

№14 ЗЕРТХАНАЛЫҚ ЖҰМЫС

САБАҚ ТАҚЫРЫБЫ: XOR операция арқылы шифрлеу

САБАҚ МАҚСАТЫ: XOR операция арқылы шифрлеу әдісін пайдалана мәтінді шифрлеу және кері шифрлеу технологиясын үйрену

ҚАРАСТЫРЫЛАТЫН НЕГІЗГІ МӘСЕЛЕЛЕР:

- XOR операция арқылы шифрлеу әдісінің көмегімен ақпаратты шифрлеу
- XOR операция арқылы шифрлеу әдісінің көмегімен ақпаратты кері шифрлеу

Тапсырмалар:

Төмендегі келтірілген программаға келесілерді орындаңыз:

1. алгоритмның блок – схемасын келтіріңіз;
2. осы программаны Делфи тіліне аударыңыз;
3. программаның нәтижесінде экранда құпиясөзді енгізу терезесі мен құпияланған сөздің терезесі болу қажет.

Орындау әдісі

ПРОГРАММА ЛИСТИНГІ:

шифр на основе операции с ключом

Program xor_with_key;

Type

str80 = string[80];

Var

inf, outf: str80;

key: byte;

ch: char;

Procedure code(inf, outf: str80; key: byte);

Var

infile, outfile: file Of byte;

ch: byte;

Begin

assign(infile, inf);

reset(infile);

assign(outfile, outf);

rewrite(outfile);

while not eof(infile) Do

Begin

Read(infile, ch);

ch := key xor ch;

Write(outfile, ch);

End;

WriteLn('файл закодирован');

close(infile);

```
close(outfile);
End;

Procedure decode(inf, outf: str80; key: byte);
```

```
Var
  infile, outfile: file Of byte;
  ch: byte;
Begin
  assign(infile, inf);
  reset(infile);
  assign(outfile, outf);
  rewrite(outfile);
  while not eof(infile) Do
  Begin
    Read(infile, ch);
    ch := key xor ch;
    Write(outfile, ch);
  End;
  WriteLn('файл декодирован');
  close(infile);
  close(outfile);
End;
```

```
Begin
  Write('введите имя входного файла: ');
  ReadLn(inf);
  Write('введите имя выходного файла: ');
  ReadLn(outf);
  Write(' введите односимвольный ключ : ');
  ReadLn(ch);
  key := ord(ch);
  Write('кодировать или декодировать (C or D): ');
  ReadLn(ch);
  If upcase(ch)='C' Then code(inf, outf, key)
  Else If upcase(ch)='D' Then decode(inf, outf, key);
End.
```

Максималды бал зертханалық жұмыстарды уақытысында орындаған және қорғау барысында қойылған сұрақтарға толық жауап берген студентке қойылады.

Қолданылған әдебиеттер:

1. К.С.Дүйсенбекова Ақпараттық қауіпсіздік және ақпаратты қорғау. Әл-Фараби атындағы ҚазҰУ .
2. Тұрым А.Ш., Мұстафина Б.М., Ақпарат қорғау және қауіпсіздендіру негіздері. – Алматы: Алматы энергетика және байланыс институты, 2002ж.
3. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. –М.: РАДИО И СВЯЗЬ, 1999.