I. Содржина на студиските програми

Во следните табели е даден список на предметите потребни за изучување на модулите Кодирање и Криптографија и сигурност на компјутерски системи.

1. Модул Кодирање

Име на предметот	Семестар		кредити
Напредни алгебарски структури	9		8
Случајни процеси	9		8
Теорија на кодирање	9		8
Изборен	9		6
Теорија на информации 2		10	8
Изборен		10	6
Магистерска тема		10	16

Задолжителни предмети кои го формираат модулот

зимски семестар					
	Предмет	Предавања	Аудиториски	Лабораториски	кредити
9	Напредни алгебарски структури	30	30		8
9	Случајни процеси	30	30		8
9	Теорија на кодирање	30	30	15	8
	Вкупно задолжителни				
	Вкупно	90	90	15	24

летен семестар					
	Предмет	Предавања	Аудиториски	Лабораториски	кредити
10	Теорија на информации 2	30	30		8
	Вкупно задолжителни				
	Вкупно	30	30		8

Опис на предметите

Во следните табели се дадени описите на задолжителните предмети на овој модул. Описот на изборните предмети е даден на крајот на оваа глава.

Име на предметот	**Напредни алгебарски структури**		
Наставник	Проф. д-р Смиле Марковски		
Статус	Задолжителен	**Кредити**	8
Семестар	9	**Неделен фонд**	2+2
Условеност			
Начин на реализација	Предавања, вежби, семинари		
Цели	Воведување на алгебраските структури кои ке се користат во другите предмети од студиите		
Содржини	Изучување на структурите и својствата на:		

	• групоидите: полугрупи, групи и квазигрупи • алгебрите со повеќе операции: прстени, полиња, булови алгебри • релационите алгебри Посебен осврт на конечните алгеарски структури од претходните видови, кои се значајни за примените.
Основна литература	1) Ѓ. Чупона: Предавања по алгебра, УКИМ Скопје 2) A. Clark: Elements of Abstract algebra, Dover Publ. Inc., New York

Име на предметот	**Случајни процеси**		
Наставник	Проф. Д-р Верица Бакева		
Статус	Задолжителен	**Кредити**	**7**
Семестар	9	**Неделен фонд**	2+2
Условеност			
Начин на реализација	Предавања, вежби, семинари		
Цели	Да се оспособат студентите да моделираат случајни процеси		
Содржини	Случајни процеси: дефиниција, карактеристики, класификација, трансформации. Стационарност на случајни процеси. Процеси со независни стационарни прираснувања; Маркови процеси со дискретно и непрекинато множество состојби: процеси на раѓање и умирање; Вериги на Марков, Вгнездени вериги на Марков. Специјални случајни процеси: случајно талкање, Поасонов, Винеров процес. Разгранувачки процеси. Процеси на обнова.		
Основна литература	Papullis: *Probability, Statistics and Stochastic Processes*., D.R.Cox, H.D.Miller: *The Theory of Stochastic Process*., Jean Walrand: Lecture Notes on Probability Theory and Random Processe, Ж. Пауше: *Веројатност, статистика и случајни процеси*.		

Име на предметот	**Теорија на кодирање**		
Наставник	Проф. д-р Верица Бакева/Проф. д-р Смиле Марковски		
Статус	Задолжителен	**Кредити**	8
Семестар	9	**Неделен фонд**	2+2+1
Условеност			
Начин на реализација	Предавања, вежби, семинари		
Цели	Запознавање на студентите со основните кодови за откривање и кодовите за поправање на грешки.		
Содржини	Математички подготовки за потребите на теоријата на кодирање: теорија на групи, теорија на конечни полиња, полиноми над конечни прстени и полиња, стохастички процеси, теорија на информации и ентропија. Основни дефиниции и својства на теорија на кодови. Теореми на Шанон. Групни кодови. Кодови што откриваат грешки и CRC. Кодови што поправаат грешки. Кодови на Рид-Милер и кодови на Рид-Соломон. Алгебарски кодови. Турбо кодови. LDPC (линеарно густи проверки на парност) кодови. Случајни проточни кодови.		
Основна литература	1. Vanstone, S.A., van Ooschot, P.S. (1989) *An Introduction to Error Correcting Codes with Applications*, Kluwer Academic Publishers, Boston 2. Hill, R. (1986) *A First Course of Coding Theory*, Clarendon Press,		

	Oxford 3. Torleiv K., (2007) *Codes for error detection*, World scientific

Име на предметот	**Теорија на информации 2**		
Наставник	Проф. д-р Верица Бакева		
Статус	Задолжителен	**Кредити**	8
Семестар	10	**Неделен фонд**	2+2
Условеност			
Начин на реализација	Предавања, вежби, семинари		
Цели	Воведување на математички модел на комуникациски систем.		
Содржини	Комуникациски систем. Ентропија. Информација. Компресија на податоци: Кодирање со загуби. Asymptotic Equipartition Property (AEP) за независни случајни променливи. Теорема на Shannon за кодирање на изворен сигнал. Кодирање без загуби. Симболични кодови. Проблем на единствено декодирање. Моментални кодови. Крафтово неравенство. Теорема за бесшумно кодирање. Конструкција на оптимални кодови. Комуникација преку канал со шум (Комуникациски канал. Модели на комуникациски канал. Дискретен канал без меморија. Капацитет на дискретен канал без меморија). Извори на информации: Вериги на Марков. Извор на информации. Регуларен Марков извор. Ентропија на извор. Ред на извор. Апроксимација на општ извор на информации со извор од конечен ред. Ергодичен извор. Теорема на Shannon – McMillan (Asymptotic Equipartition Property (AEP)). Дискретен канал со меморија: Модели на дискретен канал со меморија. Канал со конечно множество состојби. Капацитет на општ дискретен канал. Теорема за кодирање за регуларен канал со конечно множество состојби. Непрекинати канали: Ентропија на непрекинати случајни променливи. Ентропија на Гаусова случајна променлива. Видови непркинати канали. Гаусов канал (временски дискретен). AEP за непрекинати случајни променливи. Теорема за кодирање за Гаусов канал.		
Основна литература	a. Thomas M. Cover, Joy A. Thomas: *Elements of Information Theory*, John Wiley & Sons, Inc. b. Ž. Pauše: *Uvod u teoriju informacije*, Školska knjiga, Zagreb c. R.Ash: *Information Theory*, Dover Publication, Inc.		

2. *Модул Криптографија и сигурност на компјутерски системи*

Име на предметот	Семестар		Кредити
Напредни алгебарски структури	9		8
Напредна криптографија	9		8
Информациска сигурност	9		8
Изборен	9		6
Криптоанализа		10	8
Изборен		10	6
Магистерска тема		10	16

Задолжителни предмети кои го формираат модулот

зимски семестар					
	Предмет	Предавања	Аудиториски	Лабораториски	кредити
9	Напредни алгебарски структури	30	30		8
9	Напредна криптографија	30	30	15	8
9	Информациска сигурност	30	30		8
	Вкупно задолжителни				
	Вкупно	90	90	15	24

летен семестар					
	Предмет	Предавања	Аудиториски	Лабораториски	кредити
10	Криптоанализа	30	30		8
	Вкупно задолжителни				
	Вкупно	30	30		8

Опис на предметите

Во следните табели се дадени описите на задолжителните предмети на овој модул. Описот на изборните предмети е даден на крајот на оваа глава.

Име на предметот	**Напредни алгебарски структури**		
Наставник	Проф. д-р Смиле Марковски		
Статус	Задолжителен	**Кредити**	8
Семестар	9	**Неделен фонд**	2+2
Условеност			
Начин на реализација	Предавања, вежби, семинари		
Цели	Воведување на алгебраските структури кои ке се користат во другите предмети од студиите		
Содржини	Изучување на структурите и својствата на • групоидите: полугрупи, групи и квазигрупи • алгебрите со повеќе операции: прстени, полиња, булови алгебри • релационите алгебри Посебен осврт на конечните алгеарски структури од претходните видови, кои се значајни за примените.		
Основна литература	1) Ѓ. Чупона: Предавања по алгебра, УКИМ Скопје 2) A. Clark: Elements of Abstract algebra, Dover Publ. Inc., New York		

Име на предметот	**Напредна криптографија**		
Наставник	Проф. д-р Смиле Марковски, доц. д-р Весна Димитрова		
Статус	Задолжителен	**Кредити**	8
Семестар	9	**Неделен фонд**	2+2+1
Условеност			
Начин на реализација	Предавања, вежби, семинари		
Цели	Оспособеност на студентите конкретно да ги реализираат посебните видови криптографски пакети		
Содржини	Алгоритми за генерирање на огромни прости броеви и заемно прости броеви; реализација на алгоритми за симетрични крипто системи; реализација на РСА и Ел Гамал системи со јавни клучеви; реализација на протоколи за размена на клучеви; разбивање на попрости крипто системи		
Основна литература	T. Baigneres, P. Junod at al.: A classiacal introduction to cryptography exercise book, Springer, 2006		

Име на предметот	**Криптоанализа**		
Наставник	Проф. д-р Смиле Марковски, доц. д-р Весна Димитрова		
Статус	Задолжителен	**Кредити**	8
Семестар	10	**Неделен фонд**	2+2
Условеност			
Начин на реализација	Предавања, вежби, семинари		
Цели	Изучување на основните алатки за криптоанализа		
Содржини	Видови на напади со груба сила, статистички напади, диференцијална и линеарна криптоанализа, претставувања на крипто системи како булови функции и испитувања на својствата за линеарност,		

	специјални видови напади за посебни крипто продукти (хаш функции, блок шифривуаци, со јавни клуцеви, протоколи)
Основна литература	1) N. Smart: Introduction to cryptography, McGraw-Hill 2003 2) S. Vaudenay: A classical introduction to cryptography – Applications for comunications security, Springer, 2006

Име на предметот	**Информациска сигурност**		
Наставник	Проф. Д-р Смиле Марковски, доц. д-р Весна Димитрова		
Статус	Задолжителен	**Кредити**	8
Семестар	9	**Неделен фонд**	2+2
Условеност			
Начин на реализација	Предавања, вежби, семинари		
Цели	Изучување на основните сигурносни модели за контрола на пристап, на протоколи и софтвер за компјутерски конфигурации		
Содржини	Методи за автентикација, пасворди, биометрика, два-факторска автентикација, авторизација, пристап до контролна амтрицаповече степенски модели на сигурност, огнени ѕидови, детекција на напаѓачи, едноставни протоколи за автентикација,ССЛ, софтверска несигурност, вируси, црви, временски бомбифункции за сигурност на оперативни системи		
Основна литература	1) Mark Stamp: Information security principles and practice, Wiley-Interscience 2) M. Bishop: Computer security – Art and science, Addison-Wesley, 2003		

3. Изборни предмети

Во следните табели се дадени описите за изборните предмети кои важат за сите модули дефинирани во оваа насока. Студентите исто така можат да изберат како изборен предмет и предмет од листите на задолжителни и изборни предмети од останатите насоки акредитирани во Втор циклус на студии на од насоките Инженерство на интелигентни системи и Компјутерски науки при ФИНКИ.

Изборни предмети					
	Предмет	Предавања	Аудиториски	Лабораториски	кредити
	Безбедност на компјутерски мрежи	30	15	15	7
	Информациска сигурност	30	30		8
	Криптоанализа	30	30		8
	Математичка логика	30	30		8
	Напредна криптографија	30	30	15	8
	Случајни процеси	30	30		8
	Теорија на информации 2	30	30		8
	Теорија на кодирање	30	30	15	8
	Формални јазици и автомати	30	30	15	8

Опис на предметите

Во следните табели се дадени описите на предмети (задолжителни и изборни).

Име на предметот	**Безбедност на компјутерски мрежи**		
Наставник	Проф. д-р Марјан Гушев, , доц. д-р Боро Јакимовски		
Статус	Изборен	**Кредити**	7
Семестар	9 или 10	**Неделен фонд**	2+1+1
Условеност			
Начин на реализација	Предавања, вежби, домашни задачи, семинарски		
Цели	Детален и практичен преглед на мрежни и интернет сигурносни апликации и стандарди. Конкретна примена на криптографијата, покривајќи алгоритми и протоколи кои се основата на мрежните сигурни апликации, енкрипција, дигитални потписи и размена на клучеви		
Содржини	OSI сигурносен модел, сигурносни напади, сервиси и механизми, модели на интернет сигурност, интернет сигурносни стандарди, протоколи автентикација и авторизација, сигурност на електронска пошта, IP сигурност, Web сигурност и менаџмент на мрежната сигурност		
Основна литература	William Stallings, Network Security Essentials: Applications and Standards		

Име на предметот	**Информациска сигурност**		
Наставник	Проф. д-р Смиле Марковски, доц. д-р Весна Димитрова		
Статус	Изборен	**Кредити**	8
Семестар	9 или 10	**Неделен фонд**	2+2
Условеност			
Начин на реализација	Предавања, вежби, домашни задачи, семинарски		
Цели	Изучување на основните сигурносни модели за контрола на пристап, на протоколи и софтвер за компјутерски конфигурации		
Содржини	Методи за автентикација, пасворди, биометрика, два-факторска автентикација, авторизација, пристап до контролна амтрицаповече степенски модели на сигурност, огнени ѕидови, детекција на напаѓачи, едноставни протоколи за автентикација,ССЛ, софтверска несигурност, вируси, црви, временски бомбифункции за сигурност на оперативни системи		
Основна литература	1) Mark Stamp: Information security principles and practice, Wiley-Interscience 2) M. Bishop: Computer security – Aet and science, Addison-Wesley, 2003		

Име на предметот	**Криптоанализа**		
Наставник	Проф. д-р Смиле Марковски, доц. д-р Весна Димитрова		
Статус	Изборен	**Кредити**	8
Семестар	9 или 10	**Неделен фонд**	2+2
Условеност			
Начин на реализација	Предавања, вежби, домашни задачи, семинарски		
Цели	Изучување на основните алатки за криптоанализа		
Содржини	Видови на напади со груба сила, статистички напади, диференцијална и линеарна криптоанализа, претставувања на крипто системи како булови функции и испитувања на својствата за линеарност, специјални видови напади за посебни крипто продукти (хаш функции, блок шифривуаци, со јавни клуцеви, протоколи)		
Основна литература	1) N. Smart: Introduction to cryptography, McGraw-Hill 2003 2) S. Vaudenay: A classical introduction to cryptography – Applications for comunications security, Springer, 2006		

Име на предметот	**Математичка логика**		
Наставник	Проф. д-р Смиле Марковски		
Статус	Изборен	**Кредити**	8
Семестар	9 или 10	**Неделен фонд**	2+2
Условеност			
Начин на реализација	Предавања, вежби, домашни задачи, семинарски		
Цели	Оснозавање на основните поими и својства на исказното и предикатското логичко сметање и примената во информатиката		
Содржини	Исказно сметање: булови операции и интерпретации, исказни формули, логички еквиваленции и замени, семантички таблоа, дедуктивни докази, резолуции, Генценов и Хилбертов систем		

	Предикатско сметање: релации, предикатни формули, интерпретации, логички еквиваленции и замени, семантички таблоа,дедуцтивни форми, функции и терми Резолуциско и логичко програмирање: основна резолуција, замена, унификација, општа резолуција, логичко програмирање Темпоралнa логика.
Основна литература	M. Ben-ari: Mathematical logic for computer science, Prentice Hall, 1992

Име на предметот	**Напредна криптографија**		
Наставник	Проф. д-р Смиле Марковски, доц. д-р Весна Димитрова		
Статус	Изборен	**Кредити**	8
Семестар	9 или 10	**Неделен фонд**	2+2+1
Условеност			
Начин на реализација	Предавања, вежби, домашни задачи, семинарски		
Цели	Оспособеност на студентите конкретно да ги реализираат посебните видови криптографски пакети		
Содржини	Алгоритми за генерирање на огромни прости броеви и заемно прости броеви; реализација на алгоритми за симетрични крипто системи; реализација на РСА и Ел Гамал системи со јавни клуцеви; реализација на протоколи за размена на клучеви; разбивање на попрости крипто системи		
Основна литература	T. Baigneres, P. Junod at al.: A classiacal introduction to cryptography exercise book, Springer, 2006		

Име на предметот	**Случајни процеси**		
Наставник	Проф. Д-р Верица Бакева		
Статус	Изборен	**Кредити**	**7**
Семестар	9 или 10	**Неделен фонд**	2+2
Условеност			
Начин на реализација	Предавања, вежби, домашни задачи, семинарски		
Цели	Да се оспособат студентите да моделираат случајни процеси		
Содржини	Случајни процеси: дефиниција, карактеристики, класификација, трансформации. Стационарност на случајни процеси. Процеси со независни стационарни прираснувања; Маркови процеси со дискретно и непрекинато множество состојби: процеси на раѓање и умирање; Вериги на Марков, Вгнездени вериги на Марков. Специјални случајни процеси: случајно талкање, Поасонов, Винеров процес. Разгранувачки процеси. Процеси на обнова.		
Основна литература	Papullis: *Probability, Statistics and Stochastic Processes*., D.R.Cox, H.D.Miller: *The Theory of Stochastic Process*., Jean Walrand: Lecture Notes on Probability Theory and Random Processe, Ж. Пауше: *Веројатност, статистика и случајни процеси*.		

Име на предметот	**Теорија на информации 2**		
Наставник	Проф. д-р Верица Бакева		
Статус	Изборен	**Кредити**	8
Семестар	9 или 10	**Неделен фонд**	2+2
Условеност			
Начин на реализација	Предавања, вежби, домашни задачи, семинарски		
Цели	Воведување на математички модел на комуникациски систем.		
Содржини	Комуникациски систем. Ентропија. Информација. Компресија на податоци: Кодирање со загуби. Asymptotic Equipartition Property (AEP) за независни случајни променливи. Теорема на Shannon за кодирање на изворен сигнал. Кодирање без загуби. Симболични кодови. Проблем на единствено декодирање. Моментални кодови. Крафтово неравенство. Теорема за бесшумно кодирање. Конструкција на оптимални кодови. Комуникација преку канал со шум (Комуникациски канал. Модели на комуникациски канал. Дискретен канал без меморија. Капацитет на дискретен канал без меморија). Извори на информации: Вериги на Марков. Извор на информации. Регуларен Марков извор. Ентропија на извор. Ред на извор. Апроксимација на општ извор на информации со извор од конечен ред. Ергодичен извор. Теорема на Shannon – McMillan (Asymptotic Equipartition Property (AEP)). Дискретен канал со меморија: Модели на дискретен канал со меморија. Канал со конечно множество состојби. Капацитет на општ дискретен канал. Теорема за кодирање за регуларен канал со конечно множество состојби. Непрекинати канали: Ентропија на непрекинати случајни променливи. Ентропија на Гаусова случајна променлива. Видови непркинати канали. Гаусов канал (временски дискретен). AEP за непрекинати случајни променливи. Теорема за кодирање за Гаусов канал.		
Основна литература	a. Thomas M. Cover, Joy A. Thomas: *Elements of Information Theory*, John Wiley & Sons, Inc. b. Ž. Pauše: *Uvod u teoriju informacije*, Školska knjiga, Zagreb c. R.Ash: *Information Theory*, Dover Publication, Inc.		

Име на предметот	**Теорија на кодирање**		
Наставник	Проф. д-р Верица Бакева/Проф. д-р Смиле Марковски		
Статус	Изборен	**Кредити**	8
Семестар	9 или 10	**Неделен фонд**	2+2+1
Условеност			
Начин на реализација	Предавања, вежби, домашни задачи, семинарски		
Цели	Запознавање на студентите со основните кодови за откривање и кодовите за поправање на грешки.		
Содржини	Математички подготовки за потребите на теоријата на кодирање: теорија на групи, теорија на конечни полиња, полиноми над конечни прстени и полиња, стохастички процеси, теорија на информации и ентропија.		

	Основни дефиниции и својства на теорија на кодови. Теореми на Шанон. Групни кодови. Кодови што откриваат грешки и CRC. Кодови што поправаат грешки. Кодови на Рид-Милер и кодови на Рид-Соломон. Алгебарски кодови. Турбо кодови. LDPC (линеарно густи проверки на парност) кодови. Случајни проточни кодови.
Основна литература	1. Vanstone, S.A., van Ooschot, P.S. (1989) *An Introduction to Error Correcting Codes with Applications*, Kluwer Academic Publishers, Boston 2. Hill, R. (1986) *A First Course of Coding Theory*, Clarendon Press, Oxford 3. Torleiv K., (2007) *Codes for error detection*, World scientific

Име на предметот	**Формални јазици и автомати**		
Наставник	д-р Смиле Марковски, доц. д-р Боро Јакимовски		
Статус	Изборен	**Кредити**	8
Семестар	9 или 10	**Неделен фонд**	2+2+1
Условеност			
Начин на реализација	Предавања, вежби, домашни задачи, семинарски		
Цели	Запознавање со теоријата на пресметливост, теоријата на формални јазици, нивно препознавање, трансформација и обработка.		
Содржини	Вовед во теорија на пресметливост, Конечни автомати, Регулани јазици и регуларни граматики, Својства на регуларни јазици, Контекстно слободни јазици, Поедноставување на контекстно слободни јазици и нормална форма, Пушдаун автомати, Својства на контекстно слободни јазици, Тјурингови машини, Други модели на тјурингови машини, Хиерархија на формални јазици и автомати, Граници на алгоритамското пресметување, Други модели на пресметување.		
Основна литература	Биљана Јанева: Алгоритми и автомати. УКИМ, 1999. Peter Linz: *An Introduction to Formal Languages and Automata,* Jones and Bartlett Publishers, 2006. Thomas A. Sudkamp: *Languages and Machines, 3rd Edition*, Addison-Wesley, 2005.		