Қазақстан Республикасының білім және ғылым министрлігі

С. Торайғыров атындағы Павлодар мемлекеттік университеті

Есептеу техникасы және бағдарламау кафедрасы

ЖҰМЫС ОҚУ БАҒДАРЛАМАСЫ

«Ақпараттық қауіпсіздік негіздері» пәні бойынша

Павлодар, 2013 ж.

Оқу жұмыс бағдарламасы бекіту парағы (SYLLABUS)

Форма ПМУ ҰС Н 7.18.4/19

БЕКІТЕМІН
ФМжАТ факультетінің деканы
_____ Испулов Н.А.
(қолы) (аты-жөні)
«___»_____20__ж.

Құрастырған: аға оқытушы _____Ахмерова З.Р.
(лауазымы, ғылыми атағы, қолы) (аты-жөні)

ЖҰМЫС ОҚУ БАҒДАРЛАМАСЫ (Syllabus)

Ақпараттық қауіпсіздік негіздері OIB 3302
(жұмыс оқу жоспары бойынша пәннің коды мен толық атауы)
күндізгі оқу формасындағы мамандық(тар) студенттері үшін
(оқу формасы)
Есептеу техникасы және бағдарламалық қамтамасыз ету 5B070400
(мамандық(тар)дың толық атауы мен шифрі)

Бағдарлама «___» _____20__ж. бекітілген жұмыс оқу бағдарламасы негізінде құрастырылған

Кафедраның отырысында қарастырылған «___»_____20__ж.
Хаттама №_____.
Кафедра меңгерушісі _____ Потапенко О.Г. «____» _____20__ж.
(қолы) (аты-жөні)

ФМжАТ факультетінің оқу әдістемелік кеңесінде құпталған
(факультет атауы)
«____»_____20__ж. Хаттама №____

ОӘК төрайымы _____ Искакова А.Б. «____» _____20__ж.
(қолы) (аты-жөні)

1. Оқу бағдарламасының паспорты

Пән атауы Ақпараттық қауіпсіздік негіздері

Кредиттер саны мен оқыту ұзақтығы
Жалпы – *3* кредит
Курс: 3
Семестр: 6

Жалпы аудиториялық сабақтар– 52,5 сағат
Дәрстер - 15 сағат
Тәжірибелік /семинар сабақтары – 22,5 сағат
Зертханалық – 15 сағат
СӨЖ – 82,5 сағат, сонымен бірге СӨЖМ – 20,625сағат
Жалпы бейнетті- 135 сағат

Бақылау формасы
Курстық жұмыс – 6 семестр (қорғау)
Қорытынды бақылау формасы
Емтихан – 6 семестр

Пререквизиттер
«Ақпараттық қауіпсіздік негіздері» пәнінің алдында «Ақпараттану», «Математика», «Физика» және «Алгоритмдік тілде бағдарламалау» сабақтары бойынша алынған білімдерге негізделеді.

Постреквизиттер
Студенттер «Ақпараттық қауіпсіздік негіздері» пәні бойынша алған білімі мен дағдыларын мамандандырылған пәндер мен дипломдық жобалауда қолданулары мүмкін.

2. Оқытушылар жайлы мәліметтер мен жеке ақпарат

Аты-жөні Ахмерова Зарема Равильевна

«ЕТжБ» кафедрасы, аудитория А-403
E-mail: Ahmerova_Zarema@mail.ru

3. Пәні, мақсаты және мәселесі

Пән атауы Ақпараттық қауіпсіздік негіздері

Пәнді оқыту мақсаты

Ақпараттық жүйелерде ақпарат қорғау жүйелерін құрудың теориялық негіздері мен іс жүзінде қолданылуын оқыту. Деректер қорғау принциптері, әдістері мен құралдары жөнінде жүйеленген білім беру. Ақпараттық жүйелерде жобалау мен жүргізуге қажетті ақпарат қорғаудың тәжірибелік дағдыларын игерту болып табылады. Ақпараттық жүйелердің нәтижелігін арттырудың негізгі бастамаларының бірі деп ақпараттық қауіпсіздігін анықтау және дәлелдеу. Ақпараттық жүйелер құрылысының жеке әдістерді және жалпы принциптерді зерттеу.

4. Білімі, икемділігі, дағдысына және құзыретіне талаптары

Пәнді игеруде тәлімгерлер білуге тиісті:

- ақпараттық жүйелер қорғаныс құрылысының жалпы принциптерін;
- теориялық негіздер, негізгі принциптер және жобалау кезіндегі қорғаныс әдістері, әр түрлі тағайындаулар қолдану арқылы осы заманға сай есептеуіне техниканың ақпараттар жүйесінде эксплуатациялау және дайындау.

Пәнді игеруде тәлімгерлер істей білуге тиісті:

- жобалау кезіндегі ақпараттық жүйелердің керекті құрылымын қолдану, әр түрлі бағыттағы жүйелердің эксплуатациясы және дайындау;

- іздеу тапсырмаларын шешу, ақпараттық жүйелердің енгізулерін қайталамау және тысқары шығару.

5 Пәннің тақырыптық жоспары

Академиялық сағаттарды сабақтардың түрі бойынша бөлу

Оқу формасы	Пән жұмыс сыйымдылығы				Семестрлер бойынша бақылау формасы				Семестр	Семестрлер бойынша студенттердің жұмыс көлемі					
	кредиттер	академиялық сағаттар								кредиттер	аудиторных занятий (ак. часов)				СӨЖ (ак. сағат)
		жалпы	ауд	СӨЖ	емт.	сын.	КЖ	КЖ			жалпы	дәр	тәж.	зерт	жалпы
ЖОБ 2011 негізінде күндізгі	3	135	52,5	82,5	6			6	6	3	52,5	15	22,5	15	82,5

6. Дәріс сабақтарының мазмұны

1 Тақырып. Кіріспе

Ұлттық қауіпсіздендірудің негізгі түсініктері; қауіпсіздендірудің түрлері: мемлекеттік, экономикалық, қоғамдық, әскери, ақпараттық, экологиялық; ақпаратық қауіпсіздендірудің жүелік қамтамамасының ҚР ұлттық қауіпсіздендірудің жүйесіндегі ролі мен орны.

2 Тақырып. Ақпараттық қорғау

Акпараттық кауіптер. Ақпараттық қауіптерге қарсы әрекет. Ақпаратты қорғау жүйелердің сипаттамалық қасиеттері. Қорғау пәні. Қорғау құралдары.

3 Тақырып. Ақпараттық қауіпсіздендіру

Ақпараттық қауіпсіздендіруді қамтамасыз ету жүйелердің сипаттамалық қасиеттері, ақпаратты қауіпсіздендіруді қамтамасыз ету құралдары, ақпаратты қауіпсіздендіруді қамтамасыз ету әдістері.

4 Тақырып. Ақпараттық жүйелердің аппаратық және программалық платформасын анализдеу

Мәліметтрді өндеу электрондық жүйелердің құрылысы; программалы қамтамасыздандырудың құрылысы; мәліметтерді ондеудің жүйелік құралдары; мәліметтерді өңдеудің қолданбалы құралдары; ақпараттық қорғаудың аппаратық құралдары; ақпараттық қорғаудың программалық құралдары.

5 Тақырып. Ақпараттық жүйелердің қауіпсіздік модельдері

Формальды модельдер; қауіпсіздіктің модельдері; қауіпсіздіктің саясаты; есептеу техникасының құралдары мен автоматтандырылған ақпараттық жүйелердің қорғалуының кретерияларі мен кластары; корғалған жүйелерді бағалау бойынша стандарттар.

6 Тақырып. Қорғау және қауіпсіздендіру жүйелерін практикалық іске асырудың мысалдары

Құпия сөз жүйелерінің құрылуы; криптографиялық әдістерді қолданудың ерекшеліктері; криптографиялық ішкі жүйелерді іске асырудың әдістері; симметриялық және бисимметриялық кілттері бар жүйелерді іске асырудың ерекшеліктері; стенографиялық жүйелерді іске асыру түрлері.

7 Тақырып. Корланған ақпараттық жүйенің негізгі сипаттамалары

Қорланған ядроның концепциясы; тексеру әдістері; қорланған домендер; иерархиялық әдісті қорланған операциялық жүйені құрғанда қолдану.

8 Тақырып. Ақпаратты қорғау дұрыстығының әдістемесі

Қорғау жүйелерінің дұрыстығын зерттеу, қорғауды зерттеу мен жобалаудың әдістемесі; бүтіндікті тексеру саясаттың моделі.

9 Тақырып. Ақпараттық қорғау өлшемі

Ақпараттық ресурстарды қорғаудың керекті өлшемін аңықтау. Ақпаратты қорғау өлшеміне баға беру әдістері. Ақпаратты қорғау деңгейіне баға берудің негізгі көрсеткіштері. Қорғау өлшемдерінің сипаттамалары.

10 Тақырып. Қорғау процесстерің тиімді басқаруы

Қорғаудың аппараттық құралдарын жобалауды. Қорғаудың программалық жүйелерін жобалауды. Қорғау өлшемдерін ұйымдастыруды жобалауды. Қауіпсіздендіруді қамтамасыз ету процесстерін тиімді басқарудың әдістері мен модельдері.

11 Тақырып. Қорғау жүйелерге баға беру

Ақпаратты қорғау жүйесіне кешенді баға беру. Программалық қамтамасызды тестілеу. Программалық түліктерді тестілеу қыйындақтары, автоматтанған тестілеу, өзі тестіленетін программаларды жазу принциптері.

Тестерді дайын программаларға инсталяциялау.

Қорғау механизмдердің сенімділігіне баға беру. Қорғау сенімділігіне баға беру принциптері.

12 Тақырып. Компьютерлік жүйелерінің қауіпсіздігі

Жергілікті тораптарда қорғау. Жеке ақпаратты қорғаудың программалық құралдары.

Рұқсатсыз қатынауды табу үшін сараптық жүйелерді қолдану.

7. Тәжірибелік (семинар, зертханалық, студиялық өздік) сабақтар мазмұны, олардың сағаттық көлемі

Тәжірибелік жұмыс 1

Тақырып 1. «Сәкі» шифрі.

Негізгі теориялық қосымшалар

«Сәкі» шифрі келесідей жұмыс істейді: ашық текст белгілі бір ұзындықтағы жолдарға («баспалдақ» ретінде) жазылып, содан соң горизонталды түрде оқылады. Мысалы, «шифр с использованием перестановки» хабарламасын 2 ұзындықты баспалдақтармен сәкі әдісімен шифрлеу үшін хабарламаны келесідей жазамыз

Ш Ф С С О Ь О А И М Е Е Т Н В И
И Р И П Л З В Н Е П Р С А О К

Шифрленген хабарламаның түрі келесідей болады.
ШФССОЬОАИМЕЕТНВИИРИПЛЗВНЕПРСАОК

Бақылау сұрақтары:

1. Бұл әдістегі кілт нені білдіреді?
2. Шифрлеу кезінде хабарлама қалай жазылады?
3. Шифрлеу кезінде кодталған хабарлама қалай оқылады?
4. Дешифрлеу кезінде кодталған хабарлама қалай жазылады?
5. Дешифрлеу кезінде қайта құрылған хабарлама оқылады.
6. Белгісіз кілтпен дешифрлеуді ұйымдастыруға бола ма?
7. Дешифрлеуден кейін бағдарламалық түрде хабарламаның дұрыс нұсқасын анықтауға бола ма?
8. Шифрлеу алгоритмі.
9. Дешифрлеу алгоритмі.
10. Әдістің анализі.

Тапсырмаларды орындау бойынша әдістемелік кеңестер:

Ашық текстке «Сәкі» шифрі қолданылған. 3 кестедегі шифрленген текст бойынша хабарламаны қалыптастырыңыз.

№	Тапсырма
1.	ВЩИТЗЬВЬЛОНЕНИУШИЗЕГАЕТСЮЕНОЙОСВЕПТПЫВЗШТРРОБОПАЕАО МНЛОЛОТМРЯЯЕЬЛОЛЕНА
2.	ЛЕСЕПЕУЕОНЬНЯПЗННМИЬУИЩЮДТКРТЮБПОХЕИООИФАЕНШЕИБЕВО ОИЩЕАСРНИЛВЯОЦСАЕЗТОЙИММРЕЗСТАИСЬАИРИТРНАЫ

3.	МЕЕЕСНЬМТПЦСНРЧЯТЫЗДОЕЕТОЫЕТИСООВЧЛИГЧСЕСИВКИЕОИЕКЛВ САУОНСЕЛОЬЯПНМБИТСОЙНЗОИЕЕЕНФВДОАЛЕНСМО
4.	ВРОСМЕННАЗАРТМНММММИМНИАКНФЦЯСОВУЕАДЕНАНСХТАОИЛЕЛО ЮЕЖОНФЦЫТЭРЯРЯАБЬДРБНКТОИХЕЛОИМВНЯОИАУЫУА
5.	САИАЕЬДЛЬЩКТСЕМИБСДОЧКЕЬХЕОЕИИАСЕНОБИОННРЙМРСНЦТЗОЛ ЕВНЦОАСПНТФИЕОСЖСАФИСНЯЬОЕОИМПТНПТИАТЯВЮЙМР
6.	ОЗСЗСЕСЕОИИИЩДАТОТТПНЙФИКЕНДЕПИСЕАИИСАНОАМАЯЯЧДДКТС ИЙЧЫСВОЕЕЕАООЯИСБНЛБНЖНЦЧОЗИЕОЯЕИНТИНБ
7.	СЕЕАСБЕАЕМООЧЯРТОКЕАОЕИМЗСТЕЧЕВОСТЕОАЕТТРЧОНСАОНИСИТО ЖТРНТВЛФАЕИБИТБПООПВНЗНЬЕИПИЯАПДСЩЯ
8.	ОИЯИОРИОМТБЕДННСТРЕВЕКОФНАЬОШАСОСОЫМОНАПНТРМИТНТЕТ УМРЗПЕЕЧРПАЕБОГЛЕОАЦСАСОЬНЛКИУВТВС
9.	ПВАНЩОАЕИНРИЫЯТЗТЫАНРИИСРРТГЕДХВСРЕМСЫУЯТЯАМОАДАИЛЯУ ЛИСЕШЗЫТКОРПАННЯРШЬИНЕАНХТНИЕЧНЕЮАИН
10.	КЕЬИАНЗПДООИАЕИООННЦААОАТЖЕЛССВНЦОФИЧЩТНВНГИКСАФИС ОИАИОНООТОЛНИАТРОЕТКЫЗСАИГЕИДЛЬМЗТУАХМТНЧОДЯ

Ұсынылатын әдебиет тізімі (2, 5, 6)

Тәжірибелік жұмыс 2

Тақырып 2. Вертикалды ауыстырым әдісі.

Негізгі теориялық қосымшалар

Вертикалды ауыстырым шифры.

«Сәкі» шифрі криптоанализ үшін қиын емес. Қиынырақ сызба хабарлама текстін бірдей ұзындықты горизонтальды жолдарға жазу және бағандарды қандай да бір реті бойынша оқу болып табылады. мұнда бағандарды оқу тәртібі алгоритмнің кілті болады. Төменде «ПЕРЕСТАНОВКА ТЕКСТА ПО СТОЛБЦАМ» фразасын 4312567 кілтпен шифрлеу көрсетілген.

Кілт:	4	3	1	2	5	6	7
Ашық текст:	П	Е	Р	Е	С	Т	А
	Н	О	В	К	А	Т	Е
	К	С	Т	А	П	О	С
	Т	О	Л	Б	Ц	А	М

Шифрленген текст: РВТЛЕКАБЕОСОПНКТСАПЦТТОААЕСМ

Қарапайым ауыстырым шифрін тану өте оңай, өйткені ондағы әріптер ашық текстегідей жиілікпен кездеседі. Мысалы, жоғарыда қарастырылған бағандарды ауыстыру арқылы шифрлеу үшін шифр анализы өте оңай – шифрленген текстіні матрица ретінде жазып, бағандар үшін барлық мүмкін ауыстырмдарды таңдау

Ауыстырым шифрін ауыстырымды бірнеше рет қолдану арқылы қорғалған қылуға болады. Бұл жағдайда, шифрлеу үшін қолданылған ауыстырымды қайта құру мүмкін емес. Мысалы, егер алдыңғы хабарламаны сол алгоритм көмегімен шифрлесе, онда нәтиже келесідей болады:

Кілт:	4	3	1	2	5	6	7
Ашық текст:	Р	В	Т	Л	Е	К	А
	Б	Е	О	С	О	П	Н
	К	Т	С	А	П	Ц	Т
	Т	О	А	А	Е	С	М

Шифрленген текст: ТОСАЛСААВЕТОРБКТЕОПЕКПЦСАНТМ

Бақылау сұрақтары:

1. Бұл әдістегі кілт нені білдіреді?
2. Шифрлеу кезінде хабарлама қалай жазылады?
3. Шифрлеу кезінде кодталған хабарлама қалай оқылады?
4. Дешифрлеу кезінде кодталған хабарлама қалай жазылады?
5. Дешифрлеу кезінде қайта құрылған хабарлама оқылады.
6. Белгісіз кілтпен дешифрлеуді ұйымдастыруға бола ма?

7. Дешифрлеуден кейін бағдарламалық түрде хабарламаның дұрыс нұсқасын анықтауға бола ма?
8. Шифрлеу алгоритмі.
9. Дешифрлеу алгоритмі.
10. Әдістің анализі.

Тапсырмаларды орындау бойынша әдістемелік кеңестер:

Вертикалды ауыстырым әдісімен шифрленетін ұсталған хабарламалар анализі кезінде криптоаналитикктер қолданылатын кілтті жартылай қалыптастырды. Сонымен қатар, олар кілттегі символдар саны мен кейбір позициялардың сандық мәндерін анықтады. Криптоаналитиктердің жұмыс нәтижесі мәндері ағымдағы уақытта белгісіз кілттің позициялары X символымен белгіленіп, ұзындығы кілт ұзындығымен сәйкес келеттін жол ретінде көрсетілген (4 кестеден тапсырманы қараңыз). Сізден бар шифртекст бойынша қалыптастырылған кілтті аяқтап, шифрленген хабарлама сәйкес ашық текст алу қажет.

№	Тапсырма
1.	Шифрленген текст: ФТБЕОЗРЬЩМАОСЕОИАОИНШВОНЖ Жартылай қалыптастырылған кілт: XX5X1
2.	Шифрленген текст: ПНОСОЕЕНМРЗОЮЯАЬЬАПТКТБС Жартылай қалыптастырылған кілт: 6XX1X4
3.	Шифрленген текст: ОННАНЦОНДЛЬХФИСНИАТЫКЕЬД Жартылай қалыптастырылған кілт: XX24X3
4.	Шифрленген текст: СИВОСЕНЕЗОПЕОПТОЧЕБСЕСЙАИБЕТЕН Жартылай қалыптастырылған кілт: 4XX13X
5.	Шифрленген текст: СНСКЫЕЕОАНОЕЕУАБЧДПНПИТДМ Жартылай қалыптастырылған кілт: 3XXX5
6.	Шифрленген текст: АКДВСЕШНЛСООСИЫАЧЕФЯКЕТРИМИИ Жартылай қалыптастырылған кілт: 63XX27X
7.	Шифрленген текст: ИАОТЮОЕРКМФНТЫЧРИКМОШВСЫЛ Жартылай қалыптастырылған кілт: XX3X2
8.	Шифрленген текст: ЛЩЕОЬИЙМААТЛНТОАОЯСВКЗЕЗЛААТ Жартылай қалыптастырылған кілт: 7XX3X24
9.	Шифрленген текст: СУХЫЫМИЗЕМТРОТНАНЦПЙАЗИАЛЕИЩФИЬМЗИОИ Жартылай қалыптастырылған кілт: 2XX3X6
10.	Шифрленген текст: БСЕАГНМЗЛАЕООЯНПЛТБНАЕЕСЬЬЕА Жартылай қалыптастырылған кілт: 2X41XX7

Ұсынылатын әдебиет тізімі (2, 5, 6)

Тәжірибелік жұмыс 3

Тақырып 3. Виженер шифрі.

Негізгі теориялық қосымшалар

Полиалфавиттты шифрлер. Виженер шифрі.

Қарапайып көпалфавитті шрифтіні жетілдіру мүмкіндігі ашық текстіні шифрлеу кезінде бірнеше көпәріпті алмастыруды қодануда. Шифрлеудің мұндай әдістерін қолдануға негізделген шрифтілер жанұясы полиалфавитті шифрлер деп аталады. Мұндай шифрлеу әдістерінің келесідей

қасиеттері бар.

1. Моноалфавитті ауыстырым жиыны қолданылады.
2. Берілген кезеңде қандай ауыстырым қолданылу керек екенін анықтайтын қандай да бір кілт болады.

Ең кең тараған және бір уақытта ең қарапайым алгорит Виженера (Vigenure) шифрі болып табылады. Бұл шүифр Цезардің 26 шифрімен 0-ден 25-ке дейінгі (латын алфавиті үшін) жылжытумен моноалфавитті ауыстыру жиынына негізделген. Әрбір мұндай шифрді ашық текстінің А әрпіне сәйкес келетін шифрленген текстінің әрпі болатын кілттік әріппен белгілеуге болады. Мысалы. жылжытуы 3-ке тең болатын Цезарь шифрі D кілттік әрпімен белгіленеді.

Бұл сызбаны түсіну мен қолдануды жеңілдету үшін «Виженер таблосы» (1 кестесін қараңыз) деп аталған матрица ұсынылған. Барлық 26 шифр горизонталды орналасқан және әр шифрге шеткі бағанда сол жағынан көрсетілген кілттік әріп сәйкес келеді. Ашық текст әріптеріне сәйкес алфавит кестенің үстінгі жағындағы бірінші жолда орналасқан. Шифрлеу үрдісі қарапайым – **x** кілттік әрпі мен **y** ашық текст әрпі бойынша **x** жолы мен **y** бағанының қиылысуында орналасқан шифрленген тестінің әрпін табу қажет. Берілген жағдайда мұндай әріп ретінде V әрпі болады.

1 кесте. Виженер таблосы.

	a	**b**	**c**	**d**	**e**	**f**	**g**	**H**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**R**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**
a	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R

t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Хабарламаны шифрлеу үшін хабарламаның ұзындығындай кілт қажет. Әдетте кілт сәйкес ұзындықты жолды алу үшін кілттік сөздердің санын көрсетеді. Мысалы deceptive кілттік сөз болса, «we are discovered save yourself» хабарламасы келесідей шифрленеді:

Ашық текст: D E C E P T I V E D E C E P T I V E D E C E P T I V E

Кілт: W E A R E D I S C O V E R E D S A V E Y O U R S E L F

Шифрленген текст: Z I C V T W Q N G R Z G V T W A V Z H C Q Y G L M G J

Текстіні дешифрлеу өте оңай – кілт әрпі жолды анықтайды, бұл жолда орналасқан шифрленген текст әрпі бағанды анықтайды, және бұл бағанда кестенің бірінші жолында ашық текстінің сәйкес әрпі болады.

Бұл шифрдің артықшылығы – ашық текстінің бір әрпін шифрленген текстіде көрсету үшін бірнеше нұсқалар бар – кілттік сөздің қайталанбайтын әр әрпі үшін біреуден. Осылайша, әріптердің қолданылу жиілігін көрсететін ақпарат жасырылады. Бірақ бұл әдіс көмегімен де ашық текст құрылымынң шифрленген текст құрылымына әсерін керсетпеу толықтай мүмкін емес. Шифрлеу сенімділігін арттыру үшін хабарлама ұзындығымен сәйкес келетін кілт қолданылады, ал текстік сипаттамалары ашық текстінің стандартты сипаттамадарынан ауытқыған.

Бақылау сұрақтары:

1. Виженер таблосы деген не?
2. Виженер таблосын қалай ұйымдастыруға болады?
3. Шифрлеу алгоритмі.
4. Дешифрлеу алгоритмі.
5. Белгісіз кілтпен дешифрлеуді ұйымдастыруға бола ма?
6. Дешифрлеуден кейін бағдарламалық түрде хабарламаның дұрыс нұсқасын анықтауға бола ма?
7. Кілт үшін шектеулер.
8. Әдістің анализі.

Тапсырмаларды орындау бойынша әдістемелік кеңестер:
Виженер әдісі бойынша шифрлеу мен дешифрлеу үшін бағдарлама құру.

Ұсынылатын әдебиет тізімі (2, 5, 6)

Тәжірибелік жұмыс 4

Тақырып 4. Бұрылма тор әдісі.

Негізгі теориялық қосымшалар

«Бұрылма тор» шифрі.

Бұрылма тор деп аталатын шифрді қолдану үшін таза қағаз үстіне қойғанда кесімдері қағаздың барлық ауданын жабатындай тіктөртбұрышты $2m \times 2n$ торлар өлшемді қағаздан

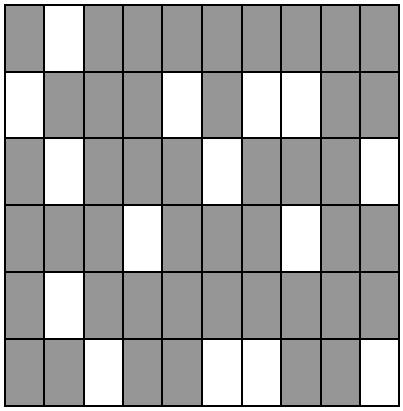
трафарет жасалады.

Хабарлама әріптері алдын ала белгіленген тәртіпте трафарет кесімдеріне жазылады(әр жолда солдан оңға қарай жол бойынша).

Шифрлеу үрдісін мысалмен қарастырайық. Кілт ретінде 3, а суретте көрсетілген 6 × 10 торы қолданылсын. Оның көмегімен мына текстіні шифрлейік

ШИФРРЕШЕТКАЯВЛЯЕТСЯЧАСТНЫМСЛУЧАЕМШИФРАМАРШРУТНОЙПЕРЕСТАНОВКИ.

а)



б)

	Ш								
И				Ф		Р	Р		
	Е				Ш				Е
			Т				К		
	А								
		Я			В	Л			Я

в)

Е	Ш		Т	С			Я		
И				Ф		Р	Р	Ч	
	Е	А			Ш	С			Е
			Т	Н			К	Ы	
	А	М	С		Л				У
		Я			В	Л		Ч	Я

г)

Е	Ш	А	Т	С	Е	М	Я		Ш
И	И			Ф		Р	Р	Ч	
	Е	А	Ф		Ш	С	Р		Е
Т	А		Т	Н	М		К	Ы	А
Р	А	М	С	Ш	Л	Р	У		У
	Т	Я			В	Л		Ч	Я

д)

Е	Ш	А	Т	С	Е	М	Я	Н	Ш
И	И	О	Й	Ф	П	Р	Р	Ч	Е
Р	Е	А	Ф	Е	Ш	С	Р	С	Е
Т	А	Т	Т	Н	М	А	К	Ы	А
Р	А	М	С	Ш	Л	Р	У	Н	У
О	Т	Я	В	К	В	Л	И	Ч	Я

Торды қағаз бетіне қойылып хабарламаның алғашқы 15 (кесілімдер саны бойынша)

әріптері жазылады. Торды алғаннан кейінгі нәтиже 3, б суретте көрсетілген. Торды 180 градусқа бұрып және келесі 15 әріпті жазып, 3, в суретте көрсетілген қағаз аламыз. Енді қағазды бұрып және дәл солай орындап, текстің қалғаны шифрленеді. (3, г және д суреті).

Хабарламаны алушы, осындай торы болса, торды шифртекстке 4 әдіспен қойып текстіні оқи алады.

Трафареттер саны, яғни «тор» шифрінің кілттер саны $T = 4^{mk}$. Бұл шифр $n = 4mk$ ұзындығы бар хабарламаға арналған. 8×8 өлшемді трафарет үшін мүмкін торлар саны 4 миллиардтан асып түседі.

Бақылау сұрақтары:

1. Шифрлеу алгоритмі.
2. Дешифрлеу алгоритмі.
3. Тор бұрылуы қалай жүзеге асады?
4. берілген әдісте не кілт болып табылады?
5. Тор өлшемділі, терезелер саны мен хабарлама ұзындығы арасында қандай қатынас бар?
6. Тор өлшемін өзгертуді бағдарлама рұқсат ете ме?
7. Әдістің анализ.

Тапсырмаларды орындау бойынша әдістемелік кеңестер:
Бұрылма тор әдісі арқылы шифрлеу мен дешифрлеу үшін бағдарлама құру.

Ұсынылатын әдебиет тізімі (2, 5, 6)

Зертханалық жұмыс 1

Тақырып 1. Цезарь шифрі.

Негізгі теориялық қосымшалар

Шифрлеудің классикалық техникасы. Ауыстырымдарды қолдану.

Ауыстырым кезінде ашық текстің жеке әріптері басқа әріптермен немесе сандармен, немесе басқа да символдармен ауыстырылады. Егер ашық текст биттер тізбегі ретінде қарастырылса, онда берілген ашық текст биттер тізбегі шифрленген текст биттер тексті тізбегімен ауыстырылады.

Цезарь шифрі.

Ең белгілі ауыстырым шифрлерінің бірі ең ежелгі және ең қарапайым Юлий Цезарьмен қоолданылған шифр болып табылады. Цезарь шифрінде алфавиттің әр әрпі осы алфавитте үш позицияға алыс тұрған іріппен ауыстырылады. Алфавит «циклді» болып есептеледі, яғни Я әрпінен соң А әрпі болады. Мысалы, мына алфавита үшін:

А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я

шифрлеу келесідей болады:

Ашық текст:	К Р И П Т О Г Р А Ф И Я
Шифрленген текст:	Н У Л Т Х С Ж У Г Ч Л В

Ауыстырымды төменде көрсетілгендей барлық нұсқаларды тексеріп көру арқылы анықтауға болады:

Ашық текст:	А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я
Шифрленген текст:	Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я А Б В

Егер әр әріпке (А = 1, Б = 2 және т.с.с.) сандық эквивалентін белгілесе, онда шифрлеу алгоритмін келесі формулалармен көрсетуге болады. Ашық текстің әр әрпі Р шифрленген текст әрпімен С ауыстырылады:

$C = E(P) = (P+3) \bmod (26)$.

Жалпы жағдайда жылжыту әр түрлі болуы мүмкін, сондықтан Цезарь алгоритмі келесі формуламен жазылады:

$C = E(P) = (P+k) \bmod (26)$,

мұндағы k 1-ден 31-ге дейінгі диапазондағы (қарастырылған алфавит үшін) мәндерді қабылдайды. Дешифрлеу алгоритмі де қарапайым:

P = D(C) = (C-k) mod (26).

Егер анықталған текст Цезарь шифр көмегімен шифрленгені белгілі болса, қарапайым барлық нұсқаларды таңдау арқылы шифрды ашуға болады – ол үшін кілттің 31 нұсқасын тексеру қажет. Тізбектелген барлық мүмкін нұсқаларды таңдау әдісін қолдану келесі үш негізгі сипаттамалармен ақталды:

1. Шифрлеу және дешифрлеу алгоритмдері белгілі.
2. Барлығы 31 нұсқа қарау қажет.
3. Ашық текст тілі белгілі және оңай таңылады.

Компьютерлік ақпаратты қорғау туралы сөз болғанда, алгоритм белгілі деп алынады. Тізбектей таңдау әдісі негізінде криптоанализ жасайтыны - өте көп кілттер таңдау қажет алгоритмді қолдану.

Моноалфавитті шифрлер.

Барлығы 31 нұсқасы бар кілттерді таңдауда Цезарь шифрі берік қорғалған емес. Существенного Кілттер кеңістігін үлкейтуді қандай да бір таңдауларды қолдану арқылы болады.

Мысалы, Цезарь шифрінде алфавиттің кез келген 31 әрпінің таңдауға мүмкіндік берсек, *k* символдарды жылжыту арқылы ғана емес, онда біз 31! мүмкін кілттерін аламыз. Ондай кілттің қолданылу мысалы төменде көрсетілген.

Ашық текст:	А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я
Шифрленген текст:	Й Р Ж Ь Ш Л Я Е В Ъ Ф К М Б С Ч Ю А Ц И Э Щ Ы Н У П Г Х Т Д О З

Осы кілтті қолданумен шифрлеу мысалы:

Ашық текст:	К	Р	И	П	Т	О	Г	Р	А	Ф	И	Я
Шифрленген текст:	Ф	Ю	В	Ч	Ц	С	Ь	Ю	Й	Э	В	З

Создается впечатление, что 31!-ды (8×10^{33} асып түсетін) таңдап алу қиын сияқты болады, ал берілген шифрдің сенімділік деңгейі өте жоғары. Бірақ криптоаналитик үшін басқа да жаулау жолы бар. Егер криптоаналитик ашық текст табиғаты туралы көрсетілімдері болса, (мысалы,бұл текст ағылшын тілінде екені туралы), сәйкес тілдегі текстке тән маңызды қасиеттері туралы ақпаратты қолдануға болады.

2 суретте ағылшын текстінде әріптерді қолданудың салыстырмалы жиілігі берілген. Ашық текстің бір әрпі кілттің бір әрпіне сәйкес болатындықтан, онда дешифрлеудің алғашқы кезеңінде криптоаналитик шифрленген тексте әріптердің қолданылу жиілігінің анализін жүргізуі мүмкін және шифртекст пен алфавит символдары арасында сәйкестікті анықтауы мүмкін (мысалы, 2 сурет диаграммасына сәйкес, шифртекстің қолданылыатын символы Е әрпіне сәйкес келеді). Әрі қарай ағылшын тілінде ең көп тараған триграмма (3 әріптен жасалған комбинация) the анықтауға болады, бұл ашық текстіні бөлшектеп қайта құруға және кілттің мүмкін мәнін нақтылауға болады. Анализді жалғастыра отыра текстің толық мазмұнын алуға болады.

Моноалфавитты шифрлер тез ашылады, өйткені нақты алфавиттен әріптер қолданылу жиілігін сақтайды. Берілген жағдайда контршама бір әріпке бір емес, бірнеше әріп (омофон деп аталады) қолданылу болып табылады. Егер әріпке белгіленген ауыстыру символдар санын бұл әріптің пайда болу жиілігіне пропорционалды алса, онда шифрленген текстте әріптердің қолданылу жиілігін есептеу мәнсіз болады. Ашық тексттің әр элементіне омофон қолданылуда шифрленген тексттің бір ғана элементі сәйкес келеді, сондықтан ақырғысында бірнеше әріптер комбинациясының қайталану жиілігінің сипаттық көрсеткіштері көрсетілу қажет, нәтижесінде криптоанализ тапсырмасы элементарлы болып қалады.

Ауыстырым әдісімен шифрленген тексте текстің құрылымы айқын көрінбегені үшін 2 әр түрлі әдіс қолдануға болады. оның біреуі ашық текстің жеке әріптерін ауыстыруда емес, бірнеше әріптер комбинациясын ауыстыруға негізделген, ал басқа әдіс шифрлеу үшін бірнеше алфавитті қолдануға негізделген.

Бақылау сұрақтары:

1. Бұл әдістегі кілт нені білдіреді?
2. Шифрлеу кезінде хабарлама қалай жазылады?
3. Шифрлеу кезінде кодталған хабарлама қалай оқылады?
4. Дешифрлеу кезінде кодталған хабарлама қалай жазылады?
5. Дешифрлеу кезінде қайта құрылған хабарлама оқылады.
6. Белгісіз кілтпен дешифрлеуді ұйымдастыруға бола ма?

7. Дешифрлеуден кейін бағдарламалық түрде хабарламаның дұрыс нұсқасын анықтауға бола ма?

8. Шифрлеу алгоритмі.

9. Дешифрлеу алгоритмі.

10. Әдістің анализі.

Тапсырмаларды орындау бойынша әдістемелік кеңестер:

Цезарь шифрімен шифрленген текст бар. Жылжыту өлшемі белгісіз. Хабарламаны шифрлеңіз.

№	Тапсырма
1.	ИЦРХЭЫЩШШЩРЫЩЩМДРШУРМЮПРЭЪЩЬЭРЪРШШЩТЛЧ РШКЭЗЩМЖВШЩРМЮЧЛСШЩРЫЩЩМДРШУР
2.	ФГМКРОНФЩЗТЪЦФЫКШНФНХРТЦЛМИЩЪШИХГЙЫМЫЪЧНШНЩН ЯНХГЩНЪЗФРЧНШНМИЯРМИХХГЭ
3.	ВЦЫБЦГЮМЦСФЦЮГВГУСЩЭЦПГХЯВГДАЫЖЯБЯЙЦЪЫБЩАГЯФБСЕ ЩИЦВЫЯЪГЦЖЮЯЬЯФЩЩ
4.	КЭЧУЙЧБЗЪАДЮНЮКБИЭКЗШФДЙНОЮБМЬЙББЙБДИБЗДАКНОПЛЬЖЖ МДЛОКЯМЬРДУБНЖДИОБСЙКЗКЯДЫИЮКБЙЙКЯКПМКЮЙЫ
5.	ТБВРЭФРАВЭЛЕЪАШЯВЮУАРДШЗХБЪШЕБШБВХЬРЕШБЯЮЫМЧГХВБП ЮФШЭШВЮВЦХЪЫОЗШФЫПИШДАЮТРЭШПШФЫПАРБИШДАЮТЪШ
6.	ШАЖЮЕИДЩЖЦКЮНЫЗАДЯЗЮЗИЫВЫЗДИАЖСИСВАБФНДВАЦЬЪСЯЮ ВЫЫИЪШЦЗШХЭЦГГСЛШЭЦЮВГДАБФНЦ
7.	ШОФТЙЧШЩМЕТУЖЦВЮБУАШЬТ,ЯТУЩОЫЫЙЧЯЭЬЪЬЗКМТЮБСЬСЬ ШЩМЕО
8.	ПМЯПРАГЛЛЩЗПГИОГРЛЩЗИЙЬХМРНОЮАЖРГЙЭКМДГРЯЩРЪЖПНМЙ ЪЕМАЮЛВЙЭЦЖТОМАИЖПММЯЧГЛЖЭ
9.	ЙЧСЦЮЬЪЩЦМЛЫЪРЫФЭИЭЪЪНЕСЩФЛРЪЦМУЗОМСЮГЮЪЪЮЫЬМО ФЮСЧСШНЗЧРСХЭЮОФЮСЧИЩЪЭЪУРМЮСЧИЭЪЪНЕСЩФЛ
10.	ЖКВИУКУЭВГЦПАНИШЕЧКЙЧЪЪАЬЭЙЭИКАМАВШКЖЪВГЦПЭБВЖКЖ ИУЭЪВГЦПШЦКЪЙЭЩЧАЬЭЕКАМАВШКЖИЗЖГФЯЖЪШКЭГЧ

Ұсынылатын әдебиет тізімі (2, 5, 6)

Зертханалық жұмыс 2

Тақырып 2. Плейфейер шифрі.

Негізгі теориялық қосымшалар

Плейфейер шифрі.

Көпәріпті шифрлеу әдісіне негізделген ең таңымал шифрлерінің бірі – Плейфейер (Playfair) шифрі. Мұнда ашық текст биграммалары шифрленген текстің берілген биграммаларына ауыстырылатын өздік бірліктер ретінде қаралады.

Плейфейер алгоритмі қандай да бір кілттік сөз негізіінде жасалған 5*5 өлшемді әріптер матрицасын қолдануға негізделген. Матрица кілттік сөзде қолданылған әріптерді оңнан солға және үстінен астына жылжыту арқылы жасалады. Содаң сон алфавиттің қалған әріптері табиғи тәртіппен матрицаның қалған жолдары мен бағандарына орналастырылады. Төменде *monarchy* (монархия) кілттік сөзі үшін матрица мысалы көрсетілген

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

Ашық текст келесі ережелерге сәйкес 2 әріп бойынша шифрленеді.

1. Егер ашық тексттің қайталанатын әріптері шифрлеу үшін бір жұпты құрса, онда бұл әріптер арасына арнайы қоюшы-әріп орналастырылады, мысалы X. *Balloon* сөзі ba lx lo on түріне келтіріледі.

2. Егер ашық текстінің әріптері матрицаның бір жолына түсе берсе, онда олардың әрбіреуі матрицаның ақырғы жолынның элементін ауыстыру үшін сол жолдың бірінші элементі қолданылады деген шартпен сол жолдағы оң жағындағы әріппен ауыстырылады. Жоғарыда

құрылған матрицаға сәйкес AR - RM ретінде шифрленеді.

3. Егер ашық текстінің әріптері матрицаның бір бағанына түсе берсе, онда олардың әрбіреуі матрицаның ең төменгі элементін ауыстыру үшін сол жолдың ең үстінгі элементі алыады деген шартпен астында тұрған әріппен ауыстырлады. Жоғарыдағы мысалда MU – CM ретінде шифрленеді.

4. Егер көрсетілген шарттардың біреуі де орындалмаса, онда ашық текст жұбының әр әрпі ашық текстің екінші әрпі орналасқан жол мен бағанның қиылысындағы әріппен ауыстырылады. Мысалы, HS - BP ретінде, ал EA – IM ретінде (немесе JM, шифрлеушінің қалауы бойынша) шифрленеді.

Плейфейер шифрі қарапаым көпалфавитті шифрлерден гөрі сенімдірек. Бір жағынан әріптер тек 26, ал биграммалар – 26×26 = 676, сондықтан жеке әріптерді идентификациялаумен салыстырғанда биграммаларды идентификациялау қиынырақ. Басқа жағынан, жеке әріптердің пайда болудың салыстырмалы жиілігі биграммалардың пайда болу жиілігімен салыстырғанда кең диапазонда өзгеріп отырады, сондықтан биграммаларды қолдану жиілігінің анализі әріптерді қолдану жиілігінің анализінен гөрі қиынырақ болады. Осы себептерден Плейфейер шифрі бұзу мүмкін емес. Ол бірінші дүниежүзілік соғыс кезінде Британдық армияның шифрлеу стандарты қызметін атқарды және екінші дүниежүзілік соғыс кезінде АҚШ әскері мен кеңестік әскерлерде қолданылды.

Өткендегі үлкен репутациясына қарамастан Плейфейер шифрін ашу салыстырмалы оңай, өйткені оның көмегімен шифрленген текст ашық текстінің статикалық сипаттамаларын сақтап қалады. Бұл шифрді бұзу үшін бірнеше жүз әріптен тұратын шифрленген текстінің болуы жеткілікті.

Бақылау сұрақтары:

1. Бұл әдісте кілтке қандай шектеулер бар?
2. Матрица қалай жасалады?
3. Ашық текст қалай шифрленеді?
4. Дешифрлеу кезінде хабарлама қалай қайта құрылады?
5. Шифрлеу алгоритмі.
6. Дешифрлеу алгоритмі.
7. Әдістің анализі.

Тапсырмаларды орындау бойынша әдістемелік кеңестер:

Орыс тілді алфавит негізінде Плейфейер әдісін қолданғанда Ё (Е әрпімен ауыстырылады) және Й әрпі (И әрпімен ауыстырылады) алынып тасталады. Ъ және Ь әріптері бір әріп болып саналады. Әріптер матрицасы мына алфавитте құрылады:

АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ,

31 әріптен, 5 жолдан және 6 бағаннан тұрады. Мысалы, ПАРУСНИК кілттік сөз негізінде әріптер матрицасы келесідей болады:

П	А	Р	У	С	Н
И	К	Б	В	Г	Д
Е	Ж	З	Л	М	О
Т	Ф	Х	Ц	Ч	Ш
Щ	Ъ/Ь	Ы	Э	Ю	Я

5 кестеден өз нұсқанынызға сәйкес кілттік сөз бен симыодар тізбегін алыңыз. Плейфейер шифрін және кілттік сөзді пайдалана отырып, «КОД ПЛЕЙФЕЙЕРА ОСНОВАН НА ИСПОЛЬЗОВАНИИ МАТРИЦЫ БУКВ» сөйлемін кодтаңыз және сиволдар тізбегін декодтаңыз.

№	Тапсырма
1.	Кілттік сөз: ПОЛЕТ Декодтайтын жол: КЛКЕПЕШОБКЕРЭЛЧСКУЛЮЕТВМВКИММЮЗОТЖША
2.	Кілттік сөз: ФИЛЬМ Декодтайтын жол: НПВЪЗПЖИКЛБЦРПЪПЭИЯЩЛИЗПБКФАГПШУХЭЧЖРЫВЦТУНЧТЩЧНХНЩТНЯХКДНЦВЗТЧИ
3.	Кілттік сөз: КАТЕР

	Декодтайтын жол: ЗЛНЖКГСЩЯЪАОЕСМЩЯСОЛКДБОУЩФРКЖФТАРТЮВИОАСЫЫРМРЕПМЩ
4.	Кілттік сөз: ПАРОЛЬ Декодтайтын жол: ЮОГНФПЛМКЮМВРМХИНЦШБЛГЖМУПЕАЮЖЧЗПДАМАЛНЪЖЕАДПУНЕЛСЪМЧП МЪЗЧЪЭАЩЩНТЗЗУАД
5.	Кілттік сөз: КОЛЬЦА Декодтайтын жол: МИПГПДПМЖВТЩВИЕИЛРЩЧЗОЛИНЦЩХЖПЪРВЦТУОЖАЫВХУКЖЕВИ
6.	Кілттік сөз: КАМЕНЬ Декодтайтын жол: РСРФЪПЧСВЛНПНЪСШТОБСХЪИЪФОПГИМФАНЪУКГЩЛНВНКХЧЪДУНЛМАХКСЛИ ЧТБЕУ
7.	Кілттік сөз: СОЛНЦЕ Декодтайтын жол: ЗОИЦОЫИТЗУСОШЖАЦФАВЗЗКЗЧНБЗЖУКПБЕЫТЗЪЗФЩ
8.	Кілттік сөз: ТОВАРИЩ Декодтайтын жол: МОЩЕЯВЧЪЛТАПЯВМОМРЗФИЫПТБКВИХБЦБЩШЪЧШЩИВТЧОАДХОПАБТИВАРМ ЖИ
9.	Кілттік сөз: СВЯЗЬ Декодтайтын жол: ЛМЧШЮГХТЯПХООПКПЖМКЧВЦАОБФЖГКХПНЯВЖФЪЛЯНХОФЗТЪСЦПИЛФЛЪ
10.	Кілттік сөз: МАТЕРИЯ Декодтайтын жол: УЕНАЕЭМЧЗПФТКСЪИАРУЕПЕСЯЕХТИСЩГХМЖФЗЧБГЩКМЮАЕЪ

Ұсынылатын әдебиет тізімі (2, 5, 6)

8. Өздік жұмысы тапсырмалары

Тақырып 1. Ақпараттық жүйелерден құралатын талдау.
Тақырып 2. Криптоқорғаудың және криптоталдаудың модельденуі.

9. Курстық жұмыстардың (жобалардың) және т.б. ұсынылатын тақырыптары

Кіру мәліметтері 4-ші әдістердің бірі көмегімен шифрлау. Шифрын анықтауды ескеру. Егер әдіс соңғы болып табылмаса, нышандық және қажетті қолданудың мақсаты бар кодтық тізбектерінің берілуі үшін тізбекті алынсын бұл басқа әдістің кіру мәліметтері.

Шифрлауды тізбек барлық 4-ші әдістердің қолдануымен өткізу.

Әдістердің қолдануын тізбек еркін қабылданады. Орындаудың жанында әрбір тапсырма жауаптың алуын әдіс толық сипаттауға керек.

Қолданылатын курстық жұмыстарда шифрлауының әдістері:

1. Цезарь шифры;
2. Баспалдақ шифр;
3. Тік орын ауыстыруды шифр;
4. Виженер шифры.

10. Кеңес алу графигі СРОП (СРО –дан СРОП 25% құрайды)

Барлық сұрақтар бойынша кеңестер СРОП-тың ағымдағы семестр графигіне сәйкес жүзеге асады.

11. Тәлімгерлердің білімін тексеру кестесі

Тәжірибелік, зертханалық сабақтары мен СӨЖМ 0-100 баллмен бағаланады

Пән бойынша тапсырмаларды орындау мен тапсыру графигі

№	Жұмыс түрлері	Тақырып, мақсат және тапсырма мазмұны	Ұсынылатын әдебиет	Орындау ұзақтығы	Бақылау формасы	Тапсыру мерзімі
1	2	3	4	5	6	7
1	Тәжірибелік жұмыс 1	«Сәкі шифрі»	2, 5, 6	3 жұма		4-ші жұма
2	Тәжірибелік жұмыс 2	Вертикалды ауыстырым әдісі	2, 5, 6	3 жұма		8- ші жұма
3	Зертханалық жұмыс 1	Цезарь шифрі	2, 5, 6	7 жұма		8- ші жұма
4	Межелік бақылау	2 тәжірибелік жұмыс пен 1 зертханалық жұмысты қорғау			сынақ	8- ші жұма
5	Тәжірибелік жұмыс 3	Виженер шифрі	2, 5, 6	3 жұма		12- ші жұма
6	Тәжірибелік жұмыс 4	Бұрылма тор әдісі	2, 5, 6	2 жұма		14- ші жұма
7	Зертханалық жұмыс 2	Плейфейер шифрі	2, 5, 6	7 жұма		14- ші жұма
8	Курстық жұмыс	Бекітілген тақырып бойынша		8 жұма	сынақ	14- ші жұма
9	Межелік бақылау	2 тәжірибелік жұмыс пен 1 зертханалық жұмысты қорғау			сынақ	15- ші жұма

12. Тәлімгерлердің білімін бағалау критерийлері

Пәнді оқыту барлыө өткен мәлеметтерден тұратын тест түріндегі емтихаенмен аяқталады. Емтиханға жібеілудің міндетті шарты бағдарламада берілген барлық тапсырмаларды орындау болып табылады.

Әрбір тапсырма 0-100 баллмен бағаланады.

Жіберілу рейтингі ағымдағы сабақтардағы (дәрісте болу, үй жұмыстары, СРО бойынша тапсырмалар, тәжірибе бойынша тапсырмалар және басқалары, межелік бақылау) орындалған тапсырмалардың орташа арифметикалық ортасын табу арқылы анықталады.

Пән бойынша қорытынды бақылауға (ҚБ) жұмыс оқу бағдарламасының барлық талаптарын (барлық тәжірибелік, зертханалық жұмыстары мен СРО бойынша тапсырмаларды орындау және тапсыру) орындаған, курстық жобаны (жұмысты) қорғауда жақсы баға алған және жіберілу рейтингін (50 баллдан кем емес) алған студенттер ғана жіберіледі.

Әрбір пән бойынша студенттердің оқу жетістіктерін ЖР мен ҚБ (емтихан, дифференциалды сынақ немесе курстық жұмыс/жоба) бағаларын салмақтық үлестерін ескере отырып қосындыдан анықталатын қорытынды (Қ) баға бойынша анықтайды.

Қ = ЖР*0,6 + ҚБ*0,4

СалмақтықүлестерВ жыл айын университет ғылым кеңесінде бекітіледі және ЖР үшін 0,6-дан көп емес, ал ҚБ үшін 0,3-тен кем емес.

ҚЖ/КЖ комиссия алдында қорғалады. Баға көрсетілген білім мен оқытушы пікірі негізінде қойылады.

Пән бойынша қорытынды баға тәлімгердің жіберу рейтингі мен қорытынды бақылау бойынша жақсы бағалары болған жағдайда саналады. Қорытынды бақылауға себепсіз келмеу «қанағаттанбайтын» бағаға тең болады. Пән бойынша емтихан мен межелік аттестация нәтижелері сол күні не егер жазбаша емтихан күннің екінші жартысында өткізілсе келесі күні студенттерге айтылады.

Білімнің қорытынды бағасының орындылығы үшін тәлімгер межелік бақылауда (рейтинг) және қорытынды емтиханда 0-ден 100%-ге дейінгі пайызбен бағаланады.

Межелік бақылау бағасы ағымдағы баға мен межелік бақылау бағасы қосндысынан құралады.

Оқу жетітіктері, яғни білімдер, дағдылар, икемдіктері мен құзыреттері көпбалдық әріптік жүйе бойынша, сонымен бірге оның цифрлық эквиваленті мен дәстүрлі баға шкаласына сәйкес бағаланады:

Әріптік жүйе бойынша баға	Баллдардың цифрлік эквиваленті	Проценттік мазмұны	Дәстүрлі жүйе бойынша бағасы
A	4,0	95-100	Өте жақсы
A-	3,67	90-94	
B+	3,33	85-89	Жақсы
B	3,0	80-84	
B-	2,67	75-79	
C+	2,33	70-74	Қанағаттанатын
C	2,0	65-69	
C-	1,67	60-64	
D+	1,33	55-59	
D	1,0	50-54	
F	0	0-49	Қанағаттанбайтын

13. Оқытушы талаптары, саясат пен тәртіптер

Тәлімгерлердің аудиториялық сабақтарына кешігусіз қатынасу міндетті болып табылады. Сабаққа келмей қалған кезде деканатта бекітілген тәртіп бойынша өтеледі. Максимум екі рет сабақтан қалу ғана жіберіледі. Сабаққа екі рет кешігу бір рет сабаққа келмеуге теңеледі. Екі реттен көп рет сабақтан қалған кезде оқытушының студетті мәселенің әкімшілік щешіміне дейін сабаққа кіргізбеуге құқығы бар. Дәрісте бөтен студент емес адамдардың болуы рұқсат етілмейді.

Жұмыстарды белгіленген мерзімде тапсыру қажет. Барлық тапсырмаларды тапсырудың ақырғы мерзімі – емтиханға дейінгі 3 күн.

Барлық тапсырмаларды тапсырмаған, курстық жұмысты қорағмаған студенттер емтиханға жіберілмейді.

Әрбір оқу сабағының өтілген материалдары бойынша тақырыпты қайталау мен өтелу міндетті болып табылады. Оқу материалдарын игеру деңгейі тестер мен жазбаша жұмыстармен тексеріледі. студенттерді тестілеу ескертусіз өтілуі мүмкін.

Оқытушы жетекшілігімен өтетін өздік жұмысты орындауда (СӨЖМ) келесі төрт негізгі функцияны ескеру қажет.

Біріншісі – пәннің бекітілген оқу бағдарлама бойынша өткізілетін сабақтар кезінде оқытушының беретін ақпаратын студенттер активті қабылдауы керек.

Екінші функция бойынша студенттер оқытушы кеңесі бойынша оқу*әдістемелік құралдар мен әдеби оқыту көздерін қолдана отырып үй жұмысын, бақылау жұмыстарын және курсытқ жұмыстарды орындайды. Бұл кезеңде студенттен жұмыс әдістерін білу, өз-өзін ұйымдастыру, өз-өзін ұстау талап етіледі.

Үшінші функция студенттер қиын жағдайда анализ бен жүйелеу, қиыншылық себептерін түсіну мен басқа оқу әрекеттерін орындауы тиіс. Студенттер қиын сұрақтарды оқытушыдан сұрап, өз жауаптарын тексереді.

Студенттің төртінші функция оқытушыдан кеңес алудан тұрады.

14. Әдебиет тізімі

Негізгі

1) Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. – М.: Логос; ПБОЮЛ Н.А. Егоров, 2001.

2) Скляров Д.В. Искусство защиты и взлома информации. — СПб.: БХВ-Петербург, 2004.

3) Жельников В. Криптография от папируса до компьютера. – М.: Dore Print, 1999.

4) Сёмкин С.Н., Беляков Э.В., Гребенёв С.В., Козачёк В.И. Основы организационного обеспечения информационной безопасности объектов информатизации. – М.: «Гелиос АРВ», 2005.

5) Саломаа А. Криптография с открытым ключом: Пер. с англ. — М.: Мир, 1995.

6) Хорошко В.А.. Чекатков. Методы и средства защиты информации. — Вінниця: ВДТУ, 2003.

Қосымша

7) Законодательные акты РК в области защиты и безопасности информации.

8) Нормативные документы РК в области защиты и безопасности информации.

9) Грушко А.А., Тимонина Е.Е. Теоретические основы защиты информации.-М.: «Яхстмен»,1996.

10) Хореев А.А. Способы и средства защиты информации. Учебное пособие.-М.: МО РФ, 2000.

15. Мультимедиялық сүйемелдеу тізімі

1) Fine Reader 5.0
2) MS Office
3) Borland Delphi 7.0