Міністерство освіти і науки України
Національний технічний університет України
“Київський політехнічний інститут імені Ігоря Сікорського”
Факультет інформатики та обчислювальної техніки
Кафедра інформаційні систем та технологій

Лабораторна робота №1

із дисципліни «Безпека інформаційних систем»

Тема: «Шифр Цезаря. Шифр Тритеміуса.Шифр Гамування**»**

Виконала:
Студент групи ІА-31
Самелюк А.С.

Перевірив:
Шимкович Л.Л.

Київ-2025

Тема: Шифр Цезаря. Шифр Тритеміуса. Шифр Гамування.

Хід роботи:

1. Шифр Цезаря.

   Шифрування:

   Припустимо, що, використовуючи шифр Цезаря, з ключем, який дорівнює 3, необхідно зашифрувати:

   1) Сьогодні яскраве сонечко світить.
   2) Ми летимо до мрій разом вперед.
   3) Хвилі співають пісню вітрам.

   Для цього зрушимо алфавіт так, щоб він починався з четвертої букви (Г). Отже, беручи вихідний алфавіт і зміщуючи всі літери вліво на 3, отримуємо відповідність:

А	Б	В	Г	Ґ	д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О	П	Р	С
Г	Ґ	д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф

Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я
Х	Ц	Ч	Ш	Щ	Ь	Ю	Я	А	Б	В

   де Г=А, Д=В, Е=Г, і т. д.

   Використовуючи цю схему, отримаємо:

   1) Фасесжрк вфнугдз фсрзьнс фдкхйха.

С => Ф
Ь => А
О => С
Г => Е
О => С
Д => Ж
Н => Р
І => К

Я => В
С => Ф

К => Н
Р => У
А => Г
В => Д
Е => З

С => Ф
О => С
Н => Р
Е => З
Ч => Ь

К => Н
О => С

С => Ф
В => Д
І => К
Т => Х
И => Й
Т => Х
Ь => А

2) Пй озхйпс жс пукм угїсп дтзузж.
3) Шдйок фткдгбха ткфрб дкхугп.

Для того, щоб одержувач повідомлення міг відновити вихідний текст, необхідно повідомити йому, що ключ — 3.

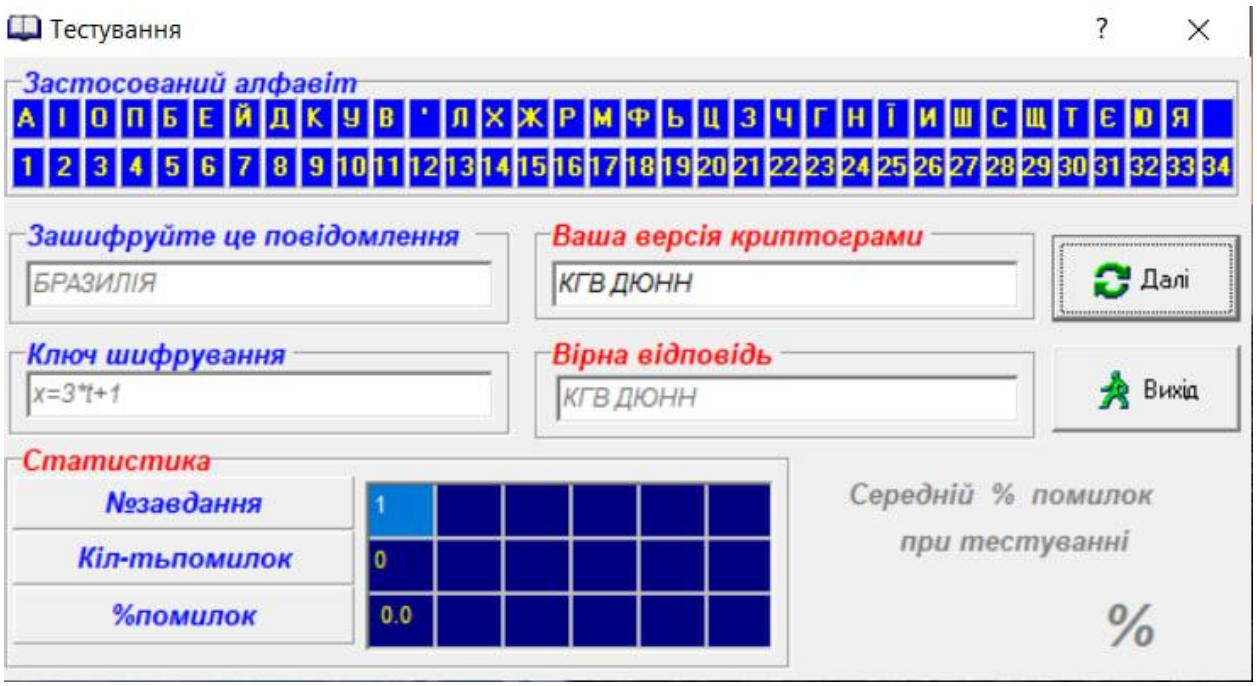
Дешифрування:

1) Сьогодні яскраве сонечко світить.
2) Ми летимо до мрій разом вперед.
3) Хвилі співають пісню вітрам.

2. Шифр Тритеміуса.

Лінійний ключ:

Шифрування:



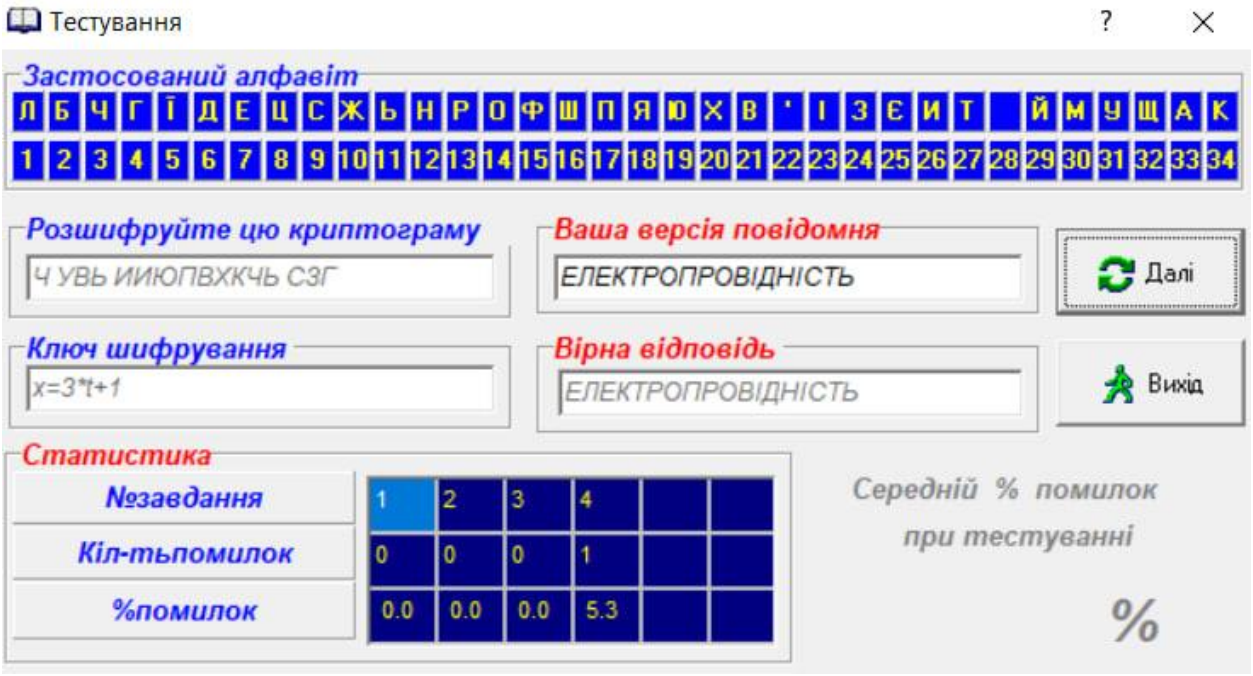
1) Б = 5, 3*1+1=4, (5+4) mod 34 = 9 => К
2) Р = 16, 3*2+1=7, (16+7) mod 34 = 23 => Г
3) А = 1, 3*3+1=10, (1+10) mod 34 = 11 => В
4) З = 21, 3*4+1=13, (21+13) mod 34 = 34 => ‘ ’
5) И = 26, 3*5+1=16, (26+16) mod 34 = 8 => Д

6) Л =13, 3*6+1=19, (13+19) mod 34 = 32 => Ю

7) І= 2, 3*7+1=22, (2+22) mod 34 = 24 => Н

8) Я = 33, 3*8+1=25, (33+25) mod 34 = 24 => Н

Дешифрування:



1) Ч = 3, 3*1+1=4, (3+4) mod 34 = 7 => Е

2) ‘ ’ = 28, 3*2+1=7, (28+7) mod 34 = 1 => Л

3) У = 31, 3*3+1=10, (31+10) mod 34 = 7 => Е

4) В = 21, 3*4+1=13, (21+13) mod 34 = 34 => К

5) Ь = 11, 3*5+1=16, (11+16) mod 34 = 27 => Т

6) ‘ ’ =28, 3*6+1=19, (28+19) mod 34 = 13 => Р

7) И = 26, 3*7+1=22, (26+22) mod 34 = 14 => О

8) И = 26, 3*8+1=25, (26+25) mod 34 = 17 => П

9) Ю = 19, 3*9+1=28, (19+28) mod 34 = 13 => Р

10) П = 17, 3*10+1=31, (17+31) mod 34 = 14 => О

11) В = 21, 3*11+1=34, (21+34) mod 34 = 21 => В

12) Х = 20, 3*12+1=37, (20+37) mod 34 = 23 => І

13) К = 34, 3*13+1=40, (34+40) mod 34 = 6 => Д

14) Ч = 3, 3*14+1=43, (3+43) mod 34 = 12 => Н

15) Ь = 11, 3*15+1=46, (11+46) mod 34 = 23 => І

16) ‘ ’ = 28, 3*16+1=49, (28+49) mod 34 = 9 => С

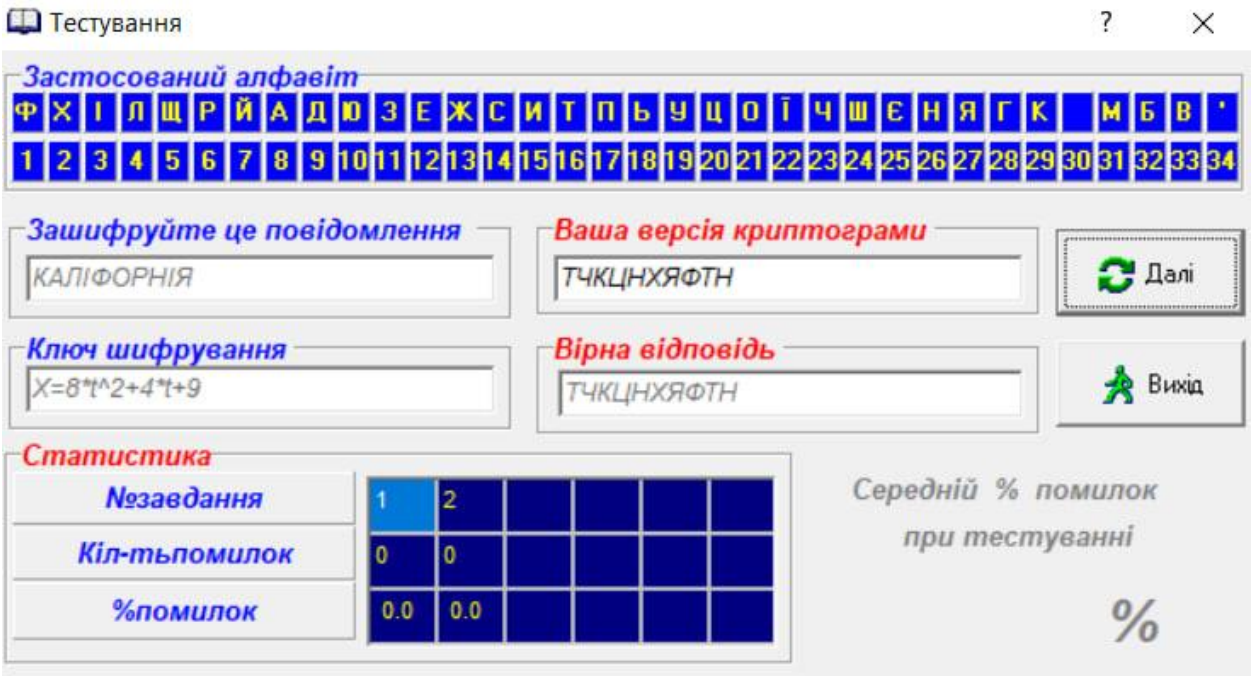
17) С = 9, 3*17+1=52, (9+52) mod 34 = 27 => Т

18) З = 24, 3*18+1=55, (24+55) mod 34 = 11 => Ь

19) Г = 4, 3*19+1=58, (4+58) mod 34 = 28 => ‘ ’

Нелінійний ключ:

Шифрування:



1) К = 29, 8*1^2+4*1+9=21, (29+21) mod 34 = 16 => Т

2) А = 8, 8*2^2+4*2+9=49, (8+49) mod 34 = 23 => Ч

3) Л = 4, 8*3^2+4*3+9=93, (4+93) mod 34 = 29 => К

4) І = 3, 8*4^2+4*4+9=153, (3+153) mod 34 = 20 => Ц

5) Ф = 1, 8*5^2+4*5+9=229, (1+229) mod 34 = 26 => Н

6) О =21, 8*6^2+4*6+9=321, (21+321) mod 34 = 2 => Х

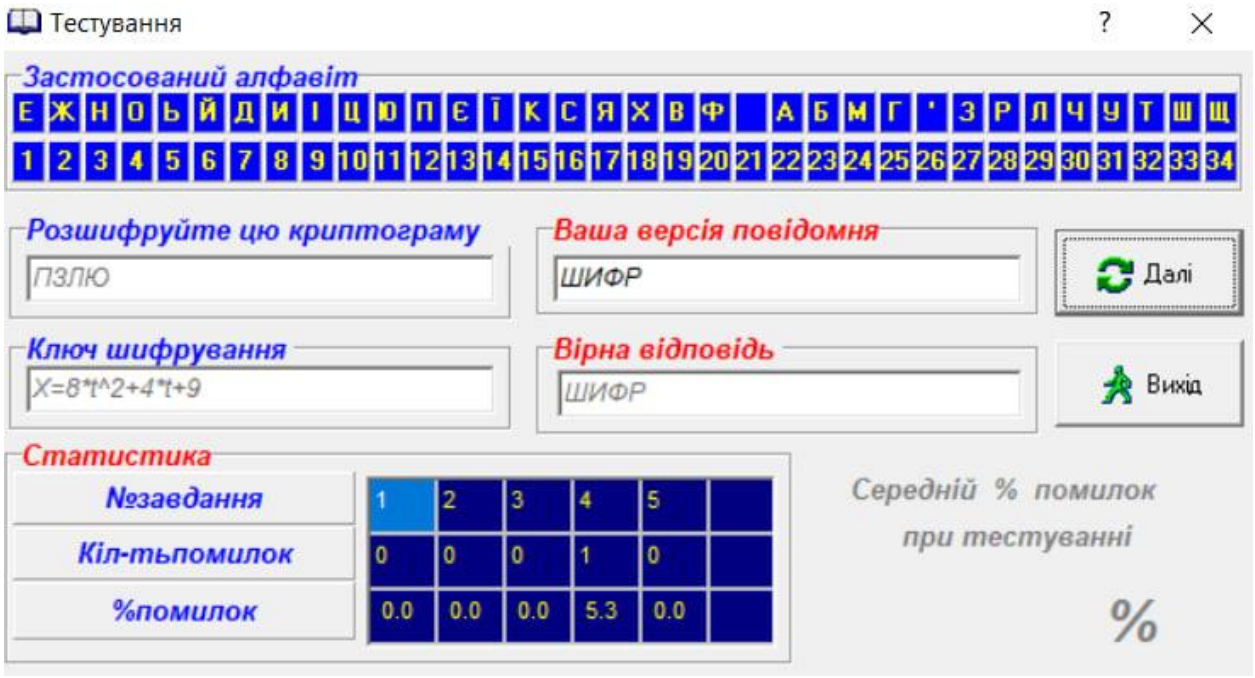
7) Р = 6, 8*7^2+4*7+9=429, (6+429) mod 34 = 27 => Я

8) Н = 26, 8*8^2+4*8+9=553, (26+553) mod 34 = 1 => Ф

9) І = 3, 8*9^2+4*9+9=693, (3+693) mod 34 = 16 => Т

10) Я = 27, 8*10^2+4*10+9=849, (27+849) mod 34 = 26 => Н

Дешифрування:



1) П = 12, 8*1^2+4*1+9=21, (12+21) mod 34 = 33 => Ш

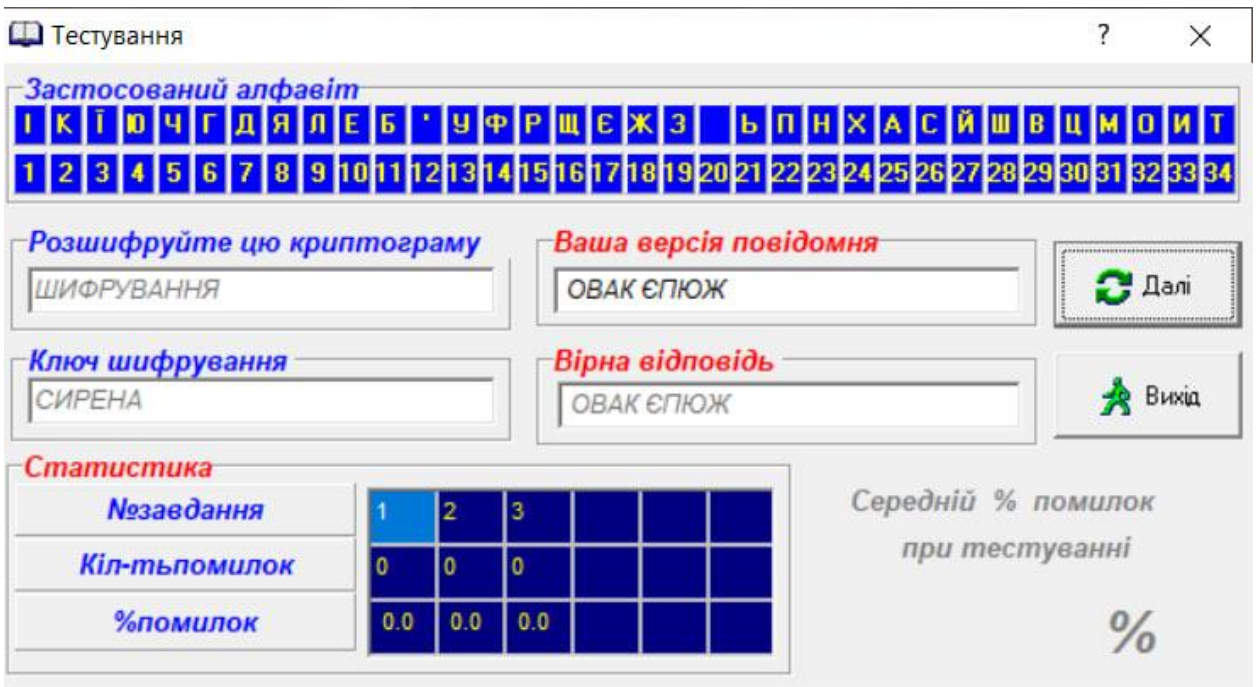
2) З = 27, 8*2^2+4*2+9=49, (27+49) mod 34 = 8 => И

3) Л = 29, 8*3^2+4*3+9=93, (29+93) mod 34 = 20 => Ф

4) Ю = 11, 8*4^2+4*4+9=153, (11+153) mod 34 = 28 => Р

Текстовий ключ:

Шифрування:



28	33	14	15	13	29	25	23	23	8

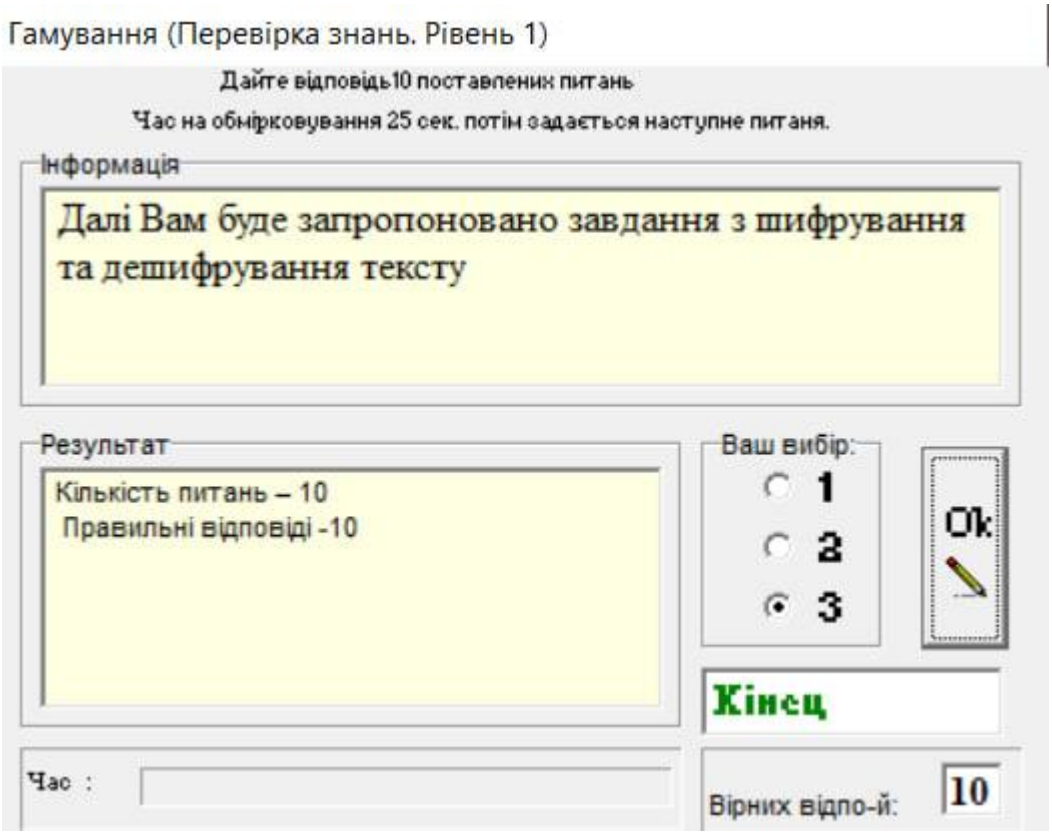
Ш	И	Ф	Р	У	В	А	Н	Н	Я
С	И	Р	Е	Н	А	С	И	Р	Е
26	33	15	10	23	25	26	33	15	10
20	32	29	25	2	20	17	22	4	18
‘ ’	О	В	А	К	‘ ’	Є	П	Ю	Ж

1) (28+26) mod 34 = 20
2) (33+33) mod 34 = 32
3) (14+15) mod 34 = 29
4) (15+10) mod 34 = 25
5) (13+23) mod 34 = 2
6) (25+29) mod 34 = 20
7) (25+26) mod 34 = 17
8) (23+33) mod 34 = 22
9) (23+15) mod 34 = 4
10) (8+10) mod 34 = 18

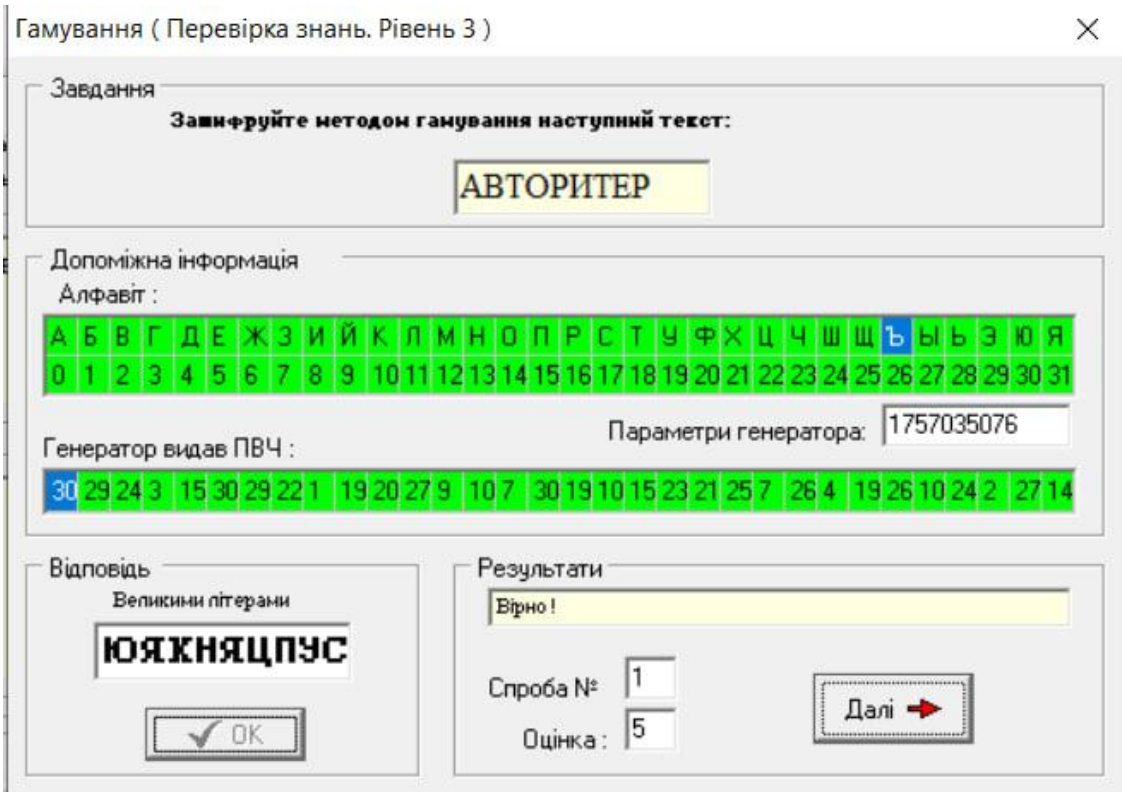
Дешифрування:

6	25	7	34	20	29	2	20	7	27	25	2	15
О	Й	І	П	К	Д	Х	К	І	В	Й	Х	Є
С	И	Р	Е	Н	А	С	И	Р	Е	Н	А	С
1	26	3	12	17	5	1	26	3	12	17	5	1
7	17	10	12	3	34	3	12	10	5	8	7	16
І	Н	Т	Е	Р	П	Р	Е	Т	А	Ц	І	Я

3. Шифр Гамування.



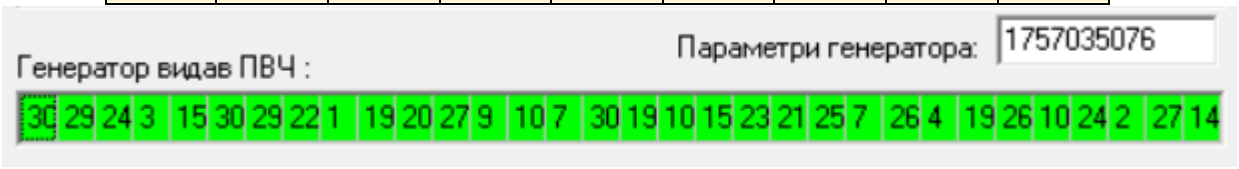
Шифрування:



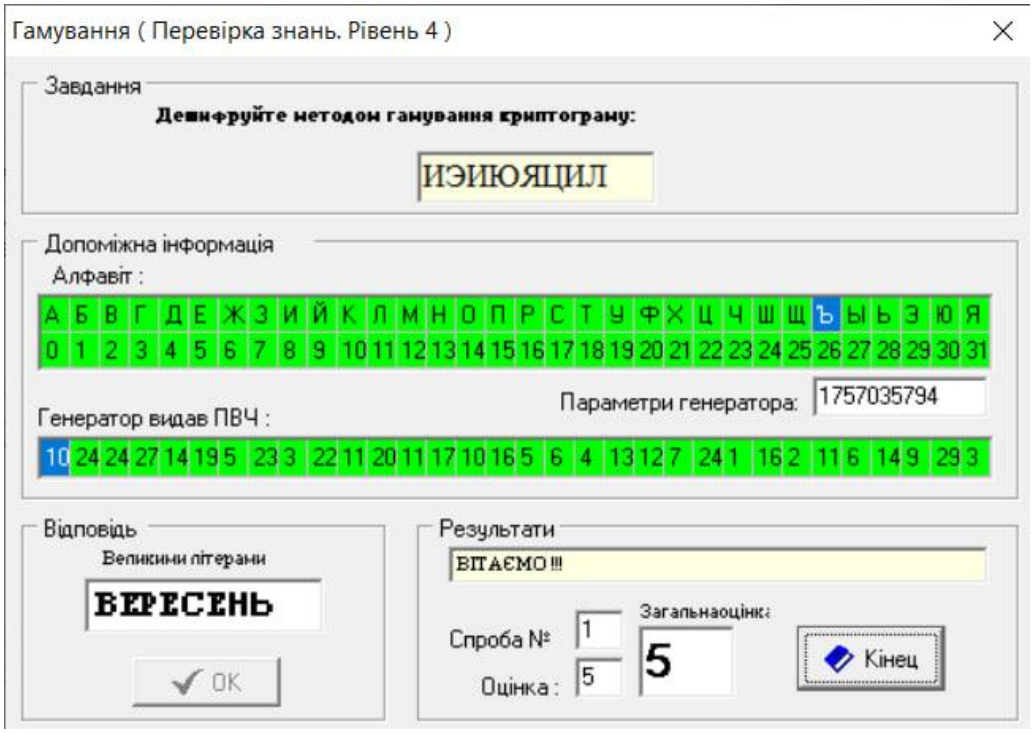
А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	З	Ю	Я

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

	А	В	Т	О	Р	И	Т	Е	Р
	0	2	18	14	16	8	18	5	16
+	30	29	24	3	15	30	29	22	1
	30	31	10	13	31	22	15	19	17
	Ю	Я	К	Н	Я	Ц	П	У	С



Дешифрування:



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	З	Ю	Я
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

	И	Є	И	Ю	Я	Ц	И	Л
	8	29	8	30	31	22	8	11
+	10	24	24	27	14	19	5	23
	2	5	16	5	17	5	13	28
	В	Е	Р	Е	С	Е	Н	Ь