1 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z | | **Forma výuky** | přednáška | | |
| **Další požadavky na studenta** | Základní znalost anglického jazyka | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | KJP | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Navazující výuka anglického jazyka pro středně pokročilé a pokročilé.* | | | | | |
|  | | | | | | |
| **Studijní literatura** | Pro úroveň C:  A.Grace, R. Acklam: New Total English Upper-Intermediate - Students' Book + Workbook with key (Pearson Longman).  Pro úroveň D:  JJ Wilson, A. Clare: New Total English Advanced - Students' Book + Workbook with key (Pearson Longman).  Pro obě úrovně materiál pro studium odborného jazyka:  A.Křepinská, M. Bubeníková, M. Mikuláš: Angličtina pro studenty MFF UK (Matfyzpress) | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Anglický jazyk pro středně pokročilé a pokročilé III** | | | | |
| **Typ předmětu** | přednáška | | | **doporučený ročník / semestr** | 2ZS |
| **Rozsah studijního předmětu** | 0/2 | **hod.** | 26 | **kreditů** | 1 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z | | **Forma výuky** | přednáška | | |
| **Další požadavky na studenta** | Základní znalost anglického jazyka | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | KJP | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Navazující výuka anglického jazyka pro středně pokročilé a pokročilé.* | | | | | |
|  | | | | | | |
| **Studijní literatura** | Pro úroveň C:  A.Grace, R. Acklam: New Total English Upper-Intermediate - Students' Book + Workbook with key (Pearson Longman).  Pro úroveň D:  JJ Wilson, A. Clare: New Total English Advanced - Students' Book + Workbook with key (Pearson Longman).  Pro obě úrovně materiál pro studium odborného jazyka:  A.Křepinská, M. Bubeníková, M. Mikuláš: Angličtina pro studenty MFF UK (Matfyzpress) | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Anglický jazyk pro středně pokročilé a pokročilé IV** | | | | |
| **Typ předmětu** | přednáška | | | **doporučený ročník / semestr** | 2LS |
| **Rozsah studijního předmětu** | 0/2 | **hod.** | 26 | **kreditů** | 1 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z | | **Forma výuky** | přednáška | | |
| **Další požadavky na studenta** | Základní znalost anglického jazyka | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | KJP | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Navazující výuka anglického jazyka pro středně pokročilé a pokročilé.* | | | | | |
|  | | | | | | |
| **Studijní literatura** | Pro úroveň C:  A.Grace, R. Acklam: New Total English Upper-Intermediate - Students' Book + Workbook with key (Pearson Longman).  Pro úroveň D:  JJ Wilson, A. Clare: New Total English Advanced - Students' Book + Workbook with key (Pearson Longman).  Pro obě úrovně materiál pro studium odborného jazyka:  A.Křepinská, M. Bubeníková, M. Mikuláš: Angličtina pro studenty MFF UK (Matfyzpress) | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Aplikovaná kryptografie** | | | | |
| **Typ předmětu** | přednáška a cvičení | | | **doporučený ročník / semestr** | 3LS |
| **Rozsah studijního předmětu** | 2/1 | **hod.** | 39 | **kreditů** | 4 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z+Zk | | **Forma výuky** | přednáška a cvičení | | |
| **Další požadavky na studenta** |  | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | Dr. rer. nat. Faruk Göloglu | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Public Key Infrastructures (PKI)*  *uživatelská autentifikace*  *autentifikační protokoly*  *kryptoměny a blockchain*  *Transport Layer Security*  *Operating System Security*  *kontrola přístupu*  *bezpečnost TCP-IP*  *cervi, DoS, botnety*  *DNS útoky*  *bezpečný routing*  *útoky na Wireless*  *VPN*  *anonymita*  *firewally*  *detekce útoku*  *bezpečnost webu, cloudu, mobilní telefonie* | | | | | |
|  | | | | | | |
| **Studijní literatura** | Ross Anderson, Security Engineering, Wiley, 2001  Elisa Bertino, Ravi Sandhu Synthesis Lectures on Information Security, Privacy, and Trust, Morgan&Claypool Publishers, 2017  Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996 | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Datové a procesní modely** | | | | |
| **Typ předmětu** | přednáška a cvičení | | | **doporučený ročník / semestr** | 3LS |
| **Rozsah studijního předmětu** | 2/2 | **hod.** | 52 | **kreditů** | 5 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z+Zk | | **Forma výuky** | přednáška a cvičení | | |
| **Další požadavky na studenta** | Znalost základů účetnictví. | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | RNDr. Jiří Měska | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Data a jejich struktura. Datové modely. E-R diagramy. Relační databáze. Normalizace a denormalizace. Jemný úvod do jazyka SQL. Transformace relačních datových schémat. Integrita dat v relačních schématech. Dimenzionální datové struktury. Procesní modely. Procesy přidávání nových dat a změn stávajících dat. Časový vývoj dat. Obecné struktury procesu. Work-flow.* | | | | | |
|  | | | | | | |
| **Studijní literatura** | Martin Gruber: Mistrovství v SQL, Svazek1,2, SoftPress, 2004.  James R.Groff, Paul N.Weinberg: SQL kompletní průvodce, Computer Press, 2005.  Bruce Momjian: PostgresSQL, Praktický průvodce, Computer Press, 2003.  Thomas Kyte: Oracle návrh a tvorba aplikací, Computer Press, 2005.  Howes, T; Smith, M; Good, G: Understanding and Deploying LDAP Directory Services | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Digitální zpracování obrazu** | | | | |
| **Typ předmětu** | přednáška | | | **doporučený ročník / semestr** | 3ZS |
| **Rozsah studijního předmětu** | 3/0 | **hod.** | 39 | **kreditů** | 5 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Zk | | **Forma výuky** | přednáška | | |
| **Další požadavky na studenta** |  | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | prof. Ing. Jan Flusser, DrSc. | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Úvodní přednáška z digitálního zpracování obrazu a rozpoznávání. Hlavní pozornost je věnována digitalizaci obrazu, předzpracování (potlačení šumu, zvýšení kontrastu, odstranění rozmazání), detekci hran, geometrickým transformacím, příznakovému popisu objektů a metodám automatického rozpoznávání (klasifikace). Výklad teorie bude doprovázen ukázkami experimentů a praktických aplikací.* | | | | | |
|  | | | | | | |
| **Studijní literatura** | Pratt W. K.: Digital Image Processing (2nd ed.), John Wiley, New York, 1991  Rosenfeld A., Kak A. C.: Digital Picture Processing, Academic Press, New York, 1982  Gonzales R. C., Woods R. E., Digital Image Processing (3rd ed.), Addison-Wesley, 1992  Duda R.O. et al., Pattern Classification, (2nd ed.), John Wiley, New York, 2001 | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Diskrétní matematika** | | | | |
| **Typ předmětu** | přednáška a cvičení  základní teoretický předmět profilujícího základu | | | **doporučený ročník / semestr** | 1ZS |
| **Rozsah studijního předmětu** | 2/2 | **hod.** | 52 | **kreditů** | 5 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z+Zk | | **Forma výuky** | přednáška a cvičení | | |
| **Další požadavky na studenta** |  | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | doc. RNDr. Vít Jelínek, Ph.D. | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Množiny a operace s nimi*  *Relace, funkce, ekvivalence*  *Kombinatorické počítání*  *Grafy, jejich isomorfismus a metrika*  *Stromy a jejich vlastnosti*  *Částečná a lineární uspořádání*  *Prostory cyklů a řezů* | | | | | |
|  | | | | | | |
| **Studijní literatura** | J. Matoušek, J. Nešetřil: Kapitoly z diskrétní matematiky, MatfyzPress, 1996.  J. Nešetřil: Kombinatorika I, grafy, SPN Praha, 1983.  P. Štěpánek, B.Balcar: Teorie množin, Academia Praha, 1986. | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Geometrické modelování** | | | | |
| **Typ předmětu** | přednáška a cvičení  základní teoretický předmět profilujícího základu | | | **doporučený ročník / semestr** | 3ZS |
| **Rozsah studijního předmětu** | 2/2 | **hod.** | 52 | **kreditů** | 6 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z+Zk | | **Forma výuky** | přednáška a cvičení | | |
| **Další požadavky na studenta** |  | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | doc. RNDr. Zbyněk Šír, Ph.D. | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Předmět je zaměřen na základní matematické principy reprezentace křivek a ploch v geometrických aplikacích.*  *Témata: po částech lineární aproximace, odhad křivosti, kruhové splajny, geometrická a analytická interpolace, Bézierovy křivky, De Casteljau algoritmus, racionální křivky a plochy, B-spline křivky a plochy, tenzorové plochy, subdivision.* | | | | | |
|  | | | | | | |
| **Studijní literatura** | J. Hoschek, D. Lasser: Fundamentals of Computer Aided Geometric Design ,A K Peters, 1993.  G. Farin, J. Hoschek, M. Kim: Handbook of Computer Aided Geometric Design, Elsevier, 2002.  I. Linkeová: Základy počítačového modelování křivek a ploch, Vydavatelství ČVUT v Praze, 2008.  I. Linkeová: NURBS křivky, Nakladatelství ČVUT, Praha, 2007. | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Geometrie 1** | | | | |
| **Typ předmětu** | přednáška a cvičení  základní teoretický předmět profilujícího základu | | | **doporučený ročník / semestr** | 2ZS |
| **Rozsah studijního předmětu** | 2/2 | **hod.** | 52 | **kreditů** | 5 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z+Zk | | **Forma výuky** | přednáška a cvičení | | |
| **Další požadavky na studenta** | Předpokládané znalosti na úrovni předmětu Matematická analýza 2 | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | doc. RNDr. Zbyněk Šír, Ph.D. | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Afinní a eukleidovská geometrie,*  *Grupy eukleidovských a afinních transformací, Projektivní geometrie,*  *Diferenciální geometrie křivek*  *Křivkový integrál 1. a 2. druhu.* | | | | | |
|  | | | | | | |
| **Studijní literatura** | M. K. Bennett, Affine and Projective Geometry,Wiley, 1995.  L. Boček, M. Sekanina: Geometrie I, SPN Praha, 1986.  L. Boček, M. Sekanina: Geometrie II, SPN Praha, 1988.  M. Lávička: Geometrie 1 a 2, ZČU Plzeň, 2006.  M. Henle, Modern Geometries: Non-Euclidean, Projective, and Discrete Geometry, Pearson 2001.  R. Hartley, A. Zisserman: Multiple View Geometry in Computer Vision, Cambridge University Press, 2004. | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Komutativni algebra** | | | | |
| **Typ předmětu** | přednáška a cvičení  základní teoretický předmět profilujícího základu | | | **doporučený ročník / semestr** | 3ZS |
| **Rozsah studijního předmětu** | 3/1 | **hod.** | 52 | **kreditů** | 6 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z+Zk | | **Forma výuky** | přednáška a cvičení | | |
| **Další požadavky na studenta** |  | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | doc. RNDr. Jan Šťovíček, Ph.D. | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Úvod*  *- Ideály a delitelnost, aritmetika ideálu, noetherovskost, hierarchie oboru*  *- Faktorokruhy, Vety o homomorfismu a izomorfismu, Cínská veta o zbytcích*  *- Gaussovo lemma, Gaussova veta a Hilbertova veta o bázi*  *Galoisova teorie*  *- rozširování homomorfismu do rozkladových nadteles a Galoisova grupa*  *- konstrukce a jednoznacnost alg. uzáveru*  *- stupen separability a separabilní rozšírení*  *- jednoduchá rozšírení, veta o primitivním prvku*  *- normální a Galoisova rozšírení*  *- hlavní veta Galoisovy teorie*  *- (ne)rešitelnost polynomu v radikálech*  *Úvod do algebraické geometrie*  *- Radikály*  *- Galoisova korespondence I,V, ireducibilita vs. prvoideály*  *- Hilbertova veta o nulách*  *Úvod do algebraické teorie císel*  *- Rešení diofantických rovnic rozkladem v císelných telesech*  *- Okruhy celistvých prvku a jejich základní vlastnost*  *- Jednoznacný rozklad ideálu*  *- Popis prvoideálu* | | | | | |
|  | | | | | | |
| **Studijní literatura** | A. Drápal, Komutativní okruhy (skriptum).  W. Fulton, Algebraic curves, online.  M. F. Atiah, I.G. Macdonald, Introduction to Commutative Algebra, Addison Wesley, 1969.  H. Matsumura, Commutative Ring Theory, W. A. Benjamin, 1970.  P. Samuel, O. Zariski, Commutative Algebra vol. I and II, Princeton, D. Van Nostrand Company, 1958, 1960.  R. Y. Sharp, Steps in Commutative Algebra (London Math. Society Student Text), Cambridge Univ. Press, 2nd ed., 2001.  L. Procházka a kol., Algebra. Academia, Praha 1990. | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Lineární algebra 1** | | | | |
| **Typ předmětu** | přednáška a cvičení  základní teoretický předmět profilujícího základu | | | **doporučený ročník / semestr** | 1ZS |
| **Rozsah studijního předmětu** | 4/2 | **hod.** | 78 | **kreditů** | 10 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z+Zk | | **Forma výuky** | přednáška a cvičení | | |
| **Další požadavky na studenta** |  | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | doc. Mgr. Libor Barto, Ph.D. | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Opakování analytické geometrie v rovině a prostoru, soustavy lineárních rovnic, tělesa, matice, vektorové prostory, lineární zobrazení, determinanty.* | | | | | |
|  | | | | | | |
| **Studijní literatura** | základní:  L. Barto, J. Tůma, Lineární algebra, elektronická skripta  L. Bican, Lineární algebra a geometrie, Academia, Praha 2000.  J. Bečvář, Vektorové prostory I, II, III, SPN Praha 1978, 1981, 1982  další doporučená:  C.D. Meyer, Matrix Analysis and Applied Linear Algebra, SIAM 2000.  T.S. Blyth, E.F. Robertson, Basic Linear Algebra, Springer Verlag London,2002,  S.H. Friedberg, A.J. Insel, L.E.Spence, Linear Algebra, Third Edition, Prentice-Hall, Inc., 1997. | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Lineární algebra 2** | | | | |
| **Typ předmětu** | přednáška a cvičení  základní teoretický předmět profilujícího základu | | | **doporučený ročník / semestr** | 1LS |
| **Rozsah studijního předmětu** | 4/2 | **hod.** | 78 | **kreditů** | 10 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z+Zk | | **Forma výuky** | přednáška a cvičení | | |
| **Další požadavky na studenta** | Předpokládané znalosti na úrovni Lineární algebra 1 | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | doc. Mgr. Libor Barto, Ph.D. | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Skalární součin, vlastní čísla a vlastní vektory, diagonalizace, ortogonální diagonalizace, bilineární a kvadratické formy.* | | | | | |
|  | | | | | | |
| **Studijní literatura** | základní:  L. Barto, J. Tůma, Lineární algebra, elektronická skripta  L. Bican, Lineární algebra a geometrie, Academia, Praha 2000.  J. Bečvář, Vektorové prostory I, II, III, SPN Praha 1978, 1981, 1982.  doporučená:  C.D. Meyer, Matrix Analysis and Applied Linear Algebra, SIAM 2000.  T.S. Blyth, E.F. Robertson, Basic Linear Algebra, Springer Verlag London,2002,  S.H. Friedberg, A.J. Insel, L.E.Spence, Linear Algebra, Third Edition, Prentice-Hall, Inc., 1997. | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Matematická analýza 1** | | | | |
| **Typ předmětu** | přednáška a cvičení  základní teoretický předmět profilujícího základu | | | **doporučený ročník / semestr** | 1ZS |
| **Rozsah studijního předmětu** | 4/4 | **hod.** | 104 | **kreditů** | 10 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z+Zk | | **Forma výuky** | přednáška a cvičení | | |
| **Další požadavky na studenta** |  | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | prof. RNDr. Luboš Pick, CSc., DSc. | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Výroková a predikátová logika, množiny, reálná a komplexni čísla, limita posloupnosti, limita a spojitost funkce, zavedení elementárních funkcí, derivace funkce, Taylorův polynom.* | | | | | |
|  | | | | | | |
| **Studijní literatura** | Základní:  V. Jarník: Diferenciální počet I, Academia, 1984.  V. Jarník: Diferenciální počet II, Academia, 1984.  B. P. Děmidovič: Sbírka úloh a cvičení z matematické analýzy, Fragment, 2003.  J. Milota: Matematická analýza I, 1. a 2. část (skriptum), MFF UK, 1978.  L. Zajíček: Vybrané úlohy z matematické analýzy pro 1. a 2. ročník, Matfyzpress, 2006.  Doplňková:  J. Čerych a kol.: Příklady z matematické analýzy V (skriptum), MFF UK, 1983.  P. Holický, O. Kalenda: Metody řešení vybraných úloh z matematické analýzy pro 2.-4. semestr, Matfyzpress, 2006.  J. Lukeš a kol.: Problémy z matematické analýzy (skriptum), MFF UK, 1982.  I. Netuka, J. Veselý: Příklady z matematické analýzy III (skriptum), MFF UK, 1977.  W. Rudin: Principles of mathematical analysis, McGraw-Hill, 1976. | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Matematická analýza 2** | | | | |
| **Typ předmětu** | přednáška a cvičení  základní teoretický předmět profilujícího základu | | | **doporučený ročník / semestr** | 1LS |
| **Rozsah studijního předmětu** | 4/4 | **hod.** | 104 | **kreditů** | 10 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z+Zk | | **Forma výuky** | přednáška a cvičení | | |
| **Další požadavky na studenta** | Předpokládané znalosti na úrovni Matematická analýza 1 | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | prof. RNDr. Luboš Pick, CSc., DSc. | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Číselné řady (kritéria konvergence, Cauchyův součin, řady s komplexními členy).*  *Primitivní funkce, určitý integrál (Riemannův a Newtonův integrál).*  *Obyčejné diferenciální rovnice (diferenciální rovnice se separovanými proměnnými, lienární diferenciální rovnice, soustavy lineárních diferenciálních rovnic).* | | | | | |
|  | | | | | | |
| **Studijní literatura** | Základní:  V. Jarník: Diferenciální počet I, Academia, 1984.  V. Jarník: Diferenciální počet II, Academia, 1984.  B. P. Děmidovič: Sbírka úloh a cvičení z matematické analýzy, Fragment, 2003.  J. Milota: Matematická analýza I, 1. a 2. část (skriptum), MFF UK, 1978.  L. Zajíček: Vybrané úlohy z matematické analýzy pro 1. a 2. ročník, Matfyzpress, 2006.  Doplňková:  J. Čerych a kol.: Příklady z matematické analýzy V (skriptum), MFF UK, 1983.  P. Holický, O. Kalenda: Metody řešení vybraných úloh z matematické analýzy pro 2.-4. semestr, Matfyzpress, 2006.  J. Lukeš a kol.: Problémy z matematické analýzy (skriptum), MFF UK, 1982.  I. Netuka, J. Veselý: Příklady z matematické analýzy III (skriptum), MFF UK, 1977.  W. Rudin: Principles of mathematical analysis, McGraw-Hill, 1976. | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Matematická analýza 3** | | | | |
| **Typ předmětu** | přednáška a cvičení  základní teoretický předmět profilujícího základu | | | **doporučený ročník / semestr** | 2ZS |
| **Rozsah studijního předmětu** | 4/2 | **hod.** | 78 | **kreditů** | 8 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z+Zk | | **Forma výuky** | přednáška a cvičení | | |
| **Další požadavky na studenta** | Předpokládané znalosti na úrovni předmětů Matematická analýza 1 a 2 | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | prof. RNDr. Luboš Pick, CSc., DSc. | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Metrické prostory (konvergence, spojitost zobrazení, kompaktní prostory a úplné metrické prostory).*  *Funkce více proměnných (parciální derivace, totální diferenciál, parciální derivace vyšších řádů, věta o implicitních funkcích, Taylorův polynom, extémy funkcí).* | | | | | |
|  | | | | | | |
| **Studijní literatura** | Základní:  V. Jarník: Diferenciální počet II  V. Jarník: Integrální počet I,II  V. Jarník: Matematická analýza pro 3. semestr (skriptum)  L. Zajíček: Vybrané partie z matematické analýzy pro 2. ročník  J. Čerych a kol.: Příklady z matematické analýzy V (skriptum)  L. Zajíček: Vybrané úlohy z matematické analýzy pro 1. a 2. ročník  P. Holický, O.Kalenda: Metody řešení vybraných úloh z matematické analýzy pro 2. až 4. semestr  Doplňková:  S. Fučík, J.Milota: Matematická analýza II (skriptum)  B. P. Demidovič: Sbornik zadač i upražnenij po matematičeskomu analizu  W. Rudin: Principles of Math. Analysis (existuje ruský překlad)  G. M. Fichtengolc: Kurs differencialnogo i integralnogo isč. I,II  J. Lukeš a kol.: Problémy z matematické analýzy (skriptum) | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Matematická kryptografie a kryptoanalýza I** | | | | |
| **Typ předmětu** | přednáška a cvičení | | | **doporučený ročník / semestr** | 3ZS |
| **Rozsah studijního předmětu** | 2/1 | **hod.** | 39 | **kreditů** | 4 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z+Zk | | **Forma výuky** | přednáška a cvičení | | |
| **Další požadavky na studenta** |  | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | Mgr. Robert El Bashir, Dr. | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Kryptosystémy - endomorfní kryptosystémy, produkt kryptosystémů, komutující kryptosystémy, idempotentní kryptosystémy, substituční a permutační šifry, iterované kryptosystémy, substitučně-permutační sítě.*  *Booleovské funkce - okruh binárních booleovských funkcí, algebraická normální forma, algebraický stupeň, korelace binárních booleovských funkcí, Walsh-Hadamardova transformace, spektrum, Parsevalova věta, korelační matice, booleovské permutace, Piling-up lemma, bricklayer funkce.*  *Lineární kryptoanalýza - lineární cesty, korelační příspěvek lineární cesty, věta o skládání lineárních cest, korelační příspěvek pro klíč alternující šifru, lineární útok na substitučně-permutační síť.* | | | | | |
|  | | | | | | |
| **Studijní literatura** | Neal Koblitz: Algebraic aspects of cryptography, Springer Verlag 1998;  Douglas R. Stinson: Cryptography: Theory and practice, Chapman and Hall, Boca Raton, 2006.  Serge Vaudenay, A classical introduction to cryptography: applications for communications security, Springer, New York, 2006.  Michael Luby: Pseudorandomness and cryptographic applications, Princeton Univ Pr. Princeton 1996. | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Matematická kryptografie a kryptoanalýza II** | | | | |
| **Typ předmětu** | přednáška | | | **doporučený ročník / semestr** | 3LS |
| **Rozsah studijního předmětu** | 2/0 | **hod.** | 26 | **kreditů** | 3 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Zk | | **Forma výuky** | přednáška | | |
| **Další požadavky na studenta** |  | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | Mgr. Robert El Bashir, Dr. | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Diferenční kryptoanalýza - matice šíření diference, diferenční cesty, váha diferenční cesty, váha pro klíč alternující šifru, diferenční útok na substitučně-permutační síť.*  *Korelační potenciál - cross-korelace, auto-korelace, Wiener-Khintchinova věta, vztah matice korelačních potenciálů a matice šíření diference.*  *Asymetrické kryptosystémy - jednosměrné funkce, RSA a faktorizační algoritmy, složitost faktorizačních algoritmů, Henselovo lemma, hladké hodnoty, kvadratické síto, problém diskrétního logaritmu, Diffie-Hellmanův problém, indexový kalkulus.* | | | | | |
|  | | | | | | |
| **Studijní literatura** | Neal Koblitz: Algebraic aspects of cryptography, Springer Verlag 1998;  Douglas R. Stinson: Cryptography: Theory and practice, Chapman and Hall, Boca Raton, 2006.  Serge Vaudenay, A classical introduction to cryptography: applications for communications security, Springer, New York, 2006.  Michael Luby: Pseudorandomness and cryptographic applications, Princeton Univ Pr. Princeton 1996. | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Matematický proseminář I** | | | | |
| **Typ předmětu** | proseminář | | | **doporučený ročník / semestr** | 1ZS |
| **Rozsah studijního předmětu** | 0/2 | **hod.** | 26 | **kreditů** | 2 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z | | **Forma výuky** | proseminář | | |
| **Další požadavky na studenta** |  | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | RNDr. Vlasta Moravcová, Ph.D. | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Výroková logika.*  *Množiny, relace, zobrazení.*  *Funkce.*  *Vztahy mezi goniometrickými funkcemi.*  *Rovnice a nerovnice.*  *Komplexní čísla.* | | | | | |
|  | | | | | | |
| **Studijní literatura** | Současné středoškolské učebnice matematiky a sbírky úloh. | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Matematický proseminář II** | | | | |
| **Typ předmětu** | proseminář | | | **doporučený ročník / semestr** | 1LS |
| **Rozsah studijního předmětu** | 0/2 | **hod.** | 26 | **kreditů** | 2 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z | | **Forma výuky** | proseminář | | |
| **Další požadavky na studenta** |  | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | RNDr. Vlasta Moravcová, Ph.D. | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Planimetrie a stereometrie.*  *Analytická geometrie v rovině a prostoru.*  *Kombinatorika.*  *Řešeny budou mimo jiné úlohy propojující uvedená témata.* | | | | | |
|  | | | | | | |
| **Studijní literatura** | Současné středoškolské učebnice matematiky a sbírky úloh. | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Počítačová algebra** | | | | |
| **Typ předmětu** | přednáška a cvičení  základní teoretický předmět profilujícího základu | | | **doporučený ročník / semestr** | 3ZS |
| **Rozsah studijního předmětu** | 3/1 | **hod.** | 52 | **kreditů** | 6 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z+Zk | | **Forma výuky** | přednáška a cvičení | | |
| **Další požadavky na studenta** |  | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | doc. RNDr. David Stanovský, Ph.D. | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Základní algoritmy pro operace s polynomy: aritmetické operace, čínská věta o zbytcích, největší společný dělitel.*  *Práce s matematickým software (Sage, Mathematica apod.).*  *1. Reprezentace dat, základní operace s čísly a polynomy, Karacubův a Eukleidův algoritmus.*  *2. Modulární reprezentace, algoritmická verze Čínské věty o zbytcích. Rychlá Fourierova transformace, její využití pro rychlé násobení polynomů.*  *3. Newtonova metoda a rychlé dělení polynomů.*  *4. Největší společný dělitel polynomů: Primitivní polynomy a Gaussovo lemma, posloupnosti polynomiálních zbytků, modulární algoritmus.* | | | | | |
|  | | | | | | |
| **Studijní literatura** | D. Stanovský, L.Barto: Počítačová algebra, Matfyzpress, 2011.  G. von zur Gathen: Modern computer algebra, Cambridge Univ. Press 1999  Knuth: The art of computer programming, vol. 1, Fundamental algorithms, Addison-Wesley, 3rd edition 1997 | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Pravděpodobnost** | | | | |
| **Typ předmětu** | přednáška a cvičení  základní teoretický předmět profilujícího základu | | | **doporučený ročník / semestr** | 2ZS |
| **Rozsah studijního předmětu** | 2/2 | **hod.** | 52 | **kreditů** | 6 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z+Zk | | **Forma výuky** | přednáška a cvičení | | |
| **Další požadavky na studenta** |  | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | doc. RNDr. Daniel Hlubinka, Ph.D. | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Základy teorie pravděpodobnosti a statistického uvažování.*  *Matematická axiomatika pravděpodobnosti, výpočetní vzorce, náhodné veličiny a vektory a jejich rozdělení, charakteristiky náhodných veličin.*  *Konvergence v pravděpodobnosti a v distribuci, zákon velkých čísel a centrální limitní věta, Markovova, Čebyševova a Chernoffova nerovnost.*  *Použití limitních vět a nerovností.*  *Odhad parametru a pravděpodobnosti pomocí limitních vět.* | | | | | |
|  | | | | | | |
| **Studijní literatura** | Ronald Meester. A Natural Introduction to Probability Theory 2nd ed. Birkhäuser 2008  Michael Mitzenmacher, Eli Upfal. Probability and Computing. Cambridge 2005  Geoffrey Grimmett , David Stirzaker. Probability and Random Processes. Oxford 2001.  Geoffrey Grimmett , David Stirzaker. One Thousand Exercises in Probability. Oxford 2001.  Zápisky k přednášce dostupné na http://www.karlin.mff.cuni.cz/~hlubinka/vyuka.php | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Pravděpodobnostní a statistické problémy** | | | | |
| **Typ předmětu** | přednáška a cvičení | | | **doporučený ročník / semestr** | 1LS |
| **Rozsah studijního předmětu** | 2/2 | **hod.** | 52 | **kreditů** | 5 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z+ZK | | **Forma výuky** | přednáška a cvičení | | |
| **Další požadavky na studenta** |  | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | doc. RNDr. Zbyněk Pawlas, Ph.D. | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Úvod do diskrétní pravděpodobnosti a řešení zajímavých problémů pomocí jednoduchých pravděpodobnostních a statistických metod.* | | | | | |
|  | | | | | | |
| **Studijní literatura** | Doporučená:  J. Anděl (2007): Matematika náhody, 3. vydání, Matfyzpress, Praha.  J. Bewersdorff (2005): Luck, Logic, and White Lies: The Mathematics of Games, A K Peters, Wellesley.  H. Tijms (2004): Understanding Probability: Chance Rules in Everyday Life, Cambridge University Press, Cambridge.  K. Zvára, J. Štěpán (2006): Pravděpodobnost a matematická statistika, 4. vydání, Matfyzpress, Praha. | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Programování 1** | | | | |
| **Typ předmětu** | laboratorní práce  předmět profilujícího základu | | | **doporučený ročník / semestr** | 1ZS |
| **Rozsah studijního předmětu** | 0/2 | **hod.** | 26 | **kreditů** | 3 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z | | **Forma výuky** | laboratorní práce | | |
| **Další požadavky na studenta** |  | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | doc. RNDr. Pavel Töpfer, CSc. | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Základy jazyka Python.*  *Cykly a pole.*  *Třídění a vyhledávání.*  *Funkce.*  *Využívání knihoven.*  *Seznamy a řetězce.*  *Základní datové struktury.*  *Objekty a třídy.*  *Práce se soubory.* | | | | | |
|  | | | | | | |
| **Studijní literatura** | Pilgrim, M.: Ponořme se do Pythonu 3, CZ.NIC, Praha 2011. | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Programování 2** | | | | |
| **Typ předmětu** | přednáška a cvičení  předmět profilujícího základu | | | **doporučený ročník / semestr** | 1LS |
| **Rozsah studijního předmětu** | 2/4 | **hod.** | 78 | **kreditů** | 8 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z+Zk | | **Forma výuky** | přednáška a cvičení | | |
| **Další požadavky na studenta** |  | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | doc. RNDr. Pavel Töpfer, CSc. | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Algoritmy a jejich složitost.*  *Třídění.*  *Reprezentace dat v paměti.*  *Rekurze.*  *Základní grafové algoritmy.*  *Metoda Rozděl a panuj.*  *Pravděpodobnostní algoritmy.* | | | | | |
|  | | | | | | |
| **Studijní literatura** | Mareš, M., Valla, T.: Průvodce labyrintem algoritmů, CZ.NIC, Praha 2017. | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Programování 3** | | | | |
| **Typ předmětu** | přednáška a cvičení  předmět profilujícího základu | | | **doporučený ročník / semestr** | 2ZS |
| **Rozsah studijního předmětu** | 2/2 | **hod.** | 52 | **kreditů** | 5 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z+Zk | | **Forma výuky** | přednáška a cvičení | | |
| **Další požadavky na studenta** |  | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | RNDr. Martin Pergel, Ph.D. | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Kurs nízkoúrovňového programování v C/C++:*  *Principy počítačů.*  *Jazyk C - principy a syntax, práce s ukazateli, preprocesor, knihovny.*  *Jazyk C++ a objektově orientované programování - principy OOP, specifika jazyka C++, knihovny.* | | | | | |
|  | | | | | | |
| **Studijní literatura** | Mareš, M., Valla, T.: Průvodce labyrintem algoritmů, CZ.NIC, Praha 2017. | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Proseminář z algebry** | | | | |
| **Typ předmětu** | proseminář | | | **doporučený ročník / semestr** | 2LS |
| **Rozsah studijního předmětu** | 0/2 | **hod.** | 26 | **kreditů** | 2 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z | | **Forma výuky** | proseminář | | |
| **Další požadavky na studenta** |  | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | Mgr. Jan Šaroch, Ph.D. | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Seminář určený k procvičení a doplnění látky základních přednášek z algebry. Doplňující témata jsou z teorie čísel, algebraické geometrie a (nejen počítačové) algebry.* | | | | | |
|  | | | | | | |
| **Studijní literatura** | D.Eisenbud, Commutative Algebra, 3rd Corrected Printing Springer, New York 1997.  S.Lang, Algebra, Revised 3rd ed., GTM 211, Springer, New York, 2002.  N. Lauritzen, Concrete Abstract Algebra, Cambridge Univ. Press, Cambridge 2003.  L.Procházka a kol., Algebra, Academia, Praha 1990. | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Proseminář z teorie čísel** | | | | |
| **Typ předmětu** | proseminář | | | **doporučený ročník / semestr** | 1LS |
| **Rozsah studijního předmětu** | 0/2 | **hod.** | 26 | **kreditů** | 2 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z | | **Forma výuky** | proseminář | | |
| **Další požadavky na studenta** |  | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | Mgr. Vítězslav Kala, Ph.D. | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Dělitelnost a kongruence: Základní vlastnosti, malá Fermatova věta, Eulerova věta, čínská zbytková věta, Wilsonova věta, kvadratické zbytky, prvočísla, aplikace Dirichletovy věty o aritmetických posloupnostech.*  *Diofantické rovnice: Metody řešení pomocí kongruencí, rozkladem, nekonečný sestup; úvod do algebraických čísel, Pellova rovnice.*  *Aritmetické funkce: Počet a součet dělitelů, Moebiova funkce a inverze.* | | | | | |
|  | | | | | | |
| **Studijní literatura** | Doporučená:  J. Herman, R. Kučera, J. Šimša, Metody řešení matematických úloh I. Masarykova univerzita 2011.  W. Stein, Elementary Number Theory: Primes, Congruences, and Secrets. http://wstein.org/ent/  Matematický korespondenční seminář, Seriál - Teorie čísel. http://mks.mff.cuni.cz/archive/28/9.pdf | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Referativní seminář k bakalářské práci** | | | | |
| **Typ předmětu** | seminář | | | **doporučený ročník / semestr** | 3LS |
| **Rozsah studijního předmětu** | 0/2 | **hod.** | 26 | **kreditů** | 4 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z | | **Forma výuky** | seminář | | |
| **Další požadavky na studenta** |  | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | doc. RNDr. David Stanovský, Ph.D. | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Předmětem semináře jsou referáty studentů adresující jejich pokroky v přípravě bakalářské práce.* | | | | | |
|  | | | | | | |
| **Studijní literatura** |  | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Řešitelský seminář** | | | | |
| **Typ předmětu** | seminář | | | **doporučený ročník / semestr** | 3ZS+LS |
| **Rozsah studijního předmětu** | 0/2 | **hod.** | 26 | **kreditů** | 3 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z | | **Forma výuky** | seminář | | |
| **Další požadavky na studenta** |  | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | doc. RNDr. Tomáš Bárta, Ph.D. | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Řešení problémů a úloh z matematické analýzy, algebry a diskrétní matematiky. Příprava na matematické soutěže vysokoškoláků.* | | | | | |
|  | | | | | | |
| **Studijní literatura** |  | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Samoopravné kódy** | | | | |
| **Typ předmětu** | přednáška a cvičení | | | **doporučený ročník / semestr** | 3ZS |
| **Rozsah studijního předmětu** | 3/1 | **hod.** | 52 | **kreditů** | 6 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z+Zk | | **Forma výuky** | přednáška a cvičení | | |
| **Další požadavky na studenta** |  | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | doc. Mgr. Štěpán Holub, Ph.D. | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Konečná tělesa.*  *Asymptotické odhady.*  *Lineární kódy.*  *Cyklické kódy.*  *Konvoluční kódy.* | | | | | |
|  | | | | | | |
| **Studijní literatura** | Cameron, van Lint: Designs, graphs, codes and their links, Cambridge Univ. Press 1991;  MacWilliams, Sloane: The theory of error-correcting codes, North-Holland 1977. | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Tělesná výchova 1** | | | | |
| **Typ předmětu** | cvičení | | | **doporučený ročník / semestr** | 1ZS |
| **Rozsah studijního předmětu** | 0/2 | **hod.** | 26 | **kreditů** | 1 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z | | **Forma výuky** | cvičení | | |
| **Další požadavky na studenta** | Základní pohybové schopnosti | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | KTV | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *V průběhu bakalářského studia jsou povinné celkem čtyři semestry tělesné výchovy. Tento předmět si zapisují studenti zpravidla v zimním semestru 1.ročníku. Zápis tohoto předmětu je kapacitně omezen.* | | | | | |
|  | | | | | | |
| **Studijní literatura** |  | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Tělesná výchova 2** | | | | |
| **Typ předmětu** | cvičení | | | **doporučený ročník / semestr** | 1LS |
| **Rozsah studijního předmětu** | 0/2 | **hod.** | 26 | **kreditů** | 1 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z | | **Forma výuky** | cvičení | | |
| **Další požadavky na studenta** | Základní pohybové schopnosti | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | KTV | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *V průběhu bakalářského studia jsou povinné celkem čtyři semestry tělesné výchovy. Tento předmět si zapisují studenti zpravidla v letním semestru 1.ročníku. Zápis tohoto předmětu je kapacitně omezen.* | | | | | |
|  | | | | | | |
| **Studijní literatura** |  | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Tělesná výchova 3** | | | | |
| **Typ předmětu** | cvičení | | | **doporučený ročník / semestr** | 2ZS |
| **Rozsah studijního předmětu** | 0/2 | **hod.** | 26 | **kreditů** | 1 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z | | **Forma výuky** | cvičení | | |
| **Další požadavky na studenta** | Základní pohybové schopnosti | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | KTV | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *V průběhu bakalářského studia jsou povinné celkem čtyři semestry tělesné výchovy. Tento předmět si zapisují studenti zpravidla v zimním semestru 2.ročníku. Zápis tohoto předmětu je kapacitně omezen.* | | | | | |
|  | | | | | | |
| **Studijní literatura** |  | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Tělesná výchova 4** | | | | |
| **Typ předmětu** | cvičení | | | **doporučený ročník / semestr** | 2LS |
| **Rozsah studijního předmětu** | 0/2 | **hod.** | 26 | **kreditů** | 1 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z | | **Forma výuky** | cvičení | | |
| **Další požadavky na studenta** | Základní pohybové schopnosti | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | KTV | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *V průběhu bakalářského studia jsou povinné celkem čtyři semestry tělesné výchovy. Tento předmět si zapisují studenti zpravidla v letním semestru 2.ročníku. Zápis tohoto předmětu je kapacitně omezen.* | | | | | |
|  | | | | | | |
| **Studijní literatura** |  | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Teorie čísel** | | | | |
| **Typ předmětu** | přednáška a cvičení | | | **doporučený ročník / semestr** | 2LS |
| **Rozsah studijního předmětu** | 2/2 | **hod.** | 52 | **kreditů** | 5 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z+Zk | | **Forma výuky** | přednáška a cvičení | | |
| **Další požadavky na studenta** |  | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | Mgr. Vítězslav Kala, Ph.D. | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Cyklické grupy: Charakterizace cyklických grup, jejich podgrupy a endomorfismy, Eulerova funkce, Eulerova veta, primitivní prvky, cínská zbytková veta, struktura Z\_n\*, Rabin-Milleruv test, RSA.*  *Kvadratické zbytky: Gaussovská celá císla, kvadratické zbytky a Legendruv symbol, charaktery, Gaussovy soucty, cyklotomické polynomy, kvadratická reciprocita, Jacobiho symbol.*  *Počet prvočísel: Čebyševovy odhady, Bertrandův postulát.*  *Řetězové zlomky: Dobré aproximace a řetězové zlomky.* | | | | | |
|  | | | | | | |
| **Studijní literatura** | A. Drápal: Teorie císel a RSA, skripta;  Ireland, Rosen: A Classical Introduction to Modern Number Theory;  Borevic, Šafarevic: Number Theory, Academic Press 1966;  Riesel: Prime numbers and computer methods for factorization, Birkhäuser 1985;  Cohen: A course in computational algebraic number theory, Springer-Verlag 1993. | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Teorie informace** | | | | |
| **Typ předmětu** | přednáška a cvičení  základní teoretický předmět profilujícího základu | | | **doporučený ročník / semestr** | 2LS |
| **Rozsah studijního předmětu** | 3/1 | **hod.** | 52 | **kreditů** | 6 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z+Zk | | **Forma výuky** | přednáška a cvičení | | |
| **Další požadavky na studenta** |  | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | doc. Mgr. Štěpán Holub, Ph.D. | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Entropie a její vlastnosti: maximalizace entropie, podmíněná entropie, vzájemná informace, data processing theorem, Fanovo lemma.*  *Kódování zdroje: Huffmanovo kódování, typické posloupnosti, střední délka zprávy.*  *Kapacita kanálu a Shannonovy věty: obecný případ, binární symetrický kanál, gaussovský kanál.*  *Skrytý Markovův model.*  *Viterbiho a Fanův dekódovací algoritmus.* | | | | | |
|  | | | | | | |
| **Studijní literatura** | Thomas M. Cover, Joy A. Thomas: Elements of Information Theory, Wiley 2006. | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Úvod do kryptografie** | | | | |
| **Typ předmětu** | přednáška a cvičení  základní teoretický předmět profilujícího základu | | | **doporučený ročník / semestr** | 2LS |
| **Rozsah studijního předmětu** | 2/2 | **hod.** | 52 | **kreditů** | 5 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z+Zk | | **Forma výuky** | přednáška a cvičení | | |
| **Další požadavky na studenta** |  | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | RNDr. Andrew Kozlík, Ph.D. | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Úvod: klasické šifry a jejich prolamování, typy útoku.*  *Blokové šifry: šifra DES, triple DES, meet-in-the-middle útok, šifra AES, klasické operacní režimy blokových šifer, padding.*  *Proudové šifry: posuvné registry s lineární zpetnou vazbou, šifra A5/1.*  *Hashovací funkce: aplikace hashovacích funkcí, narozeninový paradox, složitost hledání vzoru a kolize hrubou silou, Merkleovo-Damgĺrdovo schéma, autentizacní kód zprávy.*  *Asymetrická kryptografie: RSA, Hĺstaduv útok na malý verejný exponent, digitální podpis, slepý podpis, Diffieho-Hellmanuv protokol, perfect forward secrecy, princip Pohligova-Hellmanova algoritmu, ElGamaluv šifrovací systém, ElGamalovo podpisové schéma a algoritmus DSA.* | | | | | |
|  | | | | | | |
| **Studijní literatura** | Serge Vaudenay: A Classical Introduction to Cryptography, Springer, 2006.  Douglas R. Stinson: Cryptography: Theory and Practice, Third Edition, CRC Press, 2005.  Hans Delfs, Helmut Knebl: Introduction to Cryptography, Springer, 2015.  Christof Paar, Jan Pelzl: Understanding Cryptography: A Textbook for Students and Practitioners, Springer, 2010.  Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone: Handbook of Applied Cryptography, CRC Press, 1996.  Joan Daemen, Vincent Rijmen: The Design of Rijndael: AES - The Advanced Encryption Standard, Springer, 2002. | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Úvod do matematické logiky** | | | | |
| **Typ předmětu** | přednáška | | | **doporučený ročník / semestr** | 3LS |
| **Rozsah studijního předmětu** | 2/0 | **hod.** | 26 | **kreditů** | 3 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Zk | | **Forma výuky** | přednáška | | |
| **Další požadavky na studenta** |  | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | prof. RNDr. Jan Krajíček, DrSc. | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Základy výrokové a predikátové logiky a nejzákladnější pojmy a fakta z teorie modelů a teorie množin, neúplnost a nerozhodnutelnost, Gödelovy věty.* | | | | | |
|  | | | | | | |
| **Studijní literatura** | J.R.Shoenfield: Mathematical logic; Addison-Wesley Publishing Company, London . Don Mills, Ontario, 1967.  V.Švejdar, Logika: neúplnost, složitost a nutnost, Academia, Praha, 2002.  R.Cori, D.Lascar, Mathematical Logic (part I.), Oxford University Press, 2000.  H.D.Ebinghaus, J.Flum, W.Thomas, Mathematical Logic, 2.vyd., Springer Verlag, 1994.  literatura na webu (a další literatura): viz http://www.karlin.mff.cuni.cz/~krajicek/ml.html | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Úvod do počítačových sítí** | | | | |
| **Typ předmětu** | přednáška | | | **doporučený ročník / semestr** | 3LS |
| **Rozsah studijního předmětu** | 2/0 | **hod.** | 26 | **kreditů** | 3 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Zk | | **Forma výuky** | přednáška | | |
| **Další požadavky na studenta** |  | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | RNDr. Martin Kruliš, Ph.D. | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Základní principy a vlastnosti síťové komunikace, taxonomie sítí dle různých aspektů, historický vývoj sítí a Internetu.*  *Vrstevnatá filozofie, síťový model ISO/OSI a vztah k rodině protokolů TCP/IP.*  *Adresace uzlů a služeb (MAC, IP, TCP/UDP porty, DNS, URI), princip směrování, překlad adres.*  *Transportní protokoly (TCP, UDP) a jejich fungování.*  *Elektronická pošta a související protokoly (SMTP, POP3, IMAP).*  *Hlasové služby (VoIP) a související protokoly (SIP).Vybrané důležité aplikační protokoly TCP/IP (DNS, HTTP, FTP, SSH).*  *Základy kryptografie, zajištění utajení a integrity informace, autentizace, sytém certifikátů, vztah k TCP/IP (SSL a TLS).*  *Principy výstavby a správy internetových sítí, správa adresace a směrování, autonomní systémy.*  *Základy fungování vrstev síťového rozhraní a způsoby přenosu dat (Ethernet, Wi-Fi).*  *Historie webu, webové stránky a webové aplikace, základy HTML a CSS.* | | | | | |
|  | | | | | | |
| **Studijní literatura** |  | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Úvod do strojového učení** | | | | |
| **Typ předmětu** | přednáška a cvičení | | | **doporučený ročník / semestr** | 3ZS |
| **Rozsah studijního předmětu** | 2/2 | **hod.** | 52 | **kreditů** | 6 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z+Zk | | **Forma výuky** | přednáška a cvičení | | |
| **Další požadavky na studenta** |  | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | Mgr. Barbora Vidová Hladká, Ph.D. | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Strojové učení - základní koncepty. Co je strojové učení, ukázky praktických aplikací, teoretické základy strojového učení. Učení s učitelem, učení bez učitele. Klasifikační a regresní úlohy. Trénovací a testovací příklady. Vektory příznaků. Cílový atribut a predikční funkce. Vývojový cyklus strojového učení. Prokletí dimenzionality. Metody shlukování.*  *Rozhodovací stromy. Algoritmus učení pomocí rozhodovacích stromů, kritéria větvení, prořezávání.*  *Lineární regrese. Metoda nejmenších čtverců.*  *Učení založené na příkladech. Algoritmus k-NN.*  *Logistická regrese. Diskriminativní klasifikátor.*  *Naivní Bayesův klasifikátor. Bayesovské sítě.*  *Metoda podpůrných vektorů. Klasifikátor pro lineárně separabilní třídy, klasifikátor pro lineárně neseparabilní třídy. Jádrové funkce. Klasifikace do více tříd.*  *Metody pro kombinaci více prediktorů. Bagging a boosting. Algoritmus AdaBoost. Metoda náhodných lesů.*  *Parametry v SU. Ladění parametrů učení. Systematické prohledávání. Metoda největšího spádu. Metoda maximální věrohodnosti.*  *Vyhodnocování experimentů. Práce s testovacími daty. Chyba na vzorku, generalizační chyba. Křížová validace, metoda one-leave-out. Metoda bootstrap. Míry úspěšnosti. Vyhodnocování binárních klasifikátorů. Křívka ROC.*  *Statistické testy. Statistické hypotézy, Jednovýběrový a dvouvýběrový t-test, chí-kvadrát test dobré shody. Hladina významnosti, p-hodnota. Použití statistických testů pro vyhodnocování klasifikátorů. Hladina spolehlivosti, intervaly spolehlivosti.*  *Přetrénování. Jak odhalit a zabránit. Prořezávání rozhodovacích stromů. Regularizace.*  *Redukce dimenze. Obecné principy výběru příznaků. Filtry, obalovací a vestavěné metody. Výběr příznaků pomocí informačního zisku. Analýza hlavních komponent.*  *Základy neuronových sítí. Jednoduchý perceptron. Neuronové sítě s jednou skrytou vrstvou. Zpětná propagace. Vícevrstvé dopředné modely. Poznámky k hlubokému učení.* | | | | | |
|  | | | | | | |
| **Studijní literatura** |  | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Vypracování a konzultace bakalářské práce** | | | | |
| **Typ předmětu** | seminář  předmět profilujícího základu | | | **doporučený ročník / semestr** | 3LS |
| **Rozsah studijního předmětu** | 0/4 | **hod.** | 52 | **kreditů** | 6 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z | | **Forma výuky** | seminář | | |
| **Další požadavky na studenta** |  | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | Vedoucí bakalářské práce | | | | | |
| **Zapojení garanta do výuky předmětu** | 100% | | | | | |
| **Stručná anotace předmětu** | *Výuka probíhá formou individuálních konzultací mezi studentem a vedoucím bakalářské práce.* | | | | | |
|  | | | | | | |
| **Studijní literatura** | Podle zadání bakalářské práce. | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Základy kombinatoriky a teorie grafů** | | | | |
| **Typ předmětu** | přednáška a cvičení | | | **doporučený ročník / semestr** | 3LS |
| **Rozsah studijního předmětu** | 2/2 | **hod.** | 52 | **kreditů** | 5 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z+Zk | | **Forma výuky** | přednáška a cvičení | | |
| **Další požadavky na studenta** |  | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | prof. RNDr. Jan Kratochvíl, CSc. | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Informativní přehled o základech teoretické. informatiky (výpočetní složitost, NP-úplnost) a algoritmech (lineární programování, grafové algoritmy). Prezentace teoretických partií kombinatoriky a teorie grafů (toky v sítích, faktory grafů, množinové systémy a systémy reprezentantů, Ramseyova teorie).* | | | | | |
|  | | | | | | |
| **Studijní literatura** | L. Kučera: Kombinatorické algoritmy, Státní nakladatelství technické literatury, Praha 1989.  J. Matoušek, J. Nešetřil: Kapitoly z diskrétní matematiky, Karolinum, Praha 2009.  J. Nešetřil: Teorie grafů, Státní nakladatelství technické literatury, 1979. | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R**B-III – Charakteristika studijního předmětu** | | | | | |
| **Název studijního předmětu** | **Základy numerické lineární algebry** | | | | |
| **Typ předmětu** | přednáška a cvičení  základní teoretický předmět profilujícího základu | | | **doporučený ročník / semestr** | 2ZS |
| **Rozsah studijního předmětu** | 2/1 | **hod.** | 39 | **kreditů** | 4 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dvousemestrální předmět** | Ne | | | | | |
| **Způsob ověření studijních výsledků** | Z+Zk | | **Forma výuky** | přednáška a cvičení | | |
| **Další požadavky na studenta** |  | | | | | |
| **Garant předmětu**  **(ev. vyučující zodpovědný za předmět)** | prof. Ing. Miroslav Tůma, CSc. | | | | | |
| **Zapojení garanta do výuky předmětu** | 30% | | | | | |
| **Stručná anotace předmětu** | *Úvod. Co je numerická matematika. Příklady ukazující, jak je numerická matematika důležitá.*  *Problémy v numerické matematice: přímý problém, inverzní problém, identifikační problém. Chyby v numerické matematice: přímá chyba, zpětná chyba, chyba rezidua. Problém vlastních čísel versus rozklady.*  *Schurova věta a její důsledky.*  *Ortogonalita, QR rozklady, cena výpočtu.*  *LU rozklady a přímé řešení soustav rovnic. Kontrola růstu numerických chyb.*  *Singulární rozklad matice. Úloha nejmenších čtverců.*  *Iterační metody založené na štěpění operátoru. Mocninná metoda pro výpočet vlastních čísel. Myšlenka krylovovských metod.*  *Nelineární algebraické rovnice, Newtonova metoda, metody založené na pevném bodě.*  *Interpolace funkcí, Lagrangeova interpolace, spline funkce.* | | | | | |
|  | | | | | | |
| **Studijní literatura** | E. J. Duintjer Tebbens, I. Hnětynková, M. Plešinger, Z. Strakoš, P. Tichý: Analýza metod pro maticové výpočty - Základní metody, MatfyzPress, Praha, 2012  M. Feistauer, V. Kučera: Základy numerické matematiky, MatfyzPress, Praha, 2014  J. Segethová: Základy numerické matematiky, Skriptum MFF UK, 2002  A. Greenbaum, T. P. Chartier: Numerical Methods: Design, Analysis and Computer Implementation of Algorithms, Princeton Universtity Press, 2012  A. Quarteroni, R. Sacco, F. Saleri: Numerical Mathematics, Springer-Verlag, 2000  D. S. Watkins: Fundamentals of Matrix Computations, Wiley Interscience, New York, 2010 (third edition) | | | | | |
|  | | | | | | |
| **Informace ke kombinované nebo distanční formě** | | | | | |  |
| **Rozsah konzultací (soustředění)** | |  | | | **hodin** | |
|  | | | | | | |
| **Vzory studijních distančních textů a multimediálních pomůcek** | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| **Doplňující údaje u předmětu obsahujícího odbornou praxi** | |
| **Přehled pracovišť, na kterých má být praxe uskutečňována** | **Smluvně zajištěno** |
|  |  |
|  |  |
|  |  |
|  |  |
| **Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)** | |
|  | |