**ҒТАХР517.956.3, 517.75**

# АҚПАРАТТЫ ҚОРҒАУ ӘДІСІН ПРОГРАММАЛАУ

***Ж.А. Мүсіралиев[1], З.Т. Суранчиева[2], А.С. Маханова[3]***
[1]аға оқытушы,
[2]магистр, аға оқытушы,
[3]магистр, оқытушы,
Қазақ мемлекеттік қыздар педагогикалық университеті,
Қазақстан, Алматы қ., e-mail: musiraliev1945@mail.ru

Бұл мақалада ақпаратты шифрлау және n×m көлеміндегі шифрленген матрица мен оның түрлері қарастырылады. Шифрмәтінді қалыптастыру үшін хабар мәтінін бағаи бойынша кестені толтырудан кейін қатар бойынша кестенің құрамы есептеледі. Егер шифрмәтінді жеті әріп бойынша тобымен жазып отырса, шифрланған хабар алынады. Шифрды ашу кезінде іс-әрекеттер кері ретпен орындалады. Мақалада келтірілген кілттердің ең тиімдісі кестенің өлшемін қолдану болып табылады.

***Түйін сөздер:*** криптография, криптоанализ, криптология, конфиденциалдық, аутентификация, шифрлау, шифрмәтін, кілт.

Қазіргі уақытта есептеу жүйелерінің кеңінен қолданылуы адамның еңбек ету салаларын түгелдей қамтиды. Бұл жағдай баршамызға едәуір жеңілдіктер әкеліп, жаңа мәселелерді туындатты. Олардың бірі – ақпаратты қорғау. Компьютерлік жүйелерде ақпаратты қорғау бүгінгі ғылымның ерекше саласы болып табылады. Төмендегідей ақпаратты қорғау әдістері белгілі [1]:

- жүйе компонентерінің физикалық қатерсіздігін ұйымдастыру тәсілдері;
- бақылау, есепке алу, қатынауды басқару;
- ақпаратты қорғаудың криптографиялық тәсілдері;
- заңдылық шаралары;
- әкімшілік шаралары.

Осы тәсілдердің ішінде біз тек ақпаратты қорғаудың криптографиялық тәсілдерін қарастырдық.

Криптографияның классикалық есебі берілген ашық мәтінді бөтен адам оқи алмайтын түрге келтіру болып саналады. Әрине, бұл түрлендіруді кері бағытта да орындай алатындай болуымыз керек. Криптоанализ есебі болып криптожүйенің сенімділігін бағалау және алгоритмдерге қол сұғу саналады. Криптография және криптоанализ ғылымның бір саласын криптология ғылымы құрайды[2].

Криптографиялық алгоритм жалпыға мәлім болуы тиіс. Қазіргі криптографиялық жүйелер келесі Керкхофф ережесі бойынша құрастырылады [3]:

- алгоритмде қолданылатын түрлендірулер механизмі жалпыға белгілі деп саналады;
- алгоритмнің сенімділігі тек қана құпия кілтке байланысты деп саналады.

Бұл ереженің мағынасын, біздің ойымызша, Брюс Шнайердің «Applied Cryptography» кітабындағы мысалы жақсы түсіндіреді:«Егер мен хатты мысалға Нью-Йорк қаласында, сейфке тығып қойып, сізге тап десем, онда бұл қауіпсіздік емес. Бұл - нағыз түнек. Ал енді мен хатты алып, оны сейфке жауып, сізге сол сейфті барлық спецификацияларымен бірге тапсырайын. Тіпті жүздеген осындай сейфтерді әлемдегі ең епті ұрыларға берейін. Осы жағдайда да сіз менің хатымды сейфтен алып оқи алмасаңыз, онда бұл шын мәнінде де қауіпсіздік болады» [4].

Бүгінгі таңда ақпараттық технологияның жетілуіне байланысты (электрондық ақша, электрондық дауыс беру, цифрлік телекоммуникациялар) криптографиялық тәсілдермен шығарылатын есептердің саны өсті. Қазіргі криптография келесі есептерді шешу үшін қолданылады [5]:

1. Конфиденциалдық.

2. Аутентификация (шынайылықты тексеру). Хабарды алушы хабарды жіберуші көзді анықтай алуы керек. Хабар жіберуші өзінің шынайылығын дәлелдеу қажет.

3. Бүтіндік немесе түгелдік. Хабар алушы қолына түскен мәліметтің жол-жөнекей өзгермегендігіне көз жеткізуі керек. Ал қаскүнем шын хабарды жалған хабармен ауыстыра алмауы қажет.

4. Авторлықтан тайынбау. Хабарды жіберуші кейіннен жасаған іс-әрекеттерінен тайынбауы қажет.

5. Анонимдікті сақтау. Хабар жіберуші немесе алушы кейбір мәліметті жасыра алатындай болуы керек. Мысалы, электрондық ақша алмасу процесін жасыру немесе электрондық дауыс беру мезгілінде кімнің қалай дауыс бергендігін жасыру.

Қазіргі кезде ақпаратты шифрлаудың көптеген әдістері белгілі. Осы әдістердің ішінде ең қарапайымы және ең үнемдісі кестенің өлшемі қызмет ететін жай орын ауыстыру болып табылады [6]. Мысалы, КОМПЬЮТЕРЛІК ЖҮЙЕЛЕРДІ ҚОРҒАУ хабаркестеге баған бойынша кезектесіп жазылады. Кестенің 4 қатардан және 7 бағаннан тұратын толтыру нәтижесі 1-кестеде көрсетілген.

Шифрмәтінді қалыптастыру үшін хабар мәтінін баған бойынша кестені толтырудан кейін қатар бойынша кестенің құрамын есептейді. Егер шифрмәтінді жеті әріп бойынша тобымен жазып отырса мынадай шифрланған хабар алынады:

КЬРЖЛІҒ ОЮЛҮЕҚА МТІЙРОУ ПЕКЕДР.

Шифрды ашу кезінде іс-әрекеттер кері ретпен орындалады.

**1-кесте.** Кестенің 4 қатардан және 7 бағаннан тұратын толтырылуы

| | | | | | | |
|---|---|---|---|---|---|---|
| К | Ь | Р | Ж | Л | І | ғ |
| О | ю | Л | Ү | Е | Қ | А |
| М | Т | І | Й | Р | О | У |
| П | Е | К | Е | Д | Р | . |

Кілт бойынша орын ауыстыру әдісі.Бұл тәсіл кестенің бағандары кілттік сөз, сөздер тіркесі немесе кестенің қатарына теру ұзындығының саны бойынша орын ауыстырылады.

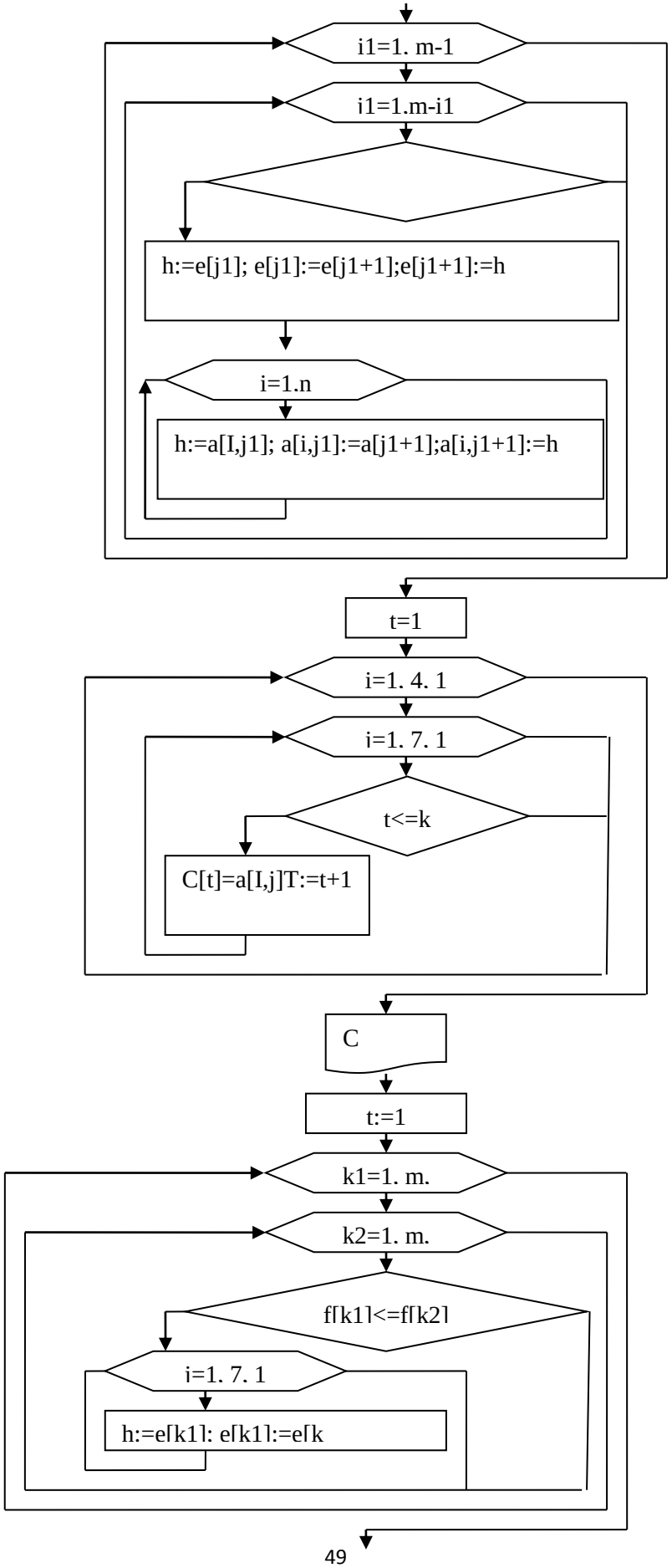
Мысалы, кілт ретіндеТЕХНИКА сөзін қолданайық, ал хабардың мәтінін «компьютерлік жүйелерді қорғау» деп алайық. 2-кестеде хабардың мәтінімен және кілттік сөзбен толтырылған екі кесте көрсетілген, бұл жерде сол жақ кесте орнын ауыстыруға дейінгі толтыруға, ал оң жақ кесте – орнын ауыстырудан кейінгі толтыруға сәйкес [7].

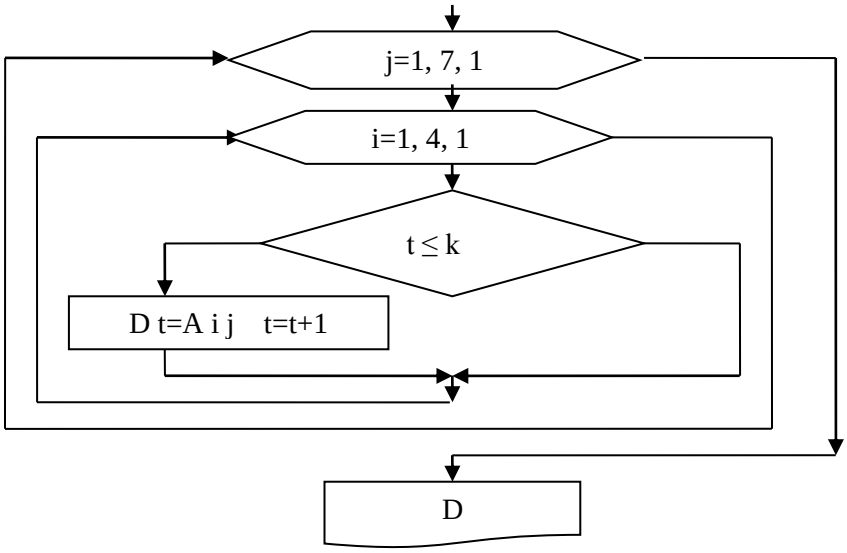
**2-кесте.** Хабардың мәтіні мен кілттік сөзбен толтырылған кесте

Кілт →

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Т | Е | Х | Н | И | К | А | | А | Е | И | К | Н | Т | Х |
| | | | 6 | 2 | 7 | 5 | 3 | 4 | 1 | | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| | | | К | Ь | Р | Ж | Л | І | Ғ | | Ғ | Ь | Л | І | Ж | К | Р |
| | | | О | Ю | Л | Ү | Е | Қ | А | | А | Ю | Е | Қ | Ү | О | Л |
| | | | М | Т | І | Й | Р | О | У | | У | Т | Р | О | Й | М | І |
| | | | П | Е | К | Е | Д | Р | . | | . | Е | Д | Р | Е | П | К |
| | | | а) Орын ауыстыруға дейін | | | | | | | | б) Орын ауыстырудан кейін | | | | | | |

Сол жақ кестенің жоғарғы қатарында кілт, ал кілттің әріптерінің астындағы нөмірлер алфавитте кілттің әріптерінің ретімен сәйкес анықталған. Егер кілтте бірдей әріптер кездессе, олар солдан оңға қарай нөмірленетін еді. Оң жақ кестенің бағандары кілттің әріптерінің реттелген нөмірімен сәйкес орындары ауыстырылған. Оң жақ кестенің құрамындағы қатар бойынша және жеті әріп бойынша шифрмәтіннің тобының жазбасын есептеу кезінде шифрланған хабарды аламыз: ҒЬЛІЖКР АЮЕҚҮОЛ УТРОЙМІ. ЕДРЕПК. Төменде кілт бойынша орын ауыстыру әдісінің блок-схемасы мен Паскаль программалау тіліндегі программасы келтірілген.


i1=1. m-1
i1=1.m-i1
h:=e[j1]; e[j1]:=e[j1+1];e[j1+1]:=h
i=1.n
h:=a[I,j1]; a[i,j1]:=a[j1+1];a[i,j1+1]:=h
t=1
i=1. 4. 1
i=1. 7. 1
t<=k
C[t]=a[I,j]T:=t+1
C
t:=1
k1=1. m.
k2=1. m.
fГk1Ј<=fГk2Ј
i=1. 7. 1
h:=eГk1Ј: eГk1Ј:=eГk




```
begin
clrscr; b:='Kompiuterlikjuielerdikorgau.'; f:='texnika';e:='texnika';
writeln('Ashyk matin =');
writeln; write('B=',B); writeln;
{writeln('Ashyk matin engiz:');}
{for i:=1 to n*m do     write('B[',i,']=',B[i],'  ');  writeln;}
{readln(b);}k:=1;
for j:=1 to m do
for i:=1 to n do
if  b[k]>=nuk then  begin
a[i,j]:=b[k]; k:=k+1; end
else  break;
for i:=1 to n do   begin
for j:=1 to m do
write('A[',i,j,']=',A[i,j],'  ');  writeln; end;
for i1:=1 to m-1 do begin
for j1:=1 to m-i1 do
if e[j1]>e[j1+1] then begin
begin h:=e[j1];
e[j1]:=e[j1+1];
e[j1+1]:=h; end;
for i:=1 to n do begin
h:=a[i,j1];
a[i,j1]:=a[i,j1+1];
a[i,j1+1]:=h;  end;
end; end;
writeln('Ozgergen kilt:');
for i:=1 to m do
write(e[i]);  writeln;
t:=1;
for i:=1 to n do
for j:=1 to m do
if  t<k then  begin
C[t]:=a[i,j]; t:=t+1;end;
write ('Jasyryn matin=',C);writeln;  write ('C=');
for i:=1 to n*m do     write(C[i]);  writeln;
for k1:=1 to m do
```

```
for k2:=1 to m do begin
if  f[k1]=e[k2] then  begin
h:=e[k1]; e[k1]:=e[k2]; e[k2]:=h;
for i:=1 to n do begin
h:=a[i,k1];    a[i,k1]:=a[i,k2];    a[i,k2]:=h; end; end;       end;
{for i:=1 to n do begin
for j:=1 to m do
write('A[',i,j,']=',A[i,j],'  ');  writeln; end;}      t:=1;
for j:=1 to m do
for i:=1 to n do
if  t<k then  begin
d[t]:=a[i,j]; t:=t+1;end;
writeln ('Bastapky matin=',d);  write ('D=');
for i:=1 to n*m do     write(D[i]);  writeln;
writeln (d); Repeat until keypressed; end.
```

**Нәтижесі:**

```
Ashyk matin =

B=Kompiuterlikjuielerdikorgau.
A[11]=K  A[12]=i  A[13]=r  A[14]=j  A[15]=l  A[16]=i  A[17]=g
A[21]=o  A[22]=u  A[23]=l  A[24]=u  A[25]=e  A[26]=k  A[27]=a
A[31]=m  A[32]=t  A[33]=i  A[34]=i  A[35]=r  A[36]=o  A[37]=u
A[41]=p  A[42]=e  A[43]=k  A[44]=e  A[45]=d  A[46]=r  A[47]=.
Ozgergen kilt:
aeikntx
Jasyryn matin=
C=gilijKrauekuolutroimi.edrepk
Bastapky matin=
D=Kompiuterlikjuielerdikorgau.
```

**Пайдаланылған әдебиеттер**


1 Молдовян А.А., Молдовян Н.А., Гуц Н.Д., Изотов Б.В. Криптография. Скоростные шифры. Петербург. 2012

2 Мүсірәлиев Ж., Суранчиева З., Маханова А.С. Электронды сызба құруда логикалық формулаларды қолдану. Қазақ мемлекеттік қыздар педагогикалық университетінің Хабаршысы, 2017. №1. 38-44 бб.

3 Мельников, В. П. Информационная безопасность и защита информации: моногр. / В.П. Мельников, С.А. Клейменов, А.М. Петраков. - М.: Academia, 2016. - 336 с.

4 Шнайер Б. Прикладная криптография. Издательство Триумф. Москва. 2012. (//http://www.ssl.stu.neva.ru/psw/crypto.html)

5 Бабенко Л.К., Ищукова Е.А. Современные алгоритмы блочного шифрования и методы их анализа. - М.: Гелиос АРВ, 2016. - 376 с., илл.

6 Turn R., Ware W. Privacy and security in computer systems, I-A1 Amer. Scientist, vol 63, 2015, pp. 196-203.

7 Ware W., Security and privacy in computer systems, in 2017 S,CC, AFIPS Cont. Proc., vol. 30, 2017, pp. 287-290.

## ПРОГРАММИРОВАНИЕ МЕТОДА ЗАЩИТЫ ИНФОРМАЦИИ

***Ж.А. Мусиралиев[1], З.Т. Суранчиева[2], А.С. Маханова[3]***
[1]ст. преподаватель,
[2]магистр, ст. преподаватель,
[3]магистр, преподаватель,
Казахский государственный женский педагогическийуниверситет,
Казахстан, г.Алматы, e-mail: musiraliev1945@mail.ru

В этой статье рассматриваетсяшифрованиеперестановкой с применением шифровальной таблицы, представляющей собой матрицу размерностью n×m. Для генерации шифрования вычисляется содержимое таблицы после заполнения таблицы в столбце. Если шифр текста будем группировать по семи буквам, получается зашифрованное сообщение. Процесс расшифровкидействия выполняется в обратном порядке. Самым выгодным из приведенных в статье ключей является использование размерности таблицы.

**Ключевые слова:** криптография, криптоанализ, криптология, конфиденциальность, аутентификация, шифрование, шифртекст, ключ.

## THE PROGRAMMING METHOD OF INFORMATION PROTECTION

***Zh.A. Musiraliev[1], Z.T. Suranchieva[2], A.S. Makhanova[3]***
[1]Senior Lecturer,
[2]MSc, Senior Lecturer,
[3]MSc, teacher,
Kazakh State Women's Teacher Training University,
Almaty, Kazakhstan, e-mail: musiraliev1945@mail.ru

In this article an encryption is examined by transposition with the use of enciphering table the being a matrix dimension of n×m. For generating encryption, the compiled tabs are followed by tabulators in the table. If the text is blocked by the text, you will receive the encrypted message. The process of decrypting is executed in the reverse order. Most effective from the considered keys over is using of dimension of table.

***Key words:*** cryptography, cryptanalysis, cryptology, privacy, authentication, encryption, cipher text, key.