Қазақстан Республикасы Білім және ғылым министрлігі

С. Торайғыров атындағы Павлодар Мемлекеттік Университеті

Информатика және ақпараттық жүйелер кафедрасы

050703 – Ақпараттық жүйелер мамандығының студенттеріне арналған
«Ақпаратты қорғау және қапарттық қауіпсіздік» пәні бойынша
тәжірибелік және зертханалық жұмыс орындауына арналған

ӘДІСТЕМЕЛІК НҰСҚАУЛАР

Павлодар

ерждения
ого указания

Форма
Ф СО ПГУ 7.18.1/05

БЕКІТЕМІН
ФМжАТФ-інің деканы
_____ Тлеукенов С.К.
«__»_____2008ж.

Құрастырушы: аға оқытушы Ақанова Ақерке Сапарқызы

Информатика және ақпараттық жүйелер кафедрасы

050703 – Ақпараттық жүйелер мамандығының студенттеріне арналған
«Ақпаратты қорғау және ақпараттық қауіпсіздік» пәні бойынша
тәжірибелік- зертханалық жұмыстарға арналған

ӘДІСТЕМЕЛІК НҰСҚАУЛАР

Кафедра отырысында құпталды

“_____” _____200__ж. Хаттама №_____

Кафедра меңгерушісі_____ Ж.К.Нұрбекова

«ФМжәнеАТ» факультетінің оқу-әдістемелік кеңесінде мақұлданды “_____” _____200__ж. Хаттама №_____

ӘК төрағасы _____А.З.Даутова

Негізгі теориялық жағдайлар.

Шифрлеудің классикалық үлгісі. Оларды қою кезінде қолдану. Қою кезінде ашық мәтіннің жекеленген әріптері басқа әріптермен немесе сандармен, немесе басқа символдармен ауысады. Егер ашық мәтін тізбектелген биттер ретінде қаралатын болса,онда шифрленген мәтіннің тізбектелген биттерімен берілген ашық мәтіннің тізбектелген биттерімен ауыстыруына әкеледі.

Зертханалық жұмыс №1.

Тақырып : Криптография . Ауыстыруға арналған шифрлар .

Жұмыс мақсаты : криптография негізгі ұғымдарын, криптографиялық жүйелердің таптастыруын , ауыстыруға арналған цезарь шифрын зерттеу .

1. Теориялық мәлімдеудің

1.1 Криптография : негізгі ұғымдары.

Компьютерлердің және автоматтандырылған ақпарат құралдарының кең тарауы мен пайда болуы, файлдарды және компьютердегі сақталатын ақпаратты қорғайтын автоматтандырылған құралдардын пайдалануын қажет етті. Қорғау құралдарының аса қажеттілігі көппайланушылар жүйесінде және де телефон желісі арқылы қосылатын немесе ашық компьютерлік желілерде байқалады. Хакерларға қарсы әрекет ретінде және мәліметтерді қорғауға арналған әдістер мен құралдарды сипаттау үшін **компьютерлік қауіпсіздік** термині пайда болды.

С помощью рисунка 1 рассмотрим основные элементы схемы традиционного шифрования.

Желі мен коммуникацияны қорғайтын негізі автоматтандырылған құралдын бірі шифрлау болып табылады.

Жасырын түрде берілетін мәлімдемені **ашық мәтін** деп атайды. Ашық мәтінді өзгелерге мәні түсінікті болмас үшін оны өзгертеді, бұл өзгертуді **шифрлау** деп атайды. Мәтінді шифрлау нәтижесінде шифрланған мәтін болып шығады.Кері әрекетті дешифлау деп атайды, немесе шифланған мәтінді қалпына әкелу. Заңсыз пайдаланушылар қорғау мақсатында, ақпаратты бір таңбадан екінші таңбаға ауыстыруды зерттейтін ғылымды **криптография** дейді.

№1 суреттке қарап дәстүрлі шифрлау сызбасының негізгі элементтерін қарастырайық.

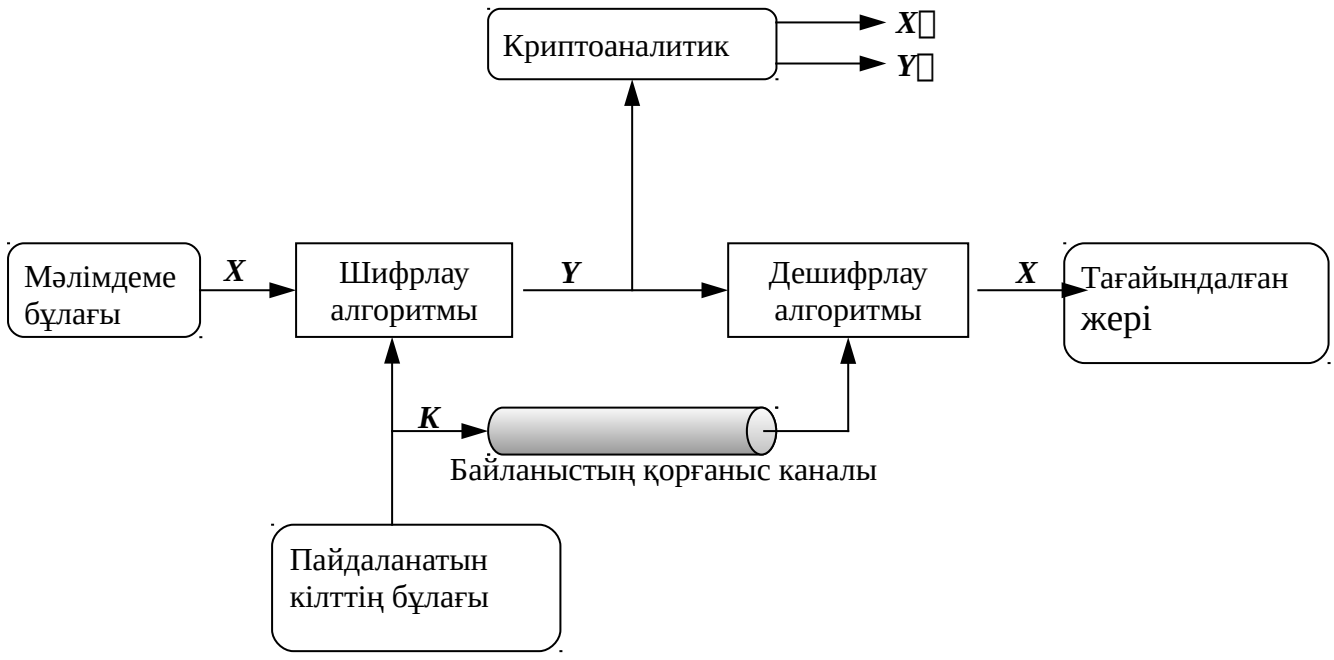


Рисунок 1 - Модель традиционной криптосистемы

Мәлімдеме бұлағы мәлдемені $X=[X_1,X_2,...X_м]$ түрінде ашық мәтінді құрастырады. Ашық X мәтіннің X_i элементтері болып қандай да бір шекті алфавиттың символдары болады. Ол мәліметті шифлау үшін қандайда бір кілт $K=[K_1,K_2,\ldots, K_J]$ ойластырылады. Берілген X мәтін

мен K кілті алынып шифрлау алгоритмы арқылы мәлімдеме шифраладыда шифрланған мәтін $Y=[Y_1,Y_2,\ldots, Y_N]$ шығады. Мұны формула арқылы көрсетуге болады:

$Y = E_K(X)$.

Бұл формуланы, Y-тің шығуы K кілтін қолданып E шифрлау алгоритмын X мәтініне пайдалануы арқылы болған. Қабылдаушы берілген кілтті пайдалана отырып кері әрекет жасай білу керек:

$X=D_K(Y)$.

Бөгде адам Y пен таныса келгенде? Ол K және X қалпына келтіруді тырысады. Осыған қарағанда Сол адам E шифрлау алгоритмын және D дешифрлау алгоритмын білуі мүмкін. Егерде бөгде адам қандайда X мәтінді ғана білгісі келсе онда ол осы X ашық мәтініне ықтималдықты құрастыраду жолдарын қарастырады. Егер мәтіннің барлығы керек болса ықтималдықты құрастыру жолдарымен K кілтін қарастырады.

1.2 Криптографиялық жүйелердің жіктелуі

Жалпы жағдайда криптографиялық жүйелердің жіктелуі келесі тәуелсіз сипаттармаларға негізделген.

Ашық мәтінді шифрленген түрге келтіру операция типі. Барлық шифрлеу алгоритмдері екі операцияға: ашық мәтіннің әрбір элементін (битті, әріпті, биттер немесе әріптер топтарын) қандай да бір басқа элементпен алмастыруды білдіретін **ауыстыру** және ашық мәтін элементтерінің орналасуын өзгертуді білдіретін **орналастыруға** негізделген. Бұл жағдайда басты талап ақпаратты жоғалтудың болмауы (яғни барлық операциялардың қалпына келуі). Көптеген нақты шифрлеу жүйелерінде біреу емес, бірнеше ауыстыру және орналастыру комбинацияларын қолданады. Сәйкес шифрлер **өнімді** деп аталады.

1.1. **Қолданылатын кілттер саны.** Егер жіберуші мен алушы бір кілт қолданса, жүйе симметриялық, бір кілтті жүйе, құпия кілтті жүйе немесе дәстүрлі шифрлеу схемасы деп аталады. Егер жіберуші мен алушы әр түрлі кілттер қолданса, онда жүйе ассиметриялы, екі кілтті жүйе немесе ашық кілтті шифрлеу схемасы деп аталады.

1.2. **Ашық мәтінді өңдеу әдісі.** **Блоктық шифрлеу** ашық мәтінді блоктармен өңдеуді білдіреді. Әр блокты өңдеу нәтижесінде шифрленген мәтін блогы пайда болады. **Ағымды шифрлеу** ашық мәтіннің барлық элементтерін бірінен соң бірін шифрлеуді білдіреді, нәтижесінде әр кезеңде шифрленген мәтіннің бір элементі пайда болады.

1.3 Шифрлеудің классикалық техникасы. Қойылымдарды қолдану

Қойылым кезінде ашық мәтіннің жеке әріптері басқа әріптер, сандар немесе басқа да бір символдармен ауыстырылады. Егер ашық мәтін биттер тізбегі ретінде қарастырылса, онда қойылым ашық мәтіннің белгілі биттер тізбегі шифрленген мәтіннің белгілі биттер тізбегімен ауыстырылады.

Тапсырма

АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ.

Цезаря шифрын пайдаланып берілген мәлімдеоелерді шешу керек. Қозғалу өлшемі белгісіз. Паскаль тілінде программа құрындар.

1 кесте – тапсырмалар нұсқасы.

№нұсқа.	**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.	ЙЧСЦЮЬЪЩЩМЛЫЪРЫФЭИЭЪЪНЕСЩФЛРЪЦМУЗОМСЮГЮЪЪЮЫЬМО ФЮСЧСШНЗЧРСХЭЮОФЮСЧИЩЪЭЪУРМЮСЧИЭЪЪНЕСЩФЛ
10.	ЖКВИУКУЭВГЦПАНИШЕЧКЙЧЪЪАЬЭЙЭИКАМАВШКЖЪВГЦПЭБВЖКЖ ИУЭЪВГЦПШЦКЪЙЭЩЧАЬЭЕКАМАВШКЖИЗЖГФЯЖЪШКЭГЧ

Зерханалық жұмыс № 2.

Тақырыбы: ащық мәтіннің статистикалық мінездемесі.

Тасмалдаушыға(қағаз, магниттік диск) жазылған ақпараттың кезкелгені қорғауға жатадын.

Сондағы мәлімдеме қандай да бір алфавиттің тізбегінен тұрады.Алфавит екіге бөлінеді табиғи алфавит (қазақ, ағылшын, оры т.с.с) және арнайы алфавит (Морзе әліппесі, компьютер кодтарты т.б).

Төмендегі қарастыратынымыз адам арасындағы байланыста пайдаланатын тілдер алфавиты, сонын ішіндегі орыс және ағылшын алфавитіне және олардың лингвистикалық ерекшеліктеріне тоқталық. Сондай ақ ерекшклікті талдау жасайтын тәсілдер барлық тілдерге бірдей пайдаланылады.

Орыс алфавиты төмендегі 33 әріптен тұрады:

А, Б, В, Г, Д, Е, Ё, 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.*

Байланыстын техникалық каналдары арқылы тасымалданатын мәлімдемелерге әдетте қысқартылған орыс алфавиты пайдаланылады, мұнда Ё-Е, Й-И, Ъ-Ь бір әріп полып есептеледі. Кейде оқуға ынғайлы болсындеп сөз арасына - бос орын белгісін қояды.

Ағылшын толық алфавиты 26 әріптен тұрады:

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.

Байланыстын техникалық каналдары арқылы тасымалданатын мәлімдемелерге әдетте қысқартылған орыс алфавиты пайдаланылады, мұнда I - J бір әріп полып есептеледі. Кейде оқуға ынғайлы болсындеп сөз арасына - бос орын белгісін қояды.

Арнайы алфавиттардың бірі болып – Морзе әліппесі, ASCII (American Standart Code for Information Interchange) және т.б.

Цезарь шифры.

Белгілі қойылымды шифрлардың ең көне және ең қарапайымы, Юлий Цезарь қолданған шифр болып табылады. Цезарь шифрінде алфавиттің әр әрібі, сол алфавитте үш орынға әрі қарай орналасқан әріппен ауыстырылады. Бұл жерде алфавит «циклдық» болып саналады, яғни Я әріпінен кейін А әрібі кетеді. Мысалы, мына алфавит 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 өтеді:

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

Жасалымды анықтау үшін барлық мүмкіндіктерді қарастыру керек.

Ащық мәтін:	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 мәтін:	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 сандық эквивалент белгілесек (А = 1, Б = 2 және т.б.), онда шифрлеу алгоритмін келесі формулаларымен беруге болады.Р ашық мәтіннің әр әрібі С шифрленген мәтіннің әрібімен ауыстырылады:

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

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

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

Мұндағы *k* 1-ден 31-ге(қарастырылған алфавит үшін) дейінгі диапазонда мән қабылдай алады. Дешифрлеу алгоритмі де қарапайым:

$$P = D(C) = (C-k) \bmod (26).$$

Егер анықталған мәтіннің, Цезарь шифрінің көмегімен аяқталғаны белгілі болса, онда шифрді барлық мүмкіндіктерді қарапайым таңдау арқылы ашу өте оңай - бұл үшін кілттің 31 мүмкіндігін тексеру жеткілікті.

Барлық мүмкін түрлердің реттік таңдау әдісін қолдану берілген шифрдің негізгші үш сипаттамасымен айқындалады.

1. Шифрлеу және дешифрлеу алгоритмдері.
2. Барлық 31 нұсқаны таңдау қажет.
3. Ашық мәтіннің тілі белгілі және түсінікті.

Көптеген жағдайларда, компьютерлік ақпаратты қорғау туралы сөз қозғалса, алгоритм белгілі деп алынады. Криптоанализ реттік таңдау әдісі кезінде қажетсіз әрекеті - көптеген кілттерді қажет ететін алгоритмді қолдану.

Тапсырма

Плейфейер шифра пайдаланғанда орыс алфавитінен Ё әріпі (заменяется буквой Е) және Й әріпі (заменяется буквой И). Ъ и Ь әріптері бір әріппен белгіленеді. Келесі 31 әріп тен тұратын алфавит бойынша матрица құрылады да 5 жол мен 6 бағаннан тұрады.

АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ,

Мысалы,ПАРУСНИК кілт сөзі келесі түрде болады.

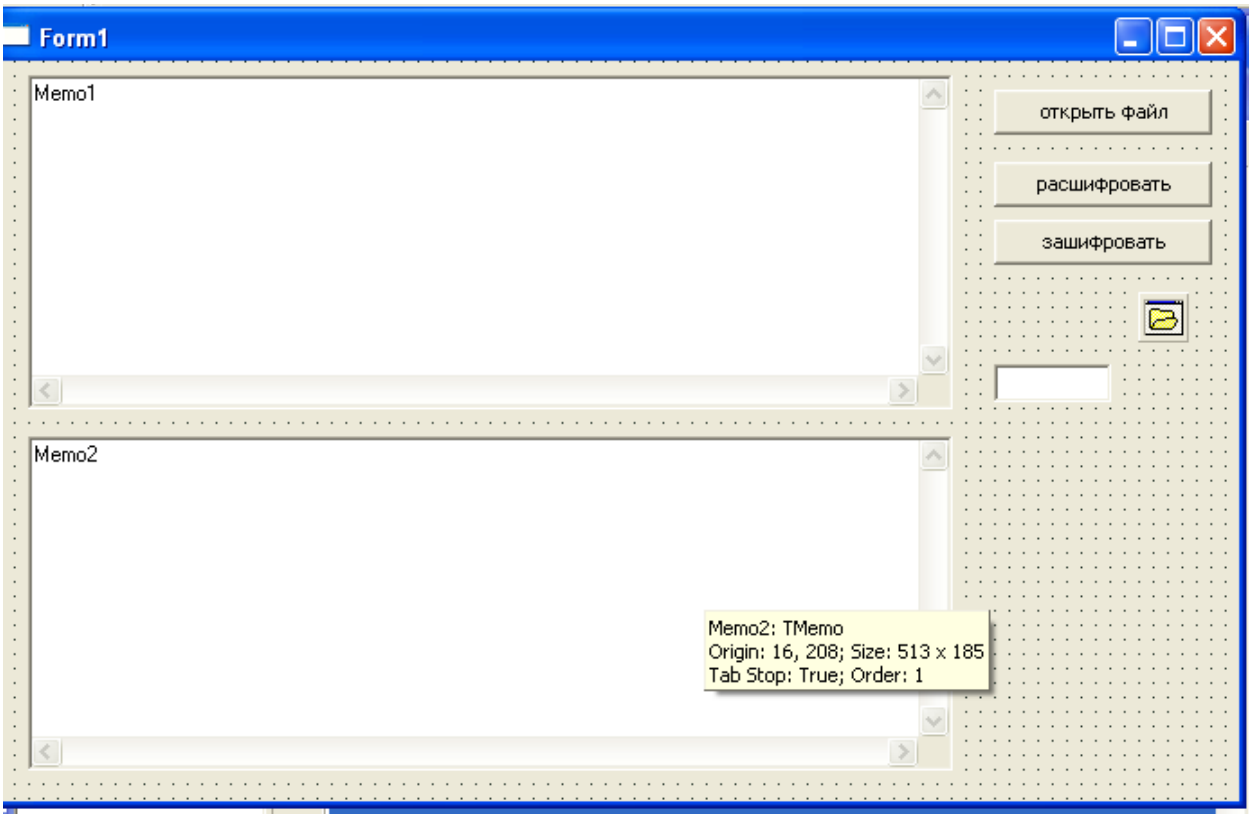
П	А	Р	У	С	Н
И	К	Б	В	Г	Д
Е	Ж	З	Л	М	О
Т	Ф	Х	Ц	Ч	Ш
Щ	Ъ/Ь	Ы	Э	Ю	Я

Таблицадан 1 кілт сөзді алыпПлейфер шифрын пайдаланып келесі сөйлемді кодыландар «КОД ПЛЕЙФЕЙЕРА ОСНОВАН НА ИСПОЛЬЗОВАНИИ МАТРИЦЫ БУКВ» и кестедегі берілген символдар тізбегін декодтандар.

Таблица 1 -

№ вар.	**Тапсырма**
1.	Кілт сөз: ПОЛЕТ Декодтауға арналған символдар тізбегі: КЛКЕПЕШОБКЕРЭЛЧСКУЛЮЕТВМВКИММЮЗОТЖША
2.	Кілт сөз: ФИЛЬМ Декодтауға арналған символдар тізбегі: НПВЪЗПЖИКЛБЦРПЪПЭИЯЩЛИЗПБКФАГПШУХЭЧЖРЫВЦТУНЧТЩЧНХНЩТНЯХКДНЦВЗТЧИ
3.	Кілт сөз: КАТЕР Декодтауға арналған символдар тізбегі: ЗЛНЖКГСЩЯЪАОЕСМЩЯСОЛКДБОУЩФРКЖФТАРТЮВИОАСЫЫРМРЕПМЩ
4.	Кілт сөз: ПАРОЛЬ Декодтауға арналған символдар тізбегі: ЮОГНФПЛМКЮМВРМХИНЦШБЛГЖМУПЕАЮЖЧЗПДАМАЛНЪЖЕАДПУНЕЛСЪ

	МЧПМЪЗЧЪЭАЩЩНТЗЗУАД
5.	Кілт сөз: КОЛЬЦА Декодтауға арналған символдар тізбегі: МИПГПДПМЖВТЩВИЕИЛРЩЧЗОЛИНЦЩХЖПЪРВЦТУОЖАЫВХУКЖЕВИ
6.	Кілт сөз: КАМЕНЬ Декодтауға арналған символдар тізбегі: РСРФЪПЧСВЛНПНЪСШТОБСХЪИЪФОПГИМФАНЪУКГЩЛНВНКХЧЪДУНЛМАХ КСЛИЧТБЕУ
7.	Кілт сөз: СОЛНЦЕ Декодтауға арналған символдар тізбегі: ЗОИЦОЫИТЗУСОШЖАЦФАВЗЗКЗЧНБЗЖУКПБЕЫТЗЪЗФЩ
8.	Кілт сөз: ТОВАРИЩ Декодтауға арналған символдар тізбегі: МОЩЕЯВЧЪЛТАПЯВМОМРЗФИЫПТБКВИХБЦБЩШЪЧШЩИВТЧОАДХОПАБТИВ АРМЖИ
9.	Кілт сөз: СВЯЗЬ Декодтауға арналған символдар тізбегі: ЛМЧШЮГХТЯПХООПКПЖМКЧВЦАОБФЖГКХПНЯВЖФЪЛЯНХОФЗТЪСЦПИЛФ ЛЪ
10.	Кілт сөз: МАТЕРИЯ Декодтауға арналған символдар тізбегі: УЕНАЕЭМЧЗПФТКСЪИАРУЕПЕСЯЕХТИСЩГХМЖФЗЧБГЩКМЮАЕЪ




```
unit Unit1;

interface

uses
```

```
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls, Forms,
  Dialogs, StdCtrls;

type
  TForm1 = class(TForm)
    Memo1: TMemo;
    Memo2: TMemo;
    Button1: TButton;
    Button2: TButton;
    OpenDialog1: TOpenDialog;
    Button3: TButton;
    Edit1: TEdit;
    procedure Button2Click(Sender: TObject);
    procedure Button1Click(Sender: TObject);
    function deshifer(str:string;sdvig:integer):string;
    procedure FormShow(Sender: TObject);
  private
    { Private declarations }
  public
    { Public declarations }
  end;

var
  Form1: TForm1;
  kiril_niz:string;
  kiril_verh:string;
  latin_niz:string;
  latin_verh:string;
implementation
{$R *.dfm}

function tform1.deshifer(str:string;sdvig:integer):string;
var
st:String;
i,n:integer;
begin
for i:=0 to Length(str)-1 do
  begin

  end;
Result:=st;
end;

procedure TForm1.Button2Click(Sender: TObject);
begin
if OpenDialog1.Execute then
  begin
     Memo1.Clear;
     Memo1.Lines.LoadFromFile(OpenDialog1.FileName);
  end;
end;

procedure TForm1.Button1Click(Sender: TObject);
var
i,j:integer;
begin
```

```
for i:=0 to Memo1.Lines.Count-1 do
  begin
    Memo2.Lines.Add(deshifer(memo1.Lines[i],strtoint(edit1.text)));
  end;
end;

procedure TForm1.FormShow(Sender: TObject);
begin
kiril_niz:='абвгдеёжзийклмнопрстуфхцчшщъыьэюя';
kiril_verh:='АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ';
latin_niz:='abcdefghijklmnopqrstuvwxyz';
latin_verh:='ABCDEFGHIJKLMNOPQRSTUVWXYZ';
end;

end
```

Лабораторлық жұмыс №3

Тақырып: Шифр Хилла

Тапсырма: Хилла әдісі бойынша шифрация мен дешифрация программасын жасау

Бақылау сұрақтары:

1. Шифрацияның алгоритімі
2. Дешифрацияның алгоритімі
3. Әдістің талдауы

Лабораторлық жұмыс №4

Тақырып:Мәтінді архивтеу

Тапсырма: Текстi және программаның әдісін іске асыру

1. Таңдалынған архивтік әдіс ненің негізінде болады
2. Шығыс файлына тоқтау бола ма?
3. Қосымша кітапханалар бар ма?
4. Архивтау алгоритмі
5. Архивтен шығу алгоритмі
6. Қысылған алгоритм қаншалықты қолайлы?
7. Әдістің талдауы

Лабораторлық жұмыс №5

Тақырып: Шифрация мәтінінің суреттегі әдісі

Тапсырма: Берілген әдісті пайдаланып мәтінді шифр арқылы суретте қолданудың программасын құру

Бақылау сұрақтары:

1. bmp файлна шектеу бар ма?
2. bmp файлының өлшемі және кодтау текстінің ұзындығы арасында қандай байланыс анықталады
3. Визуалды алынған сурет өзгереді ме?
4. Шифрация алгоритімі
5. Дешифрация алгоритімі
6. Әдістің талдауы

Тәжірибелік жұмыс №1

Тақырыбы: «Лесёнка» шифрі.

Тапсырма: Ашылған текстке «Лесёнка» шифрі қолданылған. 3-таблицадағы шифрланған мәтіннің мәліметін қалпына келтір.

Бақылау сұрақтары:

1. Бұл тәсілдегі кілт нені көрсетеді?
2. Шифрация кезінде мәлімет қалай жазылады?
3. Шифрация кезінде кодталған мәлімет қалай есептеледі?

4. Дешифрация кезінде кодталған мәлімет қалай жазылады?
5. Дешифрация кезінде кодталған мәлімет қалай есептеледі?
6. Дешифрацияны белгісіз кілтпен ұйымдастыруға бола ма?
7. Дешифрациядан кейін мәліметтің дұрыс нұсқасын программалық анықтауға бола ма?
8. Шифрацияның алгоритмі.
9. Дешифрацияның алгоритмі.
10. Әдістің талдауы.

Тәжірибелік жұмыс №2.

Тақырыбы: Көлденең ауыстыру әдісі.

Тапсырма: Талдау жасау барысындағы табылған мәліметтер, көлденең шифрациялануы әдісінің ауыстырылуы, криптоналитиктердің көмегімен осыны қалпына келтіру кілтін бөлшектеп табыу. Кілтте қанша символдар бар екенің анықтауды, сонымен бірге сандардын кейбір түрінің сандық әдісте қолдануын анықтау. Криптоналитиктердің жасаған жұмыстарының нәтижесінде жолдық түрлер, кілттің ұзындығымен сәйкес келетін, X символымен кілттік позициясы көрсетілген, қазіргі кезде мәні белгісіз.(см. 4-кестеде тапсырма). Сіздің міндетіңіз шифрленген мәліметке сәйкес шифрмәтінді аяқтау, кілтті қалпына келтіру және ашық мәтінді алу.

Бақылау сұрақтары:

1. Осы әдістегі кілт нені білдіреді?
2. Шифрация кезінде мәліметтер қалай жазылады?
3. Топталған мәліметтер шифрация кезінде қалай саналады?
4. Дешифрация кезінде топталған мәліметтер қалай саналады?
5. Мәліметтерді қалпына келтіру дешифратор кезінде қалай саналады?
6. Дешифраторды белгісіз кілтпен ұйымдастыруға болады ма?
7. Мәліметтердің дұрыс нұсқасын дешифрациядан кейін бағдарламалық анықтауға болады ма?
8. Шифратор алгоритімі.
9. Дешифратор алгоритімі.
10. Әдісті талдау.

Тәжірибелік жұмыс №3

Тақырыбы: Виженер шифры

Тапсырма: Виженер әдісін қолданып, шифрациялау және дешифрациялауға программа құрастыру.

Бақылау сұрақтары:

1. Виженер тақтасы деген не?
2. Виженер тақтасын қалай ұйымдастыруға болады?
3. Шифрация алгоритімі.
4. Дешифрация алгоритімі.
5. Дешифрацияны белгісіз кілтпен ұйымдастыруға болады ма?
6. Мәліметтердің дұрыс нұсқасын операциядан кейін анықтауға болады ма?
7. Кілтке шектеу қою.
8. Әдісті талдау.

Тәжірибелік жұмыс. №4

Тақырыбы: Бұрылу торлары әдісі.

Тапсырма: Бұрылу торлары әдісі бойынша шифрация және дешифрацияға бағдарлама жасау.

Бақылау сұрақтары:

1. Шифрациялау алгоритмі.
2. Дешифрациялау алгоритмі.
3. Бұрылу торлары қалай жасалады?
4. Берілген әдісте кілт болып не саналады?
5. Мәліметтер ұзындығы, терезелер саны және торлардың өлшемі арасындағы қатынас қандай?
6. Бағдарламада торлардың өлшемін өзгертуге болады ма?
7. Әдісті талдау.

Тәжірибелік жұмыс. №5

Тақырыбы: Әдістердің комбинациясы.

Тапсырма: Цезарь әдісін, тігінен ауыстыру, Виженер «Сатысы» комбинацияларын қолданып және осы әдістемені іске асыратын бағдарламаны пайдаланатын текстті шифрациялау әдістемесін дайындау.

Бақылау сұрақтары:

1. Шифрациялау алгоритмі.
2. Дешифрациялау алгоритмі.
3. Бағдарлама ашық кілтпен жұмыс істей алады ма?
4. Әдістерді пайдаланудың кезегін ауыстыруға бола ма?
5. Бағдарлама қалай пайдаланылуы тиіс?
6. Әдісті талдау.

Таблица 2.

№ вар	Тапсырма
11.	ИЦРХЭЫЩШШЩРЫЩЩМДРШУРМЮПРЭЪЩЬЭРЪРШШЩТЛЧ РШКЭЗЩМЖВШШРМЮЧЛСШЩРЫЩЩМДРШУР
12.	ФГМКРОНФЩЗТЪЦФЫКШНФНХРТЦЛМИЩЪШИХГЙЫМЫЪЧНШНЩН ЯНХГЩНЪЗФРЧНШНМИЯРМИХХГЭ
13.	ВЦЫБЦГЮМЦСФЦЮГВГУСЩЭЦПГХЯВГДАЫЖЯБЯЙЦЪЫБЩАГЯФБСЕ ЩИЦВЫЯЪГЦЖЮЯЬЯФЩЩ
14.	КЭЧУЙЧБЗЪАДЮНЮКБИЭКЗШФДЙНОЮБМЬЙББЙБДИБЗДАКНОПЛЬЖЖ МДЛОКЯМЬРДУБНЖДИОБСЙКЗКЯДЫИЮКБЙЙКЯКПМКЮЙЫ
15.	ТБВРЭФРАВЭЛЕЪАШЯВЮУАРДШЗХБЪШЕБШБВХЬРЕШБЯЮЫМЧГХВБП ЮФШЭШВЮВЦХЪЫОЗШФЫПИШДАЮТРЭШПШФЫПАРБИШДАЮТЪШ
16.	ШАЖЮЕИДЩЖЦКЮНЫЗАДЯЗЮЗИЫВЫЗДИАЖСИСВАБФНДВАЦЬЪСЯЮ ВЫЫИЪШЦЗШХЭЦГГСЛШЭЦЮВГДАБФНЦ
17.	ШОФТЙЧШЩМЕТУЖЦВЮБУАШЬТ,ЯТУЩОЫЫЙЧЯЭЬЪЬЗКМТЮБСЬСЬ ШЩМЕО
18.	ПМЯПРАГЛЛЩЗПГИОГРЛЩЗИЙЬХМРНОЮАЖРГЙЭКМДГРЯЩРЪЖПНМЙ ЪЕМАЮЛВЙЭЦЖТОМАИЖПММЯЧГЛЖЭ
19.	ЙЧСЦЮЬЪЩЩМЛЫЪРЫФЭИЭЪЪНЕСЩФЛРЪЦМУЗОМСЮГЮЪЪЮЫЬМО ФЮСЧСШНЗЧРСХЭЮОФЮСЧИЩЪЭЪУРМЮСЧИЭЪЪНЕСЩФЛ
20.	ЖКВИУКУЭВГЦПАНИШЕЧКЙЧЪЪАЬЭЙЭИКАМАВШКЖЪВГЦПЭБВЖКЖ ИУЭЪВГЦПШЦКЪЙЭЩЧАЬЭЕКАМАВШКЖИЗЖГФЯЖЪШКЭГЧ

Таблица 3.

№ вар	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 ОИАИОНОООТОЛНИАТРОЕТКЫЗСАИГЕИДЛЬМЗТУАХМТНЧОДЯ

Таблица 4.

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

Есеп берудің мазмұны.

1.Жұмыстың мақсаты.

2.Берілген бағдарламамен орындалатын шифрлеу алгоритмі және берілген әдіс бойынша дешифрлеу.

3.Бағдарламаны бейнелеу.

4.Құрылатын программаға қолданылатын талдаудың шектеулі мүмкіндіктері.

5.Берілген әдіске қолданылатын талдаудың шектеулі мүмкіндіктері.

Әдебиет

1. Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд.: Пер. с англ. – М.: Издательский дом «Вильямс», 2001. - 672 с.

2. Анин Б.Ю. Защита компьютерной информации. – СПб.: БХВ – Санкт-Петербург, 2000. - 384 с.

3. Введение в криптографию/Под общей ред. В.В. Ященко. – СПб.: Питер, 2001. – 288с.

4. Жельников В. Криптография от папируса до компьютера. М.: ABF, 1996

5. Салома А. Криптография с открытым ключом. М.: Мир, 1995.