



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

Лабораторна робота №1

з дисципліни «Безпека інформаційних систем»

Виконав:  
студент групи ІА-  
23:  
Лядський Д.С.

Перевірив:  
Шимкович Л.Л.

Київ 2024

### Хід роботи:

#### Шифр Цезаря

Шифрування зі зміщенням 3:

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

Ґ, ґ, д, е, є, ж, з, и, і, ї, й, к, л, м, н, о, п, р, с, т, у, ф, х, ц, ч, ш, щ, ъ, ю, я, а, б, в

"Це дуже цікаве дослідження шифру" = "Щз жціз щкнгдз жсокжізррв юйчуц"

"Програмування це дуже цікава справа" = "Тусеугпідгrrрв щз жціз щкнгдг  
фтугдг"

"Українська мова є однією з найбагатших у світі" = "Цнуглрфанг педг и сжркиб  
ї ргмгтегхюйш ц фдкхк"

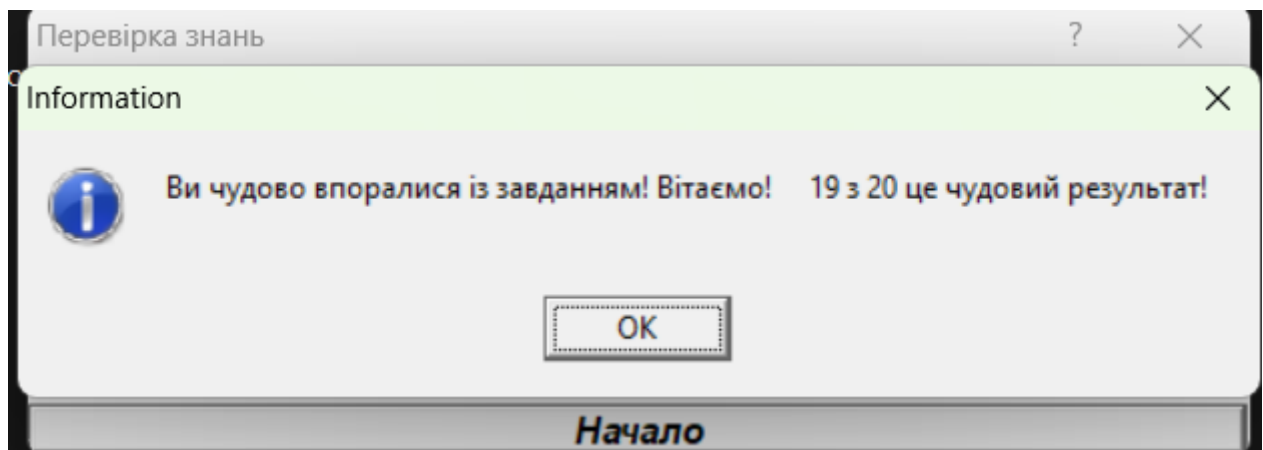
Дешифрування:

"Щз жціз щкнгдз жсокжізррв юйчуц" = "Це дуже цікаве дослідження шифру"

"Тусеугпідгrrрв щз жціз щкнгдг фтугдг" = "Програмування це дуже цікава  
справа"

"Цнуглрфанг педг и сжркиб ї ргмгтегхюйш ц фдкхк" = "Українська мова є  
однією з найбагатших у світі"

#### Шифр Тритеміуса



Тестування

**Застосований алфавіт**

Є	Е	З	Щ	Ч	Ь	І	Л	І	В	Г	Ю	Д	Я	Р	Н	О	Ц	П	Б	'	Ж	К	А	И	Й	М	С	Т	У	Ф	Х	Ш	
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	32	33	34

**Зашифруйте це повідомлення**

ШИФРУВАННЯ

**Ваша версія криптограми**

ЩХЛМДСДІВГ

**Ключ шифрування**

$x=3*t+1$

**Вірна відповідь**

ЩХЛМДСДІВГ

**Статистика**

Незавдання	1					
Кіл-ть помилок	0					
% помилок	0.0					

Середній % помилок при тестуванні

%

Далі

Вихід

$$\Pi = (34 + (3 * 1 + 1)) \bmod 34 = 4 = \Pi$$

$$\text{И} = (26 + (3 * 2 + 1)) \bmod 34 = 33 = \text{X}$$

$$\Phi = (32 + (3 * 3 + 1)) \bmod 34 = 8 = \text{Л}$$

Тестування

**Застосований алфавіт**

П	Л	Ш	Д	Р	Б	А	Ч	Й	М	Щ	С	Х	Т	Я	О	У	З	Ф	Н	К	Ц	Ь	Ю	І	И	В	Г	І	Ж	Е	Є	'	
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	32	33	34

**Розшифруйте цю криптограму**

СЕВАСТОПІЛЬ

**Ваша версія повідомня**

Ю ЄРЕКВВЖЙ

**Ключ шифрування**

СИРЕНА

**Вірна відповідь**

Ю ЄРЕКВВЖЙ

**Статистика**

Незавдання	1	2	3			
Кіл-ть помилок	0	0	0			
% помилок	0.0	0.0	0.0			

Середній % помилок при тестуванні

%

Далі

Вихід

$$\text{C} = \{\text{C}\} + \{\text{C}\} = 12 + 12 = 24 = \text{Ю}$$

$$\text{E} = \{\text{E}\} + \{\text{И}\} = 32 + 27 = 59 \bmod 34 = 25 =$$

$$\text{B} = \{\text{B}\} + \{\text{P}\} = 28 + 5 = 33 = \text{Є}$$

Тестування

Застосований алфавіт

У	Г	К	Л	Х	М	Ь	Ж	Т	Ч	Ф	І	Є	Д	Е	А	Н	Б	'	З	Ц	Ш	И	Щ	О	П	Й	Р	І	С	Я	Ю	В	
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	32	33	34

Розшифруйте цю криптограму

УЖЗФ

Ваша версія повідомня

ШИФР

Далі

Ключ шифрування

$X=8*t^2+4*t+9$

Вірна відповідь

ШИФР

Вихід

Статистика

Незавдання	1	2	3	4	5	
Кіл-ть помилок	0	0	0	8	0	
% помилок	0.0	0.0	0.0	100.0	0.0	

Середній % помилок при тестуванні

%

$$У=(1+(8*1^2+4*1+9))\bmod 34=22=Ш$$

$$Ж=(8+(8*2^2+4*2+9))\bmod 34=23=И$$

Тестування

Застосований алфавіт

'	С	Ш	А	Р	Ч	І	Т	Щ	Ь	І	Є	Ю	Е	М	Я	Й	И	Ф	П		Б	Ж	В	Г	К	У	Х	Ц	З	Д	Л	Н	О
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	32	33	34

Розшифруйте цю криптограму

ЮППФЕАЛЦФ

Ваша версія повідомня

МАГНІТОФОН

Пуск

Ключ шифрування

СИРЕНА

Вірна відповідь

МАГНІТОФОН

Вихід

Статистика

Незавдання	1	2	3	4	5	6
Кіл-ть помилок	0	0	0	8	0	0
% помилок	0.0	0.0	0.0	100.0	0.0	0.0

Середній % помилок при тестуванні

0.0 %

## Гамування (Перевірка знань. Рівень 1)

Дайте відповідь 10 поставлених питань

Час на обмірковування 25 сек. потім задається наступне питання.

### Інформація

Далі Вам буде запропоновано завдання з шифрування та дешифрування тексту

### Результат

Кількість питань – 10  
Правильні відповіді -10

### Ваш вибір:

☐ 1  
☐ 2  
☒ 3



Кінець

Час :

Вірних відпо-й:

10

## Гамування (Перевірка знань. Рівень 3)

### Завдання

Зашифруйте методом гамування наступний текст:

МИСТЕЦТВО

### Допоміжна інформація

Алфавіт :

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
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

Генератор видав ПВЧ :

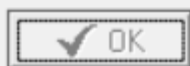
Параметри генератора: 1727742626

1	9	25	6	11	21	12	3	14	31	12	14	2	30	7	9	18	0	1	26	28	12	15	12	12	17	10	8	26	4	22	27
---	---	----	---	----	----	----	---	----	----	----	----	---	----	---	---	----	---	---	----	----	----	----	----	----	----	----	---	----	---	----	----

### Відповідь

Великими літерами

БМФОГЮБА



### Результати

Вірно !

Спроба №

1

Оцінка :

5

Далі →

$M = 12 = 1100$ ;  $1 = 0001$ ;  $1 \text{ xor } 0 = 1$ ;  $1 \text{ xor } 0 = 1$ ;  $0 \text{ xor } 0 = 0$ ;  $0 \text{ xor } 1 = 1$ ;  $1101 = 13 = H$

$I = 8 = 1000$ ;  $9 = 1001$ ;  $1 \text{ xor } 1 = 0$ ;  $0 \text{ xor } 0 = 0$ ;  $0 \text{ xor } 0 = 0$ ;  $0 \text{ xor } 1 = 1$ ;  $0001 = 1 = B$

Гамування ( Перевірка знань. Рівень 4 )

Завдання

Дешифруйте методом гамування криптограму:

ХЫЬСЕД

Допоміжна інформація

Алфавіт :

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
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

Генератор видав ПВЧ :

23 21 12 31 8 4 17 28 19 8 15 9 8 28 4 1 13 11 8 11 29 27 25 22 28 9 6 10 8 19 29 5

Параметри генератора:

1727743145

Відповідь

Великими літерами

ВОРОНА

OK

Результати

ВІТАЄМО !!!

Спроба №

1

Оцінка :

5

Загальна оцінка:

5

Кінець

**Висновок:** Отже, на цій лабораторній роботі ми розглянули Шифр Цезаря, Шифр Тритеміуса, Шифр Гамування та використали їх на практиці.