MODULIO APRAŠAS

Modulio pavadinimas	Kodas
Kriptografija ir informacijos sauga	

Dėstytojas (-ai)	Padalinys (-iai)
Koordinuojantis: Vilius Stakėnas **Kitas (-i):**	Informatikos katedra Matematikos ir informatikos fakultetas Vilniaus universitetas

Studijų pakopa	Dalyko (modulio) tipas
Pirmoji	Privalomasis

Įgyvendinimo forma	Vykdymo laikotarpis	Vykdymo kalba (-os)
Auditorinė	5 semestras	Lietuvių, anglų

Reikalavimai studijuojančiajam
Išankstiniai reikalavimai: bendrųjų matematikos kursų žinios, programavimo kokia nors kalba įgūdžiai

Modulio apimtis kreditais	Visas studento darbo krūvis	Kontaktinio darbo valandos	Savarankiško darbo valandos
5	137	68	69

Modulio tikslas: studijų programos ugdomos kompetencijos

Modulio tikslas:
ugdyti kriptografinės duomenų apsaugos uždavinių ir galimybių suvokimą, šiuolaikinės kriptografijos algoritmų veikimo supratimą, gebėjimą įvertinti jų saugumą, taikyti juos bendroje duomenų apsaugos sistemoje, atlikti atskirų atvejų kriptoanalizę.

Bendrosios kompetencijos:
- Žinias pritaikyti praktikoje (*BK2*).
- Organizuoti ir planuoti darbus, dirbti individualiai ir grupėje (*BK3*).

Dalykinės kompetencijos:
- Tolydžiųjų ir diskrečiųjų matematinių struktūrų analizės ir taikymo (*DK4*)
- Algoritmų kūrimo ir jų sudėtingumo įvertinimo (*DK5*).
- Informacijos valdymo (*DK9*).

Modulio studijų siekiniai	Studijų metodai	Vertinimo metodai
Suvoks šiuolaikinių simetrinių (blokinių ir srautinių) kriptosistemų konstravimo principus, mokės juos taikyti, gebės atlikti atskirų atvejų kriptoanalizę, žinos, kaip veikia šiuolaikiniai blokiniai ir srautiniai šifrai, mokės juos taikyti.	Paskaitos: algoritmų struktūros pagrindų dėstymas, programų pavyzdžiai, veikimo demonstravimas, individualios teorijos suvokimą tikrinančios užduotys, praktinio darbo užduotys ir konsultacijos.	Kriptografinių algoritmų taikymo, programavimo, analizės užduočių rezultatų peržiūra, aptarimas, kontrolinių užduočių bei egzamino klausimų atsakymų peržiūra.
Supras matematinius viešojo rakto kriptografijos pagrindus, skaičiavimo algoritmus, mokės juos programuoti ir taikyti įvairuose kriptografiniuose protokoluose.		
Suvoks, kaip veikia viešojo rakto kriptosistemos ir skaitmeninio parašo schemos, žinos pagrindinius praktikoje naudojamų šifravimo ir skaitmeninio parašo algoritmus, gebės juos programuoti ir taikyti, atlikti atskirų atvejų kriptoanalizę.		

Suvoks prieigos kontrolės mechanizmų taikymo principus, žinos ir mokės modeliuoti įvairios paskirties kriptografinius protokolus, suvoks informacijos apsaugos problemas susijusias su programinės įrangos naudojimu, atakų vykdomų kompiuteriniais tinklais grėsmėmis.		

Temos	**Kontaktinio darbo valandos**							**Savarankiškų studijų laikas ir užduotys**	
	Paskaitos	Konsultacijos	Seminarai	Pratybos	Laboratoriniai darbai	Praktika	**Visas kontaktinis darbas**	**Savarankiškas darbas**	**Užduotys**
1. Kriptografijos uždaviniai: informacijos slaptumas, duomenų ir šaltinio autentifikavimas, prieinamumas, išsižadėjimų prevencija. Kriptosistemos sąvoka. Saugumo vertinimo kriterijai. Algoritmai ir protokolai.	2						**2**	**2**	Savarankiškos literatūros studijos.
2. Klasikinės kriptografijos metodai. Perstatų ir keitinių šifrai. Kriptoanalizės metodai. Šifravimo įrenginiai su rotoriais. Enigma struktūra.	4				6		**10**	**8**	Klasikinės kriptografijos keitinių ir perstatų šifrų kriptoanalizė. Vigenere šifro kriptoanalizė. ENIGMA šifro dešifravimas.
3. Simetrinė kriptografija. Blokinių kriptosistemų konstravimo principai: Feistelio schema, perstatų ir keitinių tinklas. Blokinių kriptosistemų standartai (DES, AES) ir kiti praktikoje naudojami šifrai. Blokinių šifrų naudojimo režimai. Kriptoanalizės metodai.	4	1			4		**9**	**7**	Feistelio tipo kriptosistemos programavimas. Blokinių šifrų režimų programavimas.
4. Srautinių šifrų konstravimo principai. Tiesinių registrų sistemos. Kriptoanalizės metodai. Statistiniai rakto srauto vertinimo metodai. Praktikoje naudojami srautiniai šifrai.	4				4		**8**	**7**	Tiesinių registrų sistemos srauto kriptoanalizė. Statistinių srauto testų programavimas.
5. Maišos funkcijos. Maišos funkcijų konstravimas iteracijomis. MD, SHA šeimos maišos funkcijos. Maišos funkcijų taikymas duomenų vientisumui, autentiškumui užtikrinti, duomenų autentifikavimo kodai (MAC).	2				2		**4**	**4**	Maišos funkcijų konstrukcijos, kolizijų sudarymas.
6. Matematiniai viešojo rakto kriptografijos pagrindai. Skaičių teorijos struktūros ir algoritmai: skaičiavimai moduliu, Fermat teorema, kiniškoji liekanų teorema, kvadratiniai lyginiai, diskretieji logaritmai, skaičių skaidymas pirminiais daugikliais.	2				4		**6**	**6**	Skaičiavimo duotu moduliu, skaičių skaidymo, diskrečiųjų logaritmų skaičiavimo užduotys.
7. Viešojo rakto kriptografija: šifrai ir skaitmeniniai parašai. Kuprinės, RSA, Rabino, ElGamalio kriptosistemos, kriptoanalizės atvejai. RSA, ElGamalio, DSS, Rabino skaitmeninių parašų schemos, jų saugumo analizė.	6	1			6		**13**	**10**	Kuprinės, RSA, Rabino šifrų kriptoanalizės užduotys. ElGamalio šifro dešifravimo, skaitmeninio parašo sudarymo užduotys. Kitos skaitmeninių parašų schemos.

8. Paslapties padalijimo protokolai: Shamiro, Assmutho-Bloomo paslapties padalijimo su slenksčiu protokolai, paslapties padalijimas pagal leidimų struktūrą. Netiesioginių įrodymų (zero knowledge proofs) protokolai ir jų taikymai.	2				2		**4**	**4**	Padalytos paslapties atskleidimo, paslapties padalijimo užduotys. Netiesioginių įrodymų protokolų modeliavimo užduotys.
9. Prieigos kontrolės mechanizmai, autorizacija ir autentifikavimas. Slaptažodžiai, autentifikavimo protokolai. Ryšių praktikoje naudojami protokolai: TSL, Kerberos, WEP.	2				2		**4**	**4**	Autentifikavimo protokolų bei atakų modeliavimo užduotys.
10. Informacijos saugumo sistemos pažeidimai susiję su pragramine įranga bei jos naudojimu: virusai, trikdžiai, atakos. Operacinės sistemos ir informacijos sauga.	2						**2**	**2**	Savarankiškos literatūros studijos.
11. Įvairūs kriptografijos metodų taikymai: skaitmeniniai pinigai, elektroniniai rinkimai ir aukcionai.	2				2		**2**	**3**	Skaitmeninių pinigų elektroninių rinkimų protokolų modeliavimo užduotys.
12. Pasirengimas egzaminui ir egzaminavimas							**2**	**12**	
Iš viso	**32**	**2**			**32**		**68**	**69**	

Vertinimo strategija	**Svoris proc.**	**Atsiskaitymo laikas**	**Vertinimo kriterijai**
Darbas auditorijoje laboratorinių darbų metu bei savarankiškas uždavinių sprendimas namuose	40	Semestro metu	Individualios užduotys skiriamos per pratybas. Sprendimai, kuriuos reikalaujama pateikti iki kitų pratybų, vertinami taškais. Sukauptas balas apskaičiuojamas pagal formulę: 4 □ sukauptas taškų skaičius/maksimalus taškų skaičius.
Aktyvios kurso temų studijos semestro metu	Iki 30	Semestro metu	Paskaitos pabaigoje klausytojams pateikiamos nesudėtingos individualios užduotys, tikrinančios paskaitoje (ir anksčiau) išdėstytos medžiagos suvokimą. Atsakymai raštu vertinami iki 0,2 balo. Maksimali už kontrolines užduotis sukaupto balo reikšmė - 3.
Egzaminas	30-60	Sesijos metu	Egzamino užduotį sudaro klausimų rinkinys, kurio vertė lygi 6-x, x - per semestrą už kontrolines užduotis sukauptas balas.

Autorius	**Leidimo metai**	**Pavadinimas**	**Periodinio leidinio Nr. ar leidinio tomas**	**Leidimo vieta ir leidykla ar internetinė nuoroda**
Privalomoji literatūra				
V. Stakėnas	2007	Kodai ir šifrai		TEV, http://www.mif.vu.lt/lmd/kodai_sifrai.pdf
D. Stinson	2005	Cryptography Theory and Practice		Taylor & Francis
Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone	2001	Handbook of applied cryptography		http://cacr.uwaterloo.ca/hac/
Papildoma literatūra				
N. Smart	2002	Cryptography, An Introduction : Third Edition		http://www.cs.bris.ac.uk/~nigel/Crypto_Book/
B. Schneier	1995	Applied Cryptography: Protocols, Algorithms, and Source Code in C		Wiley