Қазақстан Республикасының білім және ғылым министрлігі

Қарағанды мемлекеттік техникалық университеті

Бекітемін
Ғылыми кеңес төрағасы,
ректор, ҚР ҰҒА академигі
Ғазалиев А.М.

_____
«____» _____ 2013ж.

СТУДЕНТКЕ АРНАЛҒАН ПӘН БОЙЫНША ОҚЫТУ БАҒДАРЛАМАСЫ (SYLLABUS)

Krip 3213 «Криптология» пәні

МКЕ 19 «Математикалық қамтамасыз ету» модулі

5В100200 – «Ақпараттық қауіпсіздендіру жүйесі» мамандығы

Ақпараттық технологиялар факультеті

Ақпараттық технология және қауіпсіздік кафедрасы

2013

Алғы сөз

Студентке арналған пән бойынша оқыту бағдарламасы (syllabus) әзірленеді: АТҚ кафедрасының аға оқытушысы Мурых Е.Л.

«Ақпараттық технологиялар және қауіпсіздік» кафедрасының отырысында талқыланған

«____»_____2013 ж. № _____ хаттама

Кафедра меңгерушісі _____ Көккөз М.М. «____»_____2013 ж.

(қолы)

Ақпараттық технологиялар факультетінің оқу-әдістемелік кеңесі мақұлдаған

«____»_____2013 ж. № _____ хаттама

Төраға _____ Мустафина Л.М. «____»_____ 2013 ж.

(қолы)

Оқытушылар туралы мағлұмат және байланыс ақпараты

АТҚ кафедрасының аға оқытушысы Мурых Е.Л.

«Ақпараттық технологиялар және қауіпсіздік» кафедрасы ҚарМТУ (Б.Мира, 56) бас корпусында, 429аудитория, байланыс телефоны 56-75-98 қос. 1028.

Пәннің еңбек көлемділігі

Семестр	Кредиттер саны	ECTS кредиттер	Сабақ түрі					СӨЖ сағаттар саны	Жалпы сағаттар саны	Бақылау түрі
			Қатынас сабақтарының саны			ОСӨЖ сағатта-рының саны	Барлығы сағаттар саны			
			Дәріс	Практикалық сабақтар	Зертханалық сабақтар					
5	3	5	15	15	15	45	90	45	135	КЖ

Пәннің сипаттамасы

«Криптология» пәні базалық пәндердің таңдау бойынша циклына жатады.

Пәннің мақсаты

«Криптология» пәні өз мақсатына криптографиялық әдістермен ақпаратты қорғау және осы әдістердің мысладарын тәжірибеде іске асыру негіз қағидаларын мазмұндауды қояды.

Пәннің міндеттері

Осы пәнді оқу нәтижесінде студенттер:

−Ақпаратты қорғау ұйымдастыру жүйелік тәсілдемесің, берілетін және өңделетін техникалық құралдармен криптографиялық әдістер негізінде қолдану; шифрларының әзірлеу қағидаларың; криптография пайдаланатын математикалық әдістердің негіздерін беру.

түсінік алуы керек:

- ақпараттық қауіпсіздік жүйесі ішінде криптографиялық қорғауның орын туралы;
- қазіргі заманғы шифрлеу алгоритмдер және ақпарат алмасуның криптографиялық хаттамалар туралы;

білуы керек:

− криптографияның негізгі міндеттерін және ұғымдарын;
− шифрларға талаптарын және шифрлардың негеізгі сипаттамаларын;
− ашық мәтіндердің жиілік сипаттамаларын және олардын карапайым симметриялы криптожүйелернің талдауына қолдану;
− типтік ағылмалы және блоктық шифрлер, сонымен қатар асимметриялық криптожүйелер;
− негізгі шифрлеу жүйелерінің криптографиялық хаттамалар ашық кілтермен;

істей алуы керек:

- криптожүйелерді математикалық сипаттау және зерттеу әдістерді қолдану;
- шифрларының крипторгафиялық тұрақтығын бағалау;

практикалық машықтануы керек:

- типтік крипторгафиялық алгоритмдерді пайдалану;
- криптографияда математикалық модельдеу.

Пререквизиттер

Бұл пәнді оқу үшін келесі пәндерді игеру қажет: «Информатика», «Математика», «Алгоритмдік тілдер және бағдарламалау»

Постреквизиттер

«Криптология» пәнін оқу кезінде алынған білім «Ақпаратты қорғау жүйелерін жобалау» пәндерін игеру кезінде қолданылады:

Пәннің тақырыптық жоспары

Тарау атауы, (тақыптар)	Сабақ түрлері бойынша еңбек көлемділігі, сағ.				
	Дәріс	Практикалық саб.	Зертханалық саб.	ОСӨЖ	СӨЖ
1	2	3	4	5	6
1. Компьютерлік жүйелер қауіпсіздігіне қатерлер. Ақпаратты қорғау	1			3	3
2. Криптологияның негізгі ұғымдары мен міндеттері	1			3	3
3. Криптографияның математикалық негіздері	2	4	2	10	10
4. Криптография. Моноалфавиттік, полиалфавиттік шифрлар. Ауыстыру және орнын өзгерту шифрлар.	1	1	2	6	6
5. Симметриялық криптографиялық жүйелер.	2	2	2	6	6
6. Симметриялық емес криптографиялық жүйелер.	2	2	3	8	8
7. Криптографиялық хаттама. RSA криптожүйе	2	2	2	3	3
8. Блоктық шифрлар. Ағылмалы шифрлар	1			10	10
9. Электрондық сандық қолтаңба (ЭСҚ). Хеш-функция.	1	2	2	3	3
10. Криптоанализ. Шифрге шабуыл, жиілік талдау. Шифрдың тұрақтығы. Мүлдем тұрақты	2	2	2	3	3

шифры.					
БАРЛЫҒЫ:	15	15	15	45	45

Практикалық (семинарлық) сабақтар тізімі

1. Криптографияның математикалық негіздері.
2. Моноалфавиттік, полиалфавиттік шифрлар. Ауыстыру және орнын өзгерту шифрлар.
3. Симметриялық криптографиялық жүйелер.
4. Симметриялы емес криптографиялық жүйелер.
5. RSA криптожүйе
6. Хеш-функция.
7. Шифрге шабуыл, жиілік талдау.

Зертханалық сабақтар тізімі

Зертханалық жұмыс № 1 Криптографияның негіздерін зерттеу

Зертханалық жұмыс № 2 Ауыстыру және орнын өзгерту әдіспен шифрлеуге арналған бағдарламаны әзірлеу.

Зертханалық жұмыс № 3 Симметриялық жүйе шифрлеу әдіспен шифрлеуге арналған бағдарламаны әзірлеу.

Зертханалық жұмыс № 4 Ассимметриялық жүйе шифрлеу әдіспен шифрлеуге арналған бағдарламаны әзірлеу.

Зертханалық жұмыс № 5 RSA алгоритм бойынша электрондық сандық қолтаңба қою бағдарламасын әзірлеу.

Зертханалық жұмыс № 6 Hash –функция жасау бағдарламасын әзірлеу.

Зертханалық жұмыс № 7 Криптоанализ эдістерін зерттеу.

Курстық жобалар (жұмыстар) тақырыбы

Бағдарламалық қамтамасыз етуді әзірлеу «Ашық кілтпен криптожүйелер».

Бағдарламалық қамтамасыз етуді әзірлеу «Симметриялық криптожүйлер».

Бағдарламалық қамтамасыз етуді әзірлеу «Сандық қолтаңба».

СӨЖ-ге арналған бақылау тапсырмаларының тақырыптары

1. Сақталған құпиясөздерді бұзудан қорғау қағидаларын қарастыру.
2. Желіде сақталған құпиясөздерді қорғау қағидаларын қарастыру.
3. Жылжу регистрлерінің бір-бір модельдер негізінде кездейсоқ сандар генераторды әзірлеу.
4. Әдістемесін қарастыру және үлкен сандар разрядтық тор машинасын модуль алу үшін модульдік арифметикой жұмыс істеу үшін бағдарламасын құру.
5. Жеделдету әдістердің бірі арқылы модульдік арифметиканың үлкен сандар көбейту моделін қарастыру
6. Жеделдету әдістердің бірі арқылы модульдік арифметиканың үлкен сандардың дәрежесін шығарумоделін қарастыру.
7. Үлкен сандарға желілік қабысулық генераторды жүзеге асыруды қарастыру (разрядтық тор машинадан артық)

8. 32 биттік машинаға арналған ГОСТ 28147-89 жекелеген блоктарды жүзеге асыруды қарастыру.

9. Бұрын әзірленген рәсімдер негізінде қарапайым ауыстыру режимінде шифрлау блок моделін құрау.

10. SHA стандартында Hash алуы моделін қарастыру.

Студенттер білімін бағалау критерийлері

Пән бойынша емтихан бағасы межелік бақылаулар бойынша максимум көрсеткіштер (60%-ға дейін) мен қортынды аттестаттаудың (емтихан) (40%-ға дейін) сомасы ретінде анықталады және кестеге сәйкес 100%-ға дейінгі мәнді құрайды.

Пән бойынша берілген тапсырмаларды орындау мен тапсыру кестесі

Бақылау түрі	Тапсырма мақсаты мен мазмұны	Ұсынылатын әдебиет	Орындау ұзақтығы	Бақылау түрі	Тапсыру мерзімі	Балл
1	2	3	4	5	6	7
Қатысу	Қатысудың бақылау		Семестр бойынша	ағымдағы	Апта сайын	1
СӨЖ бойынша есеп	«Компьютерлік жүйелер қауіпсіздігіне қатерлер. Ақпаратты қорғау» бойынша білімді тереңдету	[1], [2], [3] [5]	2 апта	ағымдағы	2 апта	1
№ 1 тәжірибелік жұмысты қорғау	Криптографияның негіздерін зерттеу	[1], [2], [3], [5], [12],[11]	1 апта	ағымдағы	2 апта	2
№ 2 тәжірибелік жұмысты қорғау	Ауыстыру және орнын өзгерту әдіспен шифрлеуге арналған бағдарламаны әзірлеу	[1], [2], [3], [5], [12],[11]	1 апта	ағымдағы	3 апта	2
СӨЖ бойынша есеп	«Криптологияның негізгі ұғымдары мен міндеттері» бойынша білімді тереңдету	[1], [2], [3] [5]	2 апта	ағымдағы	3 апта	1
№3 тәжірибелік жұмысты қорғау	Симметриялық жүйе шифрлеу әдіспен шифрлеуге арналған бағдарламаны әзірлеу	[1], [2], [3], [5], [12],[11]	1 апта	ағымдағы	4 апта	3
СӨЖ	«Криптографияның	[1], [2], [3], [5],	2 апта	ағымдағы	5 неделя	1

бойынша есеп	математикалық негіздері» бойынша білімді тереңдету	[6],[10]				
№4 тәжірибелік жұмысты қорғау	Ассимметриялық жүйе шифрлеу әдіспен шифрлеуге арналған бағдарламаны әзірлеу	[1], [2], [3], [5], [12],[11]	1 апта	ағымдағы	5 неделя	3
СӨЖ бойынша есеп	«Криптография. Моноалфавиттік, полиалфавиттік шифрлар. Ауыстыру және орнын өзгерту шифрлар.» бойынша білімді тереңдету	[1], [2], [3], [5], [6],[10]	2 апта	ағымдағы	6 неделя	1
№5 тәжірибелік жұмысты қорғау	RSA алгоритм бойынша электрондық сандық қолтаңба қою бағдарламасын әзірлеу	[1], [2], [3], [5], [12],[11]	1 апта	ағымдағы	6 апта	3
Тәжірибелік сабақ бойынша есеп	Тәжірибелік және теоритикалық икемдерді тексеру	Бүкіл негізгі және косымша әдебиет	1 апта	ағымдағы	6 апта	4
Жазбаша сұрастыру	Тәжірибелік және теоритикалық икемдерді тексеру	[1-19] дәрістердің конспектісі	1 қатынас сағаттары	аралық	7 апта	10
СӨЖ бойынша есеп	«Симметриялық криптографиялық жүйелер» бойынша білімді тереңдету	[1], [2], [3], [5], [6],[10]	2 апта	ағымдағы	7 апта	1
№6 тәжірибелік жұмысты қорғау	Hash–функция жасау бағдарламасын әзірлеу	[1], [2], [3], [5], [12],[11]	1 апта	ағымдағы	7 апта	2
СӨЖ бойынша есеп	«Симметриялық емес криптографиялық жүйелер» бойынша білімді тереңдету	[1], [2], [3], [10], [14],	2 апта	ағымдағы	9 апта	1
СӨЖ бойынша есеп	«Криптографиялық хаттама. RSA криптожүйе»	[1], [2], [3], [10],	2 апта	ағымдағы	10 апта	1

	бойынша білімді тереңдету					
СӨЖ бойынша есеп	«Блоктық шифрлар. Ағылмалы шифрлар» бойынша білімді тереңдету	[1], [2], [3], [5], [12],[11]	2 апта	ағымдағы	12 апта	1
СӨЖ бойынша есеп	«Электрондық сандық қолтаңба (ЭСҚ). Хеш-функция.» бойынша білімді тереңдету	[1], [2], [3], [5], [12],[11]	2 апта	ағымдағы	13 апта	1
СӨЖ бойынша есеп	«Криптоанализ. Шифрге шабуыл, жиілік талдау. Шифрдың тұрақтығы. Мүлдем тұрақты шифры.» бойынша білімді тереңдету	[1], [2], [3], [5], [12],[11]	2 апта	ағымдағы	14 апта	1
№7 тәжірибелік жұмысты қорғау	Криптоанализ әдістерін зерттеу	[1], [2], [3], [5], [12],[11]	1 апта	ағымдағы	14 апта	3
Тәжірибелік сабақ бойынша есеп	Тәжірибелік және теоритикалық икемдерді тексеру	Бүкіл негізгі және косымша әдебиет	1 апта	ағымдағы	14 апта	4
Жазбаша сұрастыру	Тәжірибелік және теоритикалық икемдерді тексеру	[1-19] дәрістердің конспектісі	1 қатынас сағаттары	аралық	14 апта	10
Курстық жоба	Пән материалының игерілуін тексеру	[1-19] Негізгі және қосымша әдебиет тізімі	3 қатынас сағаттары	Қорытынды	Сессия кезінде	40
Барлығы						100

Саясат және процедуралар

«Криптология» пәнін оқу кезінде келесі ережелерді ұстануды сұраймын:

1 Сабаққа кешікпеу.

2 Сабақтан дәлелді себепсіз қалмау, ауырған жағдайда анықтама, ал басқа жағдайларда түсіндірме хат ұсынуды.

3 Сабақтың барлық түрлеріне қатысу студент міндеттерінің қатарына жатады.

4 Оқу процесінің күнтізбелік кестесіне сәйкес барлық бақылау түрін тапсыру.

5 Қатыспаған практикалық және зертханалық сабақтарды оқытушы көрсеткен уақытта өтеу.

Негізгі әдебиет тізімі

1. Грибунин В.Г. Комплексная система защиты информации на предприятии: Учеб. Пособие. - М.: Академия, 2009. - 412 с.
2. Арутюнов В.В. Защита информации: Учебно-методическое пособие. - М.: Либерея-Бибинформ, 2010. - 56 с.
3. Варлатая С.К., Шаханова М.В. Программно-аппаратная защита информации: учеб. пособие. - Владивосток: Изд-во ДВГТУ, 2010. - 318 с.
4. Бузов Г. Практическое руководство по выявлению специальных технических средств несанкционированного получения информации. - М.: Горячая Линия - Телеком,-2010, - 240 с.
5. Шаньгин В. Защита компьютерной информации. Эффективные методы и средства. - М.: ДМК Пресс, 2010, - 544 с.
6. Шаньгин Ф. Комплексная защита информации в корпоративных системах. Учебное пособие. - М.: Форум, 2010, - 592 с.
7. Щербаков В., Ермаков С., Безопасность беспроводных сетей. Стандарт IEEE 802.11. - М.: РадиоСофт, 2010, - 256 с.
8. Хореев П.Б. Методы и средства защиты информации в компьютерных системах. - М.: Академия, 2007. 256 с.
9. Белов Е. Б. и др. Основы информационной безопасности: Учеб. пособие. М.: Горячая линия-Телеком, 2006. - 544 с.
10. Ярочкин В.И. Информационная безопасность: Учебник. - М.: Академический проект, Трикста, 2005. - 544 с.
11. Садердинов А.А. Информационная безопасность предприятия: Учеб. Пособие,- М.: Дашков и К, 2005. - 336 с.
12. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: Учеб. пособие. - М.: Горячая линия-Телеком, 2004. - 280с.
13. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. - М.: ТРИУМФ, 2003. - 400 с.
14. Зегжда Д. П., Ивашко А. М. Основы безопасности информационных систем. - М.: Горячая линия - Телеком, 2000. - 452 с.

Қосымша әдебиет тізімі

15. Проскурин В.Г. Защита программ и данных. - М.: Академия, 2011, - 208 с.
16. Касперский К. Фундаментальные основы хакерства (искусство дизассемблирования). - М.: Солон-Р, 2008. - 288 с.
17. Ященко В.В. Введение в криптографию. Новые математические дисциплины. - М.: МЦНМО Питер, 2001. - 287 с.
18. Хорев А. А. Способы и средства защиты информации. Учеб. пособие. -М.: МОРФ, 2000.-316 с.
19. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. - М.: Кудиц-образ, 2001.- 363 с

СТУДЕНТКЕ АРНАЛҒАН ПӘН БОЙЫНША ОҚЫТУ БАҒДАРЛАМАСЫ (SYLLABUS)

Krip 3213 «Криптология» пәні

МКЕ 19 «Математикалық қамтамасыз ету» модулі

31.03.2004 ж. № 50 мемл. бас. лиц..

Баспаға _____ 20__ж. қол қойылды. Пішіні 90х60/16. Таралымы _____ дана

Көлемі ___ оқу бас. п. № _____ тапсырыс Бағасы келісілген

_____

100027. ҚарМТУ баспасы, Қарағанды, Бейбітшілік бульвары, 56