

Тесты для лабораторной работы 3
Вариант 2

Буховец Илиан 351002

1) Шифрование картинки

Тест 1.1(шифровка)
Свойства исходного файла:

Свойства: Crazy_Frog.jpg

Безопасность

Общие

Подробно

Цифровые подписи

Предыдущие версии

Crazy_Frog.jpg

Тип файла: Файл "JPG" (.jpg)

Приложение: Фотографии

Изменить...

Расположение: C:\BSUIR\ТИ\ТИ_2025\I3\I3\Tests\image

Размер: 91,7 КБ (93 939 байт)

На диске: 92,0 КБ (94 208 байт)

Создан: вторник, 22 апреля 2025 г., 17:47:03

Изменен: суббота, 22 марта 2025 г., 16:15:34

Открыт: Сегодня, 22 апреля 2025 г., 1 минуту назад

Атрибуты: ☐ Только чтение ☐ Скрытый

ОК

Отмена

Применить

Crazy_Frog.jpg

00000000	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00000000	ff	d8	ff	e0	00	10	4a	46	49	46	00	01	01	01	00	60
00000010	00	60	00	00	ff	fe	00	3b	43	52	45	41	54	4f	52	3a
00000020	20	67	64	2d	6a	70	65	67	20	76	31	2e	30	20	28	75
00000030	73	69	6e	67	20	49	4a	47	20	4a	50	45	47	20	76	38
00016ec0	34	8f	68	65	8a	30	a8	aa	98	03	04	9c	92	4f	6a	ef
00016ed0	c1	e0	71	14	b1	2e	bd	79	a9	4a	ca	2a	ca	ca	c9	b7
00016ee0	dd	ea	ce	7a	d5	e9	ca	92	a7	4e	36	57	be	ae	fa	fd
00016ef0	c8	ff	d9

Результат программы:

ElGamal File Encryptor

ElGamal File Encryption

Encryption Parameters

Prime (p): 257

Private Key (x): 99

Random k: 255

Calculate Public Keys

Public Key (p, g, y): {"P":257,"G":254,"Y":149}

254

File Operations

Input File: C:\BSUIR\ТИ\ТИ_2025\I3\I3\Tests\image\Crazy_Frog.jpg

Output File: C:\BSUIR\ТИ\ТИ_2025\I3\I3\Tests\image\encrCrazyFrog.jpg

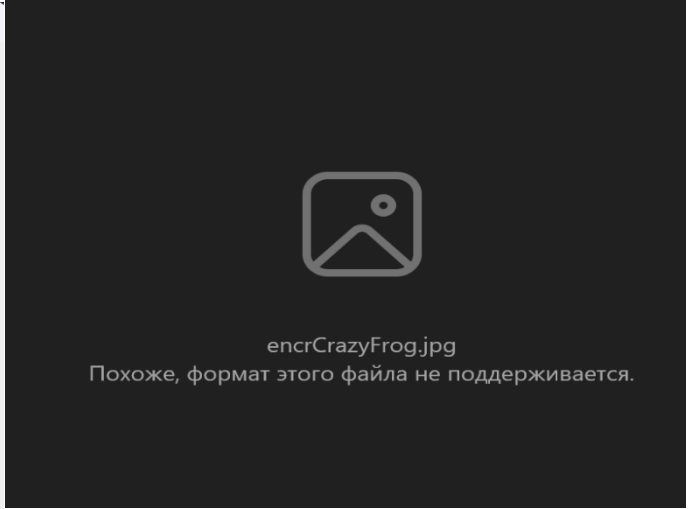
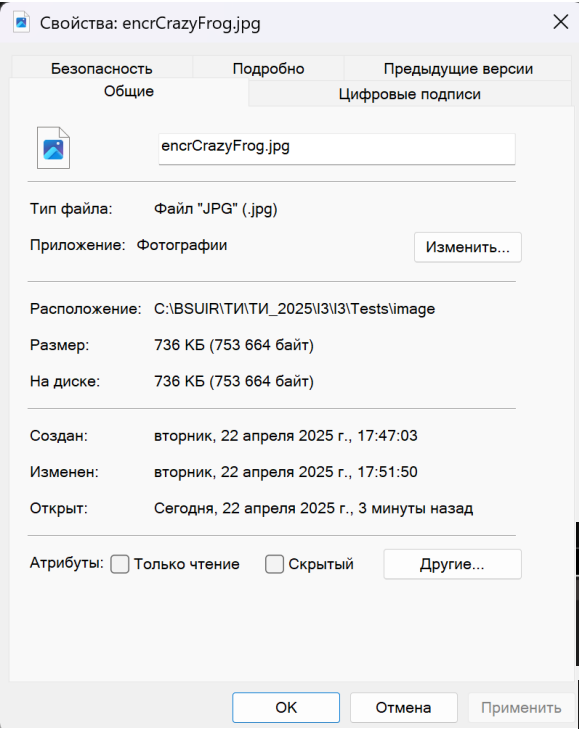
Encrypt Decrypt

Input File: 255,216,255,224,000...174,250,253,200,255,217

Output File: {171,119},{171,255},{171,119},{171,36},{171,0},{171,76}...{171,233},{171,94},{171,119}

Ready

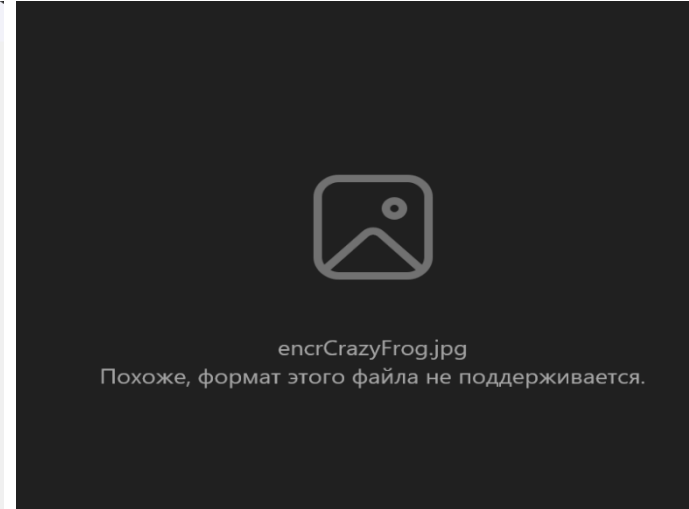
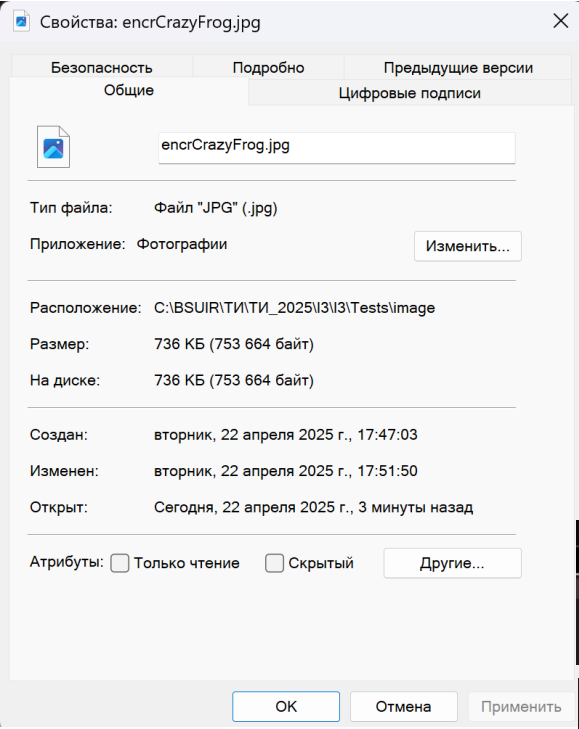
Свойства сохраненного зашифрованного файла



	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00000000	ab	00	00	00	77	00	00	00	ab	00	00	00	ff	00	00	00
00000010	ab	00	00	00	77	00	00	00	ab	00	00	00	24	00	00	00
00000020	ab	00	00	00	00	00	00	00	ab	00	00	00	4c	00	00	00
00000030	ab	00	00	00	df	00	00	00	ab	00	00	00	cc	00	00	00
000b7fc0	ab	00	00	00	92	00	00	00	ab	00	00	00	5e	00	00	00
000b7fd0	ab	00	00	00	e9	00	00	00	ab	00	00	00	5e	00	00	00
000b7fe0	ab	00	00	00	66	00	00	00	ab	00	00	00	f6	00	00	00
000b7ff0	ab	00	00	00	6b	00	00	00	ab	00	00	00	be	00	00	00

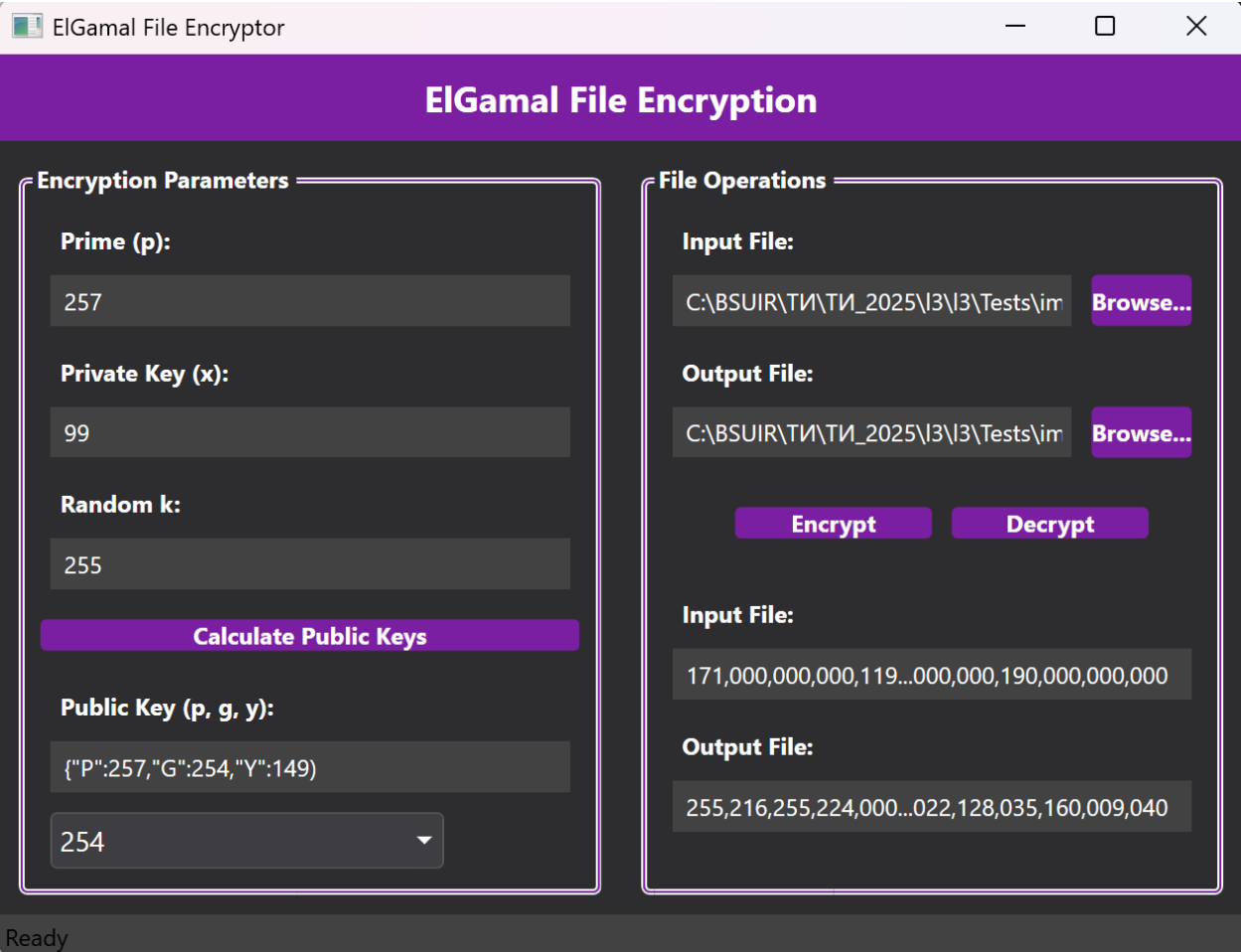
Тест 1.2(расшифровка)

Свойства зашифрованного файла:

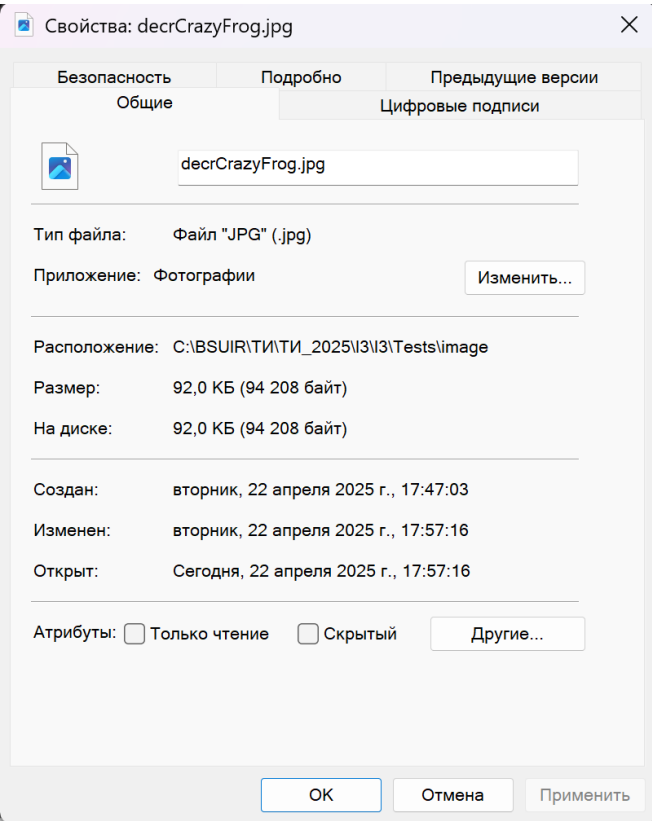


	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00000000	ab	00	00	00	77	00	00	00	ab	00	00	00	ff	00	00	00
00000010	ab	00	00	00	77	00	00	00	ab	00	00	00	24	00	00	00
00000020	ab	00	00	00	00	00	00	00	ab	00	00	00	4c	00	00	00
00000030	ab	00	00	00	df	00	00	00	ab	00	00	00	cc	00	00	00
000b7fc0	ab	00	00	00	92	00	00	00	ab	00	00	00	5e	00	00	00
000b7fd0	ab	00	00	00	e9	00	00	00	ab	00	00	00	5e	00	00	00
000b7fe0	ab	00	00	00	66	00	00	00	ab	00	00	00	f6	00	00	00
000b7ff0	ab	00	00	00	6b	00	00	00	ab	00	00	00	be	00	00	00

Результат программы:



Свойства сохраненного расшифрованного файла:

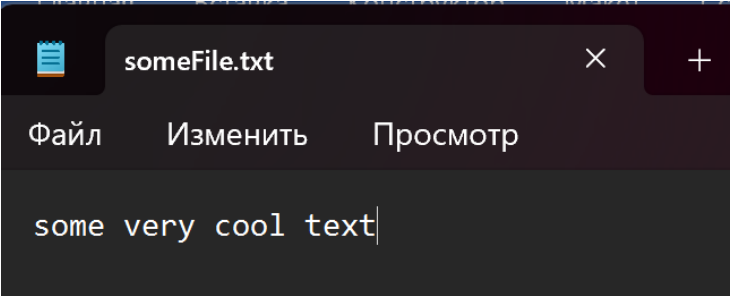
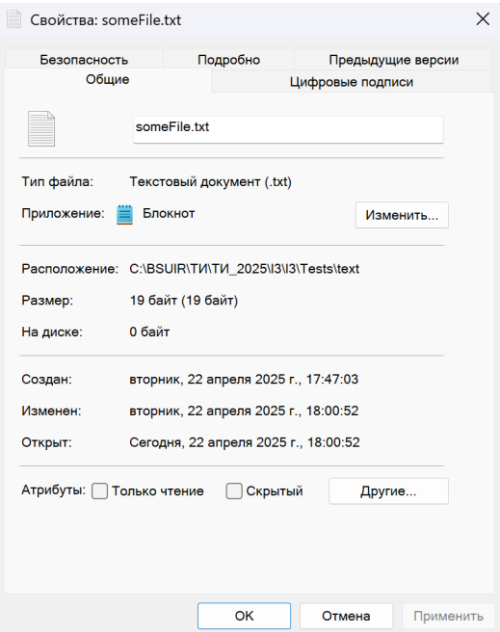


	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00000000	ff	d8	ff	e0	00	10	4a	46	49	46	00	01	01	01	00	60
00000010	00	60	00	00	ff	fe	00	3b	43	52	45	41	54	4f	52	3a
00000020	20	67	64	2d	6a	70	65	67	20	76	31	2e	30	20	28	75
00000030	73	69	6e	67	20	49	4a	47	20	4a	50	45	47	20	76	38
00000040	30	29	2c	20	71	75	61	6c	69	74	79	20	3d	20	39	35
00000050	0a	ff	db	00	43	00	02	01	01	01	01	01	02	01	01	01
00016fb0	f2	ff	00	79	40	07	97	ef	40	0c	d8	3d	4d	00	3f	cb
00016fc0	f7	a0	06	6c	1e	a6	80	0f	2f	f7	94	01	66	80	0a	00
00016fd0	28	00	a0	09	28	00	a0	08	e8	01	fb	07	a9	a0	06	50
00016fe0	04	94	01	1d	00	49	40	11	d0	01	40	12	50	01	40	11
00016ff0	d0	01	40	12	50	02	6c	1e	a6	80	16	80	23	a0	09	28

2) Шифрование текстового файла

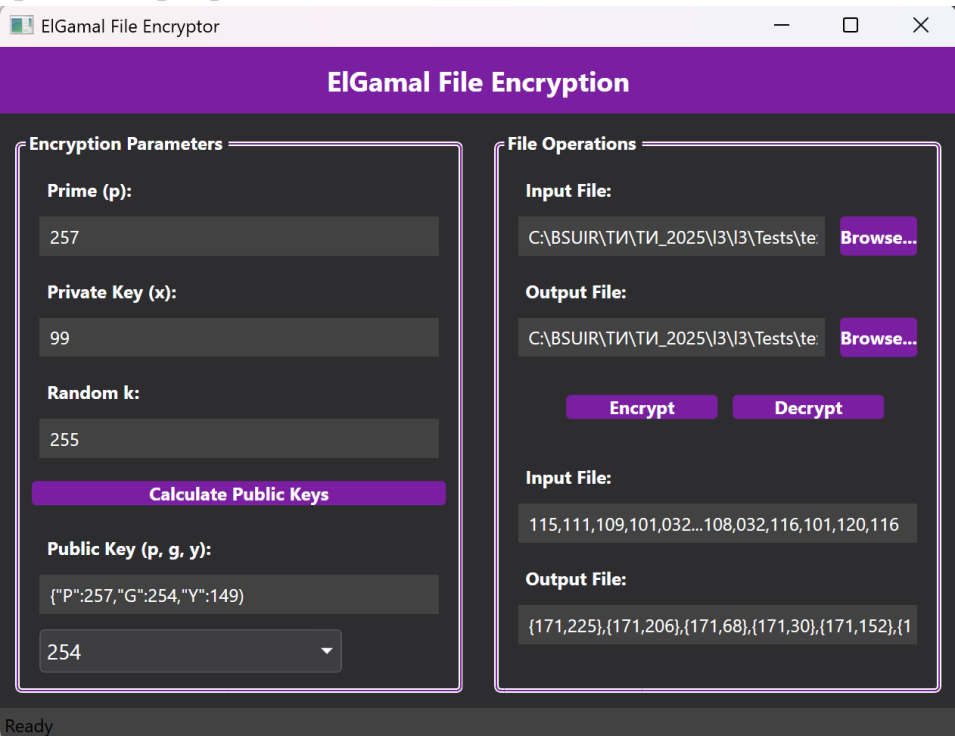
Тест 2.1(шифровка)

Свойства исходного файла:

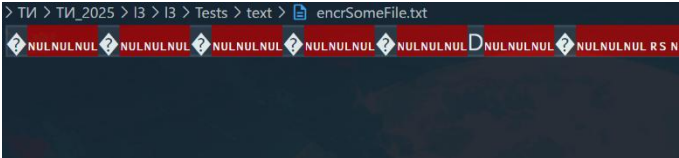
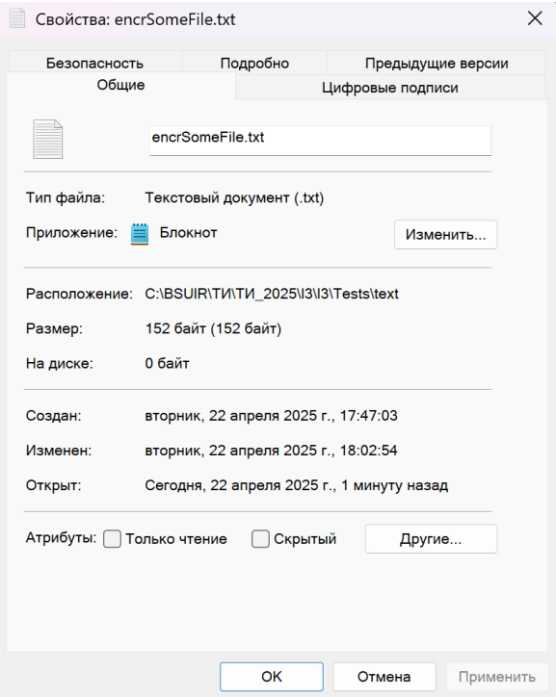


00000000	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f	
00000000	73	6f	6d	65	20	76	65	72	79	20	63	6f	6f	6c	20	74	some very cool t
00000010	65	78	74	ext

Результат работы программы:



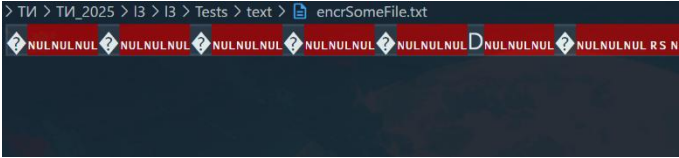
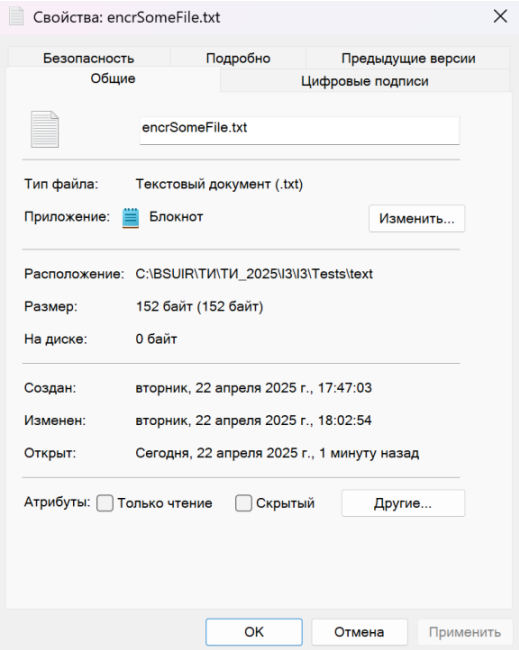
Свойства сохраненного зашифрованного файла:



00000000	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f	
00000000	ab	00	00	00	e1	00	00	00	ab	00	00	00	ce	00	00	00	«...6...«...O...
00000010	ab	00	00	00	44	00	00	00	ab	00	00	00	1e	00	00	00	«...D...«.....
00000020	ab	00	00	00	98	00	00	00	ab	00	00	00	af	00	00	00	«.....«...ï...
00000030	ab	00	00	00	1e	00	00	00	ab	00	00	00	9c	00	00	00	«.....«...Ъ...
00000040	ab	00	00	00	7d	00	00	00	ab	00	00	00	98	00	00	00	«...}...«.....
00000050	ab	00	00	00	95	00	00	00	ab	00	00	00	ce	00	00	00	«...•...«...O...
00000060	ab	00	00	00	ce	00	00	00	ab	00	00	00	00	01	00	00	«...O...«.....
00000070	ab	00	00	00	98	00	00	00	ab	00	00	00	25	00	00	00	«.....«...%...
00000080	ab	00	00	00	1e	00	00	00	ab	00	00	00	38	00	00	00	«.....«...8...
00000090	ab	00	00	00	25	00	00	00	«...%...

Тест 2.2(расшифровка)

Свойства зашифрованного файла:



someFile.txt	encrSomeFile.txt															
00000000	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00000000	ab	00	00	00	e1	00	00	00	ab	00	00	00	ce	00	00	00
00000010	ab	00	00	00	44	00	00	00	ab	00	00	00	1e	00	00	00
00000020	ab	00	00	00	98	00	00	00	ab	00	00	00	af	00	00	00
00000030	ab	00	00	00	1e	00	00	00	ab	00	00	00	9c	00	00	00
00000040	ab	00	00	00	7d	00	00	00	ab	00	00	00	98	00	00	00
00000050	ab	00	00	00	95	00	00	00	ab	00	00	00	ce	00	00	00
00000060	ab	00	00	00	ce	00	00	00	ab	00	00	00	00	01	00	00
00000070	ab	00	00	00	98	00	00	00	ab	00	00	00	25	00	00	00
00000080	ab	00	00	00	1e	00	00	00	ab	00	00	00	38	00	00	00
00000090	ab	00	00	00	25	00	00	00

Результат работы программы:

ElGamal File Encryptor

ElGamal File Encryption

Encryption Parameters

Prime (p):

257

Private Key (x):

99

Random k:

255

Calculate Public Keys

Public Key (p, g, y):

{"P":257,"G":254,"Y":149}

254

File Operations

Input File:

C:\BSUIR\ТИ\ТИ_2025\3\3\Tests\te

Browse...

Output File:

C:\BSUIR\ТИ\ТИ_2025\3\3\Tests\te

Browse...

Encrypt

Decrypt

Input File:

171,000,000,000,225...000,000,037,000,000,000

Output File:

115,111,109,101,032...108,032,116,101,120,116

Ready

Свойства сохраненного расшифрованного файла:

Свойства: decrSomeFile.txt

Безопасность

Общие

Подробно

Предыдущие версии

Цифровые подписи

decrSomeFile.txt

Тип файла:

Текстовый документ (.txt)

Приложение:

Блокнот

Изменить...

Расположение:

C:\BSUIR\ТИ\ТИ_2025\I3\I3\Tests\text

Размер:

19 байт (19 байт)

На диске:

0 байт

Создан:

вторник, 22 апреля 2025 г., 17:47:03

Изменен:

вторник, 22 апреля 2025 г., 18:06:47

Открыт:

Сегодня, 22 апреля 2025 г., 1 минуту назад

Атрибуты:

☐ Только чтение

☐ Скрытый

Другие...

OK

Отмена

Применить

decrSomeFile.txt

Файл

Изменить

Просмотр

some very cool text

someFile.txt	encrSomeFile.txt	decrSomeFile.txt
00000000	00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f	
00000000	73 6f 6d 65 20 76 65 72 79 20 63 6f 6f 6c 20 74	some very cool t
00000010	65 78 74	ext