



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.

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 => Ї

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:

Тестування

?

×

Застосований алфавіт

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

БРАЗИЛІЯ

Ваша версія криптограми

КГВ ДЮНН

Далі

Ключ шифрування

$x=3*t+1$

Вірна відповідь

КГВ ДЮНН

Вихід

Статистика

Незавдання	1								
Кіл-ть помилок	0								
% помилок	0.0								

Середній % помилок при тестуванні

%

- 1) Б = 5, $3*1+1=4$, $(5+4) \bmod 34 = 9 \Rightarrow К$
- 2) Р = 16, $3*2+1=7$, $(16+7) \bmod 34 = 23 \Rightarrow Г$
- 3) А = 1, $3*3+1=10$, $(1+10) \bmod 34 = 11 \Rightarrow В$
- 4) З = 21, $3*4+1=13$, $(21+13) \bmod 34 = 34 \Rightarrow ' '$
- 5) И = 26, $3*5+1=16$, $(26+16) \bmod 34 = 8 \Rightarrow Д$

$$6) Л = 13, 3 \cdot 6 + 1 = 19, (13 + 19) \bmod 34 = 32 \Rightarrow Ю$$

$$7) І = 2, 3 \cdot 7 + 1 = 22, (2 + 22) \bmod 34 = 24 \Rightarrow Н$$

$$8) Я = 33, 3 \cdot 8 + 1 = 25, (33 + 25) \bmod 34 = 24 \Rightarrow Н$$

Дешифрування:

Тестування

Застосований алфавіт

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

Ч У В Ї И І Ю П В Х К Ч Ї С З Г

Ваша версія повідомня

ЕЛЕКТРОПРОВІДНІСТЬ

Ключ шифрування

$x = 3 \cdot t + 1$

Вірна відповідь

ЕЛЕКТРОПРОВІДНІСТЬ

Статистика

Незавершення	1	2	3	4		
Кількість помилок	0	0	0	1		
% помилок	0.0	0.0	0.0	5.3		

Середній % помилок при тестуванні

%

Далі

Вихід

$$1) Ч = 3, 3 \cdot 1 + 1 = 4, (3 + 4) \bmod 34 = 7 \Rightarrow Е$$

$$2) ' = 28, 3 \cdot 2 + 1 = 7, (28 + 7) \bmod 34 = 1 \Rightarrow Л$$

$$3) У = 31, 3 \cdot 3 + 1 = 10, (31 + 10) \bmod 34 = 7 \Rightarrow Е$$

$$4) В = 21, 3 \cdot 4 + 1 = 13, (21 + 13) \bmod 34 = 34 \Rightarrow К$$

$$5) Ь = 11, 3 \cdot 5 + 1 = 16, (11 + 16) \bmod 34 = 27 \Rightarrow Т$$

$$6) ' = 28, 3 \cdot 6 + 1 = 19, (28 + 19) \bmod 34 = 13 \Rightarrow Р$$

$$7) И = 26, 3 \cdot 7 + 1 = 22, (26 + 22) \bmod 34 = 14 \Rightarrow О$$

$$8) И = 26, 3 \cdot 8 + 1 = 25, (26 + 25) \bmod 34 = 17 \Rightarrow П$$

$$9) Ю = 19, 3 \cdot 9 + 1 = 28, (19 + 28) \bmod 34 = 13 \Rightarrow Р$$

$$10) П = 17, 3 \cdot 10 + 1 = 31, (17 + 31) \bmod 34 = 14 \Rightarrow О$$

$$11) В = 21, 3 \cdot 11 + 1 = 34, (21 + 34) \bmod 34 = 21 \Rightarrow В$$

$$12) Х = 20, 3 \cdot 12 + 1 = 37, (20 + 37) \bmod 34 = 23 \Rightarrow І$$

$$13) К = 34, 3 \cdot 13 + 1 = 40, (34 + 40) \bmod 34 = 6 \Rightarrow Д$$

$$14) Ч = 3, 3 \cdot 14 + 1 = 43, (3 + 43) \bmod 34 = 12 \Rightarrow Н$$

$$15) Ь = 11, 3 \cdot 15 + 1 = 46, (11 + 46) \bmod 34 = 23 \Rightarrow І$$

- 16) ' ' = 28, $3 \cdot 16 + 1 = 49$, $(28 + 49) \bmod 34 = 9 \Rightarrow C$
 17) $C = 9$, $3 \cdot 17 + 1 = 52$, $(9 + 52) \bmod 34 = 27 \Rightarrow T$
 18) $3 = 24$, $3 \cdot 18 + 1 = 55$, $(24 + 55) \bmod 34 = 11 \Rightarrow Б$
 19) $Г = 4$, $3 \cdot 19 + 1 = 58$, $(4 + 58) \bmod 34 = 28 \Rightarrow ' '$

Нелінійний ключ:

Шифрування:

Тестування

Застосований алфавіт

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

Зашифруйте це повідомлення

КАЛІФОРНІЯ

Ваша версія криптограми

ТЧКЦНХЯФТН

Ключ шифрування

$X = 8 \cdot t^2 + 4 \cdot t + 9$

Вірна відповідь

ТЧКЦНХЯФТН

Статистика

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

Середній % помилок при тестуванні

%

Далі

Вихід

- 1) $K = 29$, $8 \cdot 1^2 + 4 \cdot 1 + 9 = 21$, $(29 + 21) \bmod 34 = 16 \Rightarrow T$
 2) $A = 8$, $8 \cdot 2^2 + 4 \cdot 2 + 9 = 49$, $(8 + 49) \bmod 34 = 23 \Rightarrow Ч$
 3) $Л = 4$, $8 \cdot 3^2 + 4 \cdot 3 + 9 = 93$, $(4 + 93) \bmod 34 = 29 \Rightarrow К$
 4) $I = 3$, $8 \cdot 4^2 + 4 \cdot 4 + 9 = 153$, $(3 + 153) \bmod 34 = 20 \Rightarrow Ц$
 5) $\Phi = 1$, $8 \cdot 5^2 + 4 \cdot 5 + 9 = 229$, $(1 + 229) \bmod 34 = 26 \Rightarrow Н$
 6) $O = 21$, $8 \cdot 6^2 + 4 \cdot 6 + 9 = 321$, $(21 + 321) \bmod 34 = 2 \Rightarrow Х$
 7) $P = 6$, $8 \cdot 7^2 + 4 \cdot 7 + 9 = 429$, $(6 + 429) \bmod 34 = 27 \Rightarrow Я$
 8) $H = 26$, $8 \cdot 8^2 + 4 \cdot 8 + 9 = 553$, $(26 + 553) \bmod 34 = 1 \Rightarrow \Phi$
 9) $I = 3$, $8 \cdot 9^2 + 4 \cdot 9 + 9 = 693$, $(3 + 693) \bmod 34 = 16 \Rightarrow T$
 10) $Я = 27$, $8 \cdot 10^2 + 4 \cdot 10 + 9 = 849$, $(27 + 849) \bmod 34 = 26 \Rightarrow Н$

Дешифрування:

Тестування

Застосований алфавіт

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

ПЗЛЮ

Ключ шифрування

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

Ваша версія повідомня

ШИФР

Вірна відповідь

ШИФР

Статистика

Незавдання	1	2	3	4	5	
Кіл-ть помилок	0	0	0	1	0	
% помилок	0.0	0.0	0.0	5.3	0.0	

Середній % помилок при тестуванні

%

Далі

Вихід

- 1) $P = 12, 8*1^2+4*1+9=21, (12+21) \bmod 34 = 33 \Rightarrow Ш$
- 2) $З = 27, 8*2^2+4*2+9=49, (27+49) \bmod 34 = 8 \Rightarrow И$
- 3) $Л = 29, 8*3^2+4*3+9=93, (29+93) \bmod 34 = 20 \Rightarrow Ф$
- 4) $Ю = 11, 8*4^2+4*4+9=153, (11+153) \bmod 34 = 28 \Rightarrow Р$

Текстовий ключ:

Шифрування:

Тестування

Застосований алфавіт

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

ШИФРУВАННЯ

Ключ шифрування

СИРЕНА

Ваша версія повідомня

ОВАК ЄПЮЖ

Вірна відповідь

ОВАК ЄПЮЖ

Статистика

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

Середній % помилок при тестуванні

%

Далі

Вихід

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

Дешифрування:

Тестування

?

×

Застосований алфавіт

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

ОЙГПҚДХКІВЙХЄ

Ваша версія повідомня

ІНТЕРПРЕТАЦІЯ

Ключ шифрування

СИРЕНА

Вірна відповідь

ІНТЕРПРЕТАЦІЯ

Статистика

Незавдання

Кіл-ть помилок

% помилок

1	2	3	4	5	6
0	0	0	1	0	0
0.0	0.0	0.0	5.3	0.0	0.0

Середній % помилок при тестуванні

-0.0 %

Пуск

Вихід

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.

Гамування (Перевірка знань. Рівень 1)

Дайте відповідь 10 поставленим питанням
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

Ok

Кінець

Час :

Вірних відпо-й: **10**

Шифрування:

Гамування (Перевірка знань. Рівень 3)

Завдання

Зашифруйте методом гамування наступний текст:

АВТОРИТЕР

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 : **30 29 24 3 15 30 29 22 1 19 20 27 9 10 7 30 19 10 15 23 21 25 7 26 4 19 26 10 24 2 27 14**

Параметри генератора: 1757035076

Відповідь

Великими літерами

ЮЯКНЯЦПЭС

OK

Результати

Вірно !

Спроба № **1**

Оцінка : **5**

Далі →

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
---	---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

	A	B	T	O	P	И	T	E	P
+	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

Генератор видав ПВЧ :

Параметри генератора: 1757035076

30 29 24 3 15 30 29 22 1 19 20 27 9 10 7 30 19 10 15 23 21 25 7 26 4 19 26 10 24 2 27 14

Дешифрування:

Гамування (Перевірка знань. Рівень 4)

Завдання

Дешифруйте методом гамування криптограму:

ИЭИЮЯЦИЛ

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: 1757035794

10 24 24 27 14 19 5 23 3 22 11 20 11 17 10 16 5 6 4 13 12 7 24 1 16 2 11 6 14 9 29 3

Відповідь

Великими літерами

БЕРЕСЕНЬ

OK

Результати

ВІТАЄМО !!!

Спроба № 1
Оцінка : 5

Загальна оцінка: 5
Кінець

A	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

	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