**Министерство образования Республики Беларусь**

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей

Кафедра программного обеспечения информационных технологий

**ОТЧЕТ**

по лабораторной работе

на тему:

КРИПТОАНАЛИЗ МЕТОДОВ ПРОСТОЙ ПОДСТАНОВКИ

Выполнил

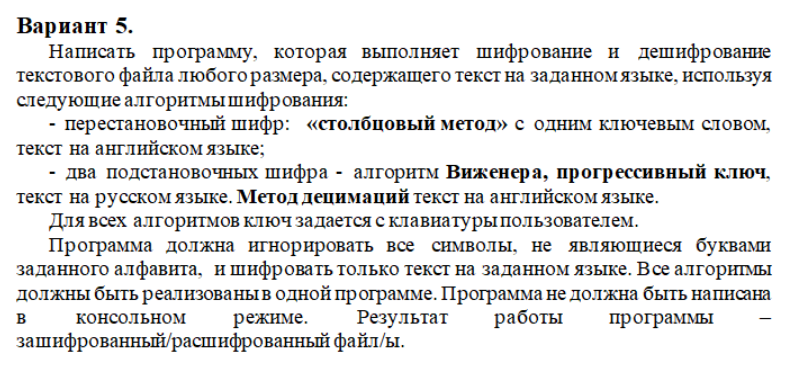
Студент гр. 051007 **Н. А. Захаренко**

Проверил **Асс. C.В. Болтак**

Минск, 2022

# 1. Задание

**1.1 Постановка задачи**



# 

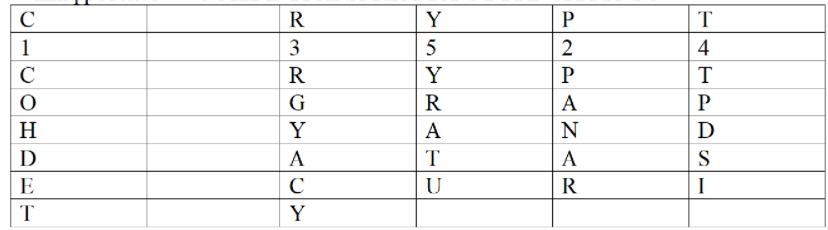
# 1.2 Тесты и скриншоты

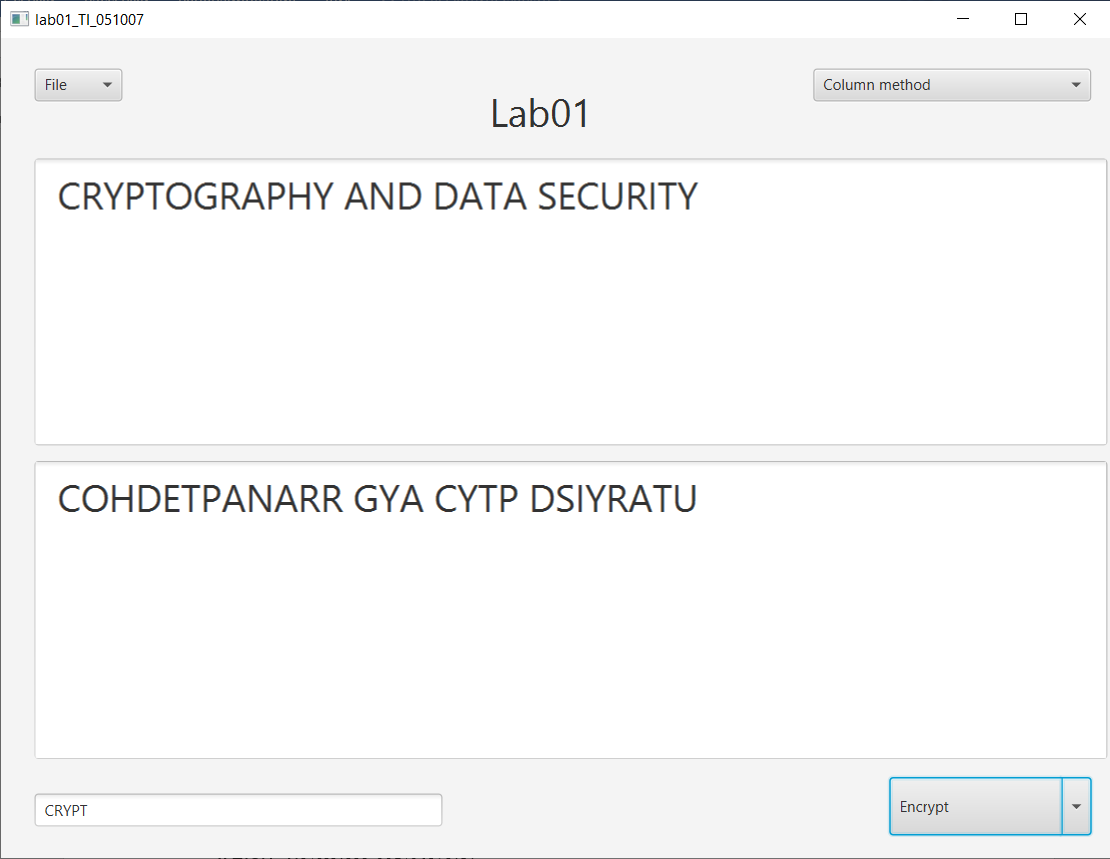
# Столбцовый метод:

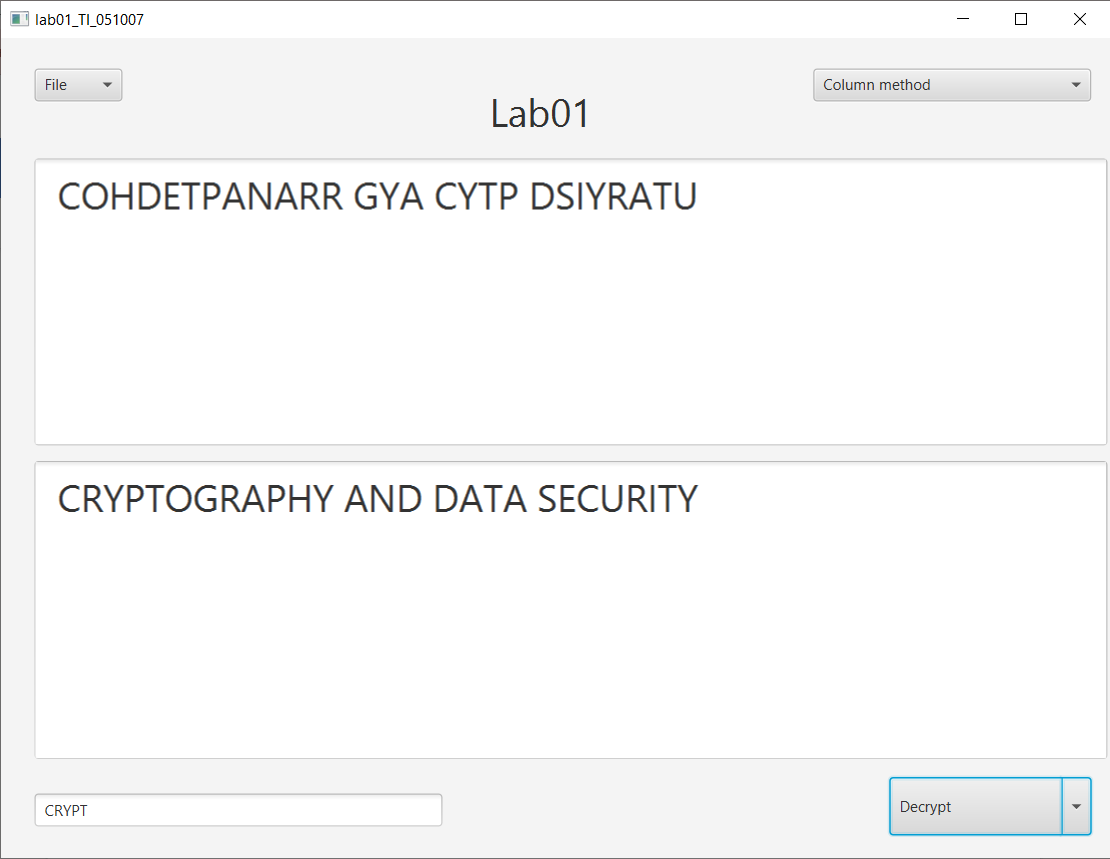
# Входная строка: CRYPTOGRAPHY AND DATA SECURITY

# Ключ: CRYPT

# Результат: COHDETPANARR GYA CYTP DSIYRATU







# Входная строка: TEXT

# Ключ: SUPERLONGKEY

# Результат: TXTE

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| S | U | P | E | R | L | O | N | G | K | E | Y |
| 10 | 11 | 8 | 1 | 9 | 5 | 7 | 6 | 3 | 4 | 2 | 12 |
| T | E | X | T |  |  |  |  |  |  |  |  |
| Результат: TXTE | | | | | | | | | | | |

# Входная строка: YES

# Ключ: A

# Результат: YES

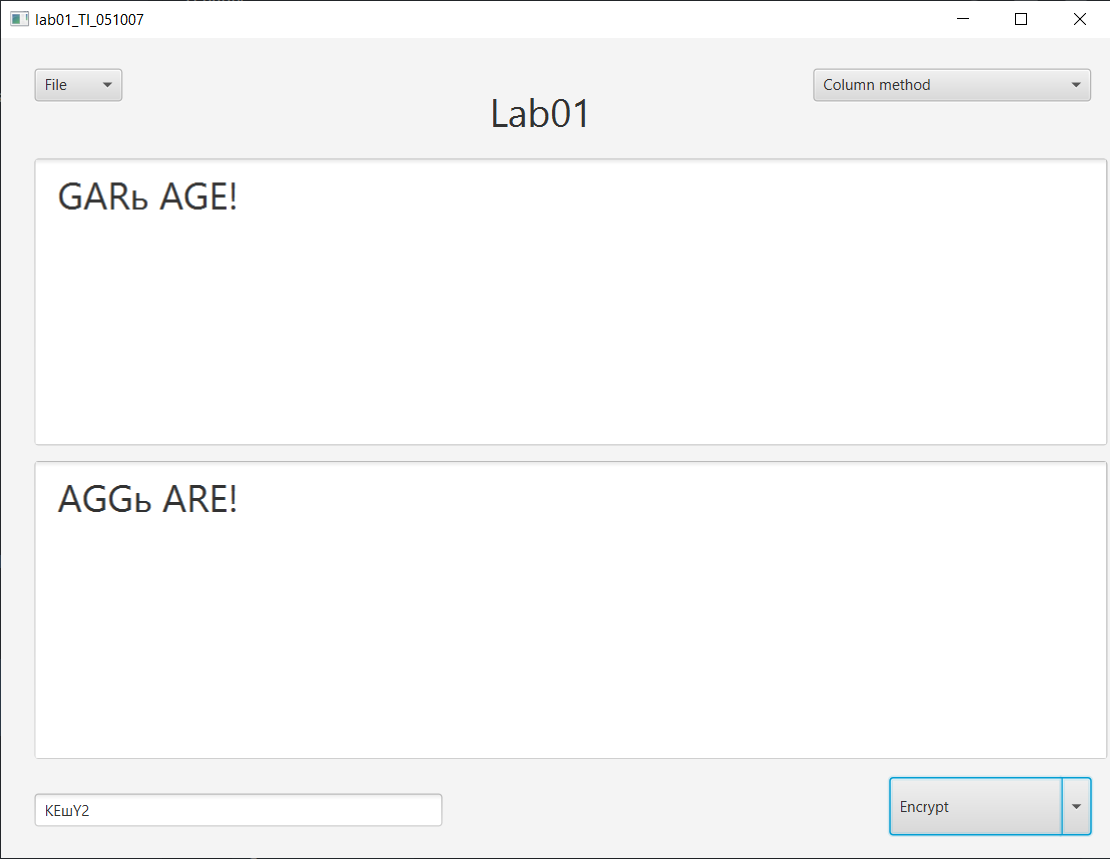
|  |
| --- |
| A |
| 1 |
| Y |
| E |
| S |
| Результат: YES |

# Входная строка: GARь AGE!

# Ключ: KEшY2

# Результат: AGGь ARE!

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| K | E | Ш | Y | 2 |
| 2 | 1 | - | 3 | - |
| G | A | - | R | - |
| A | G | - | E | - |
| Результат: AGGь ARE! | | | | |



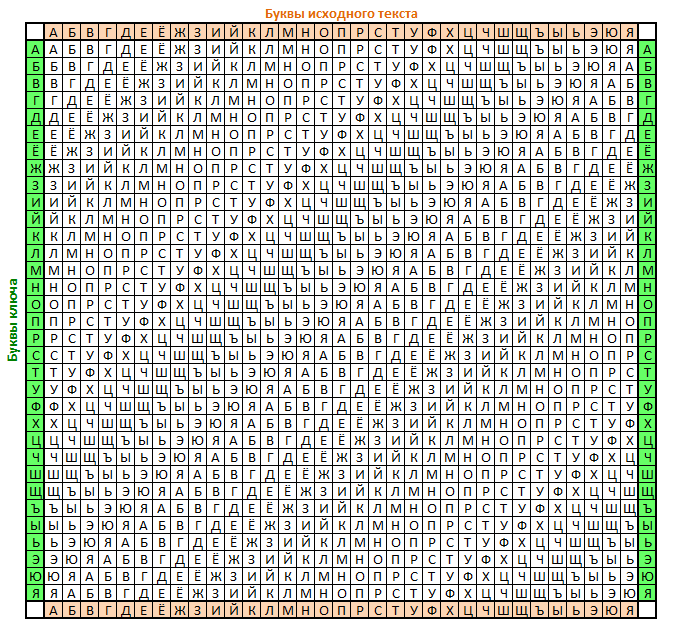
# Входная строка: abcde

# Ключ: edcba

**Результат:** edcba

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **e** | **d** | **c** | **b** | **a** |
| **5** | **4** | **3** | **2** | **1** |
| **a** | **b** | **c** | **d** | **e** |

**Метод Виженера:**



# Входная строка: Исходный текст

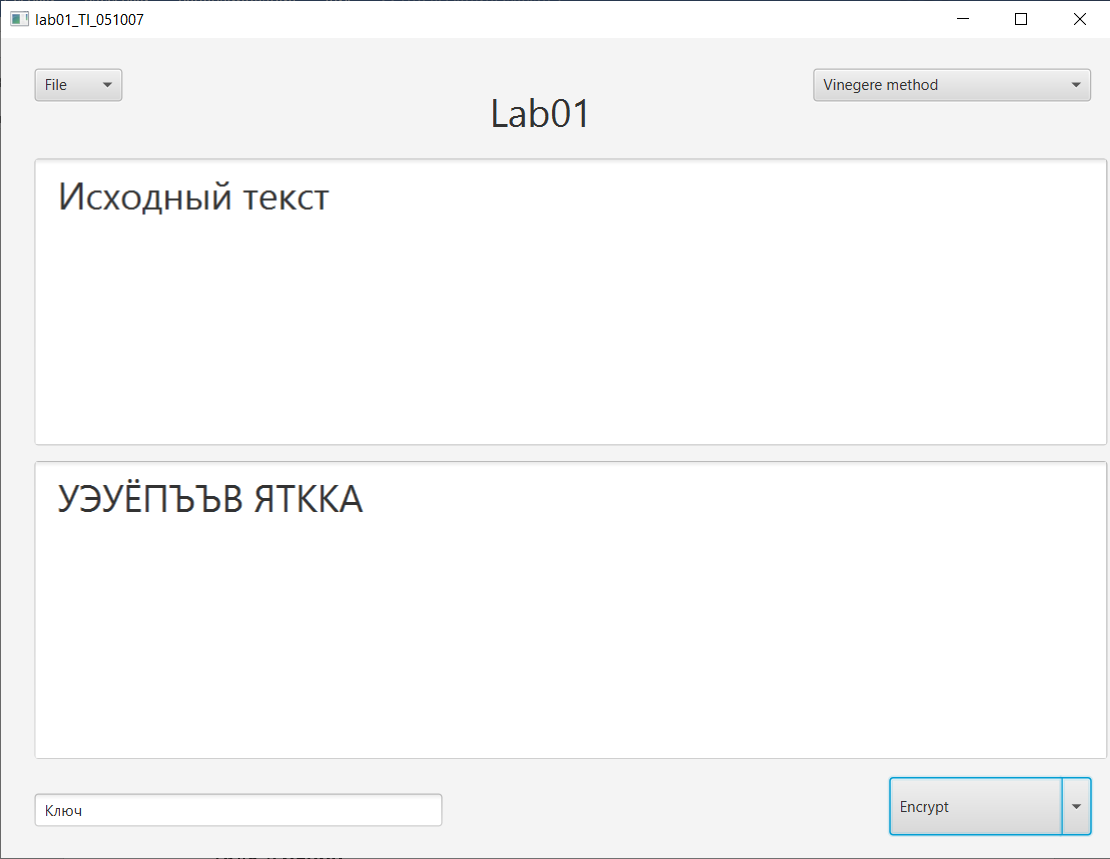
Ключ: **Ключ** (Прогрессивный ключ: КЛЮЧ|ЛМЯШ|МНАЩ|Н)

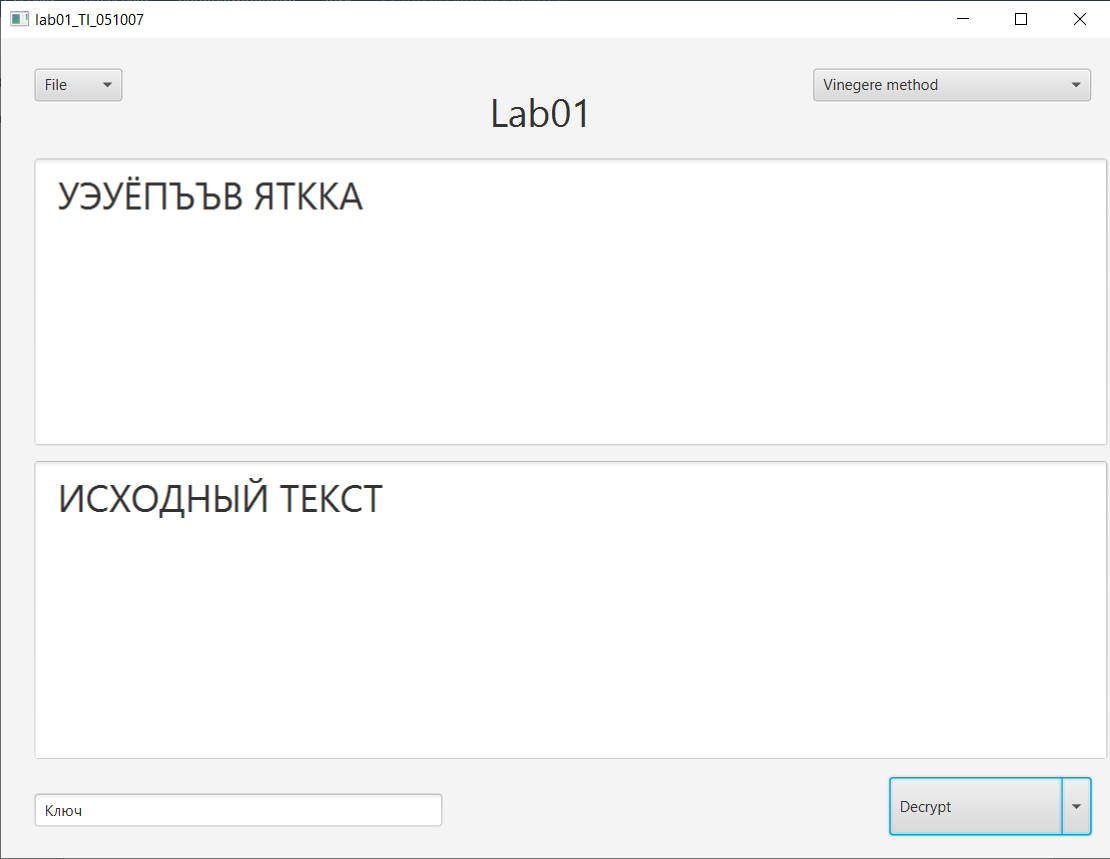
Результат: УЭУЁПЪЪВ ЯТККА

# Входная строка: Ёжик

Ключ: **ё**(Прогрессивный ключ: ёжзи)

Результат: ЛНРУ





# Входная строка: САНКТ-ПЕТЕРБУРГ – ГОРОД СВЯТОГО ПЕТРА

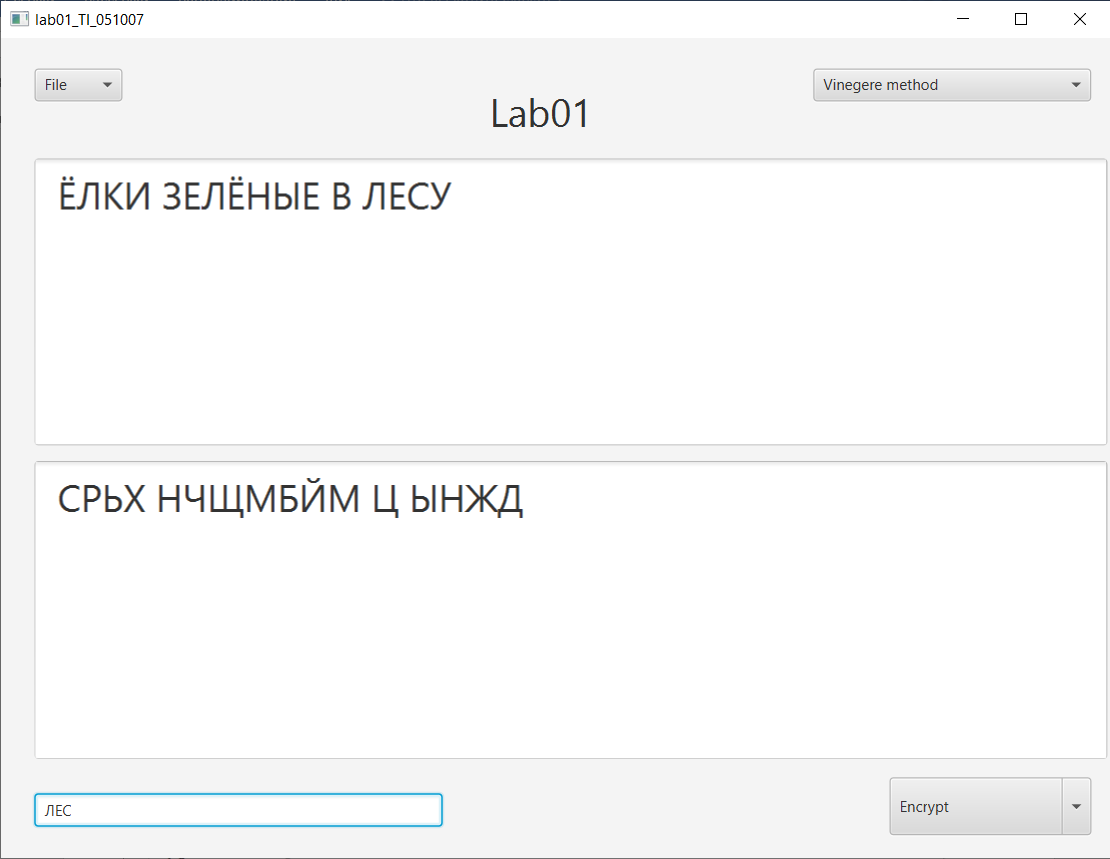
Ключ: **ленин**

# Результат: ЭЕЫУА-ЬКБОЯОЪАН – ТЭШЯП ВСЗДЫФЯ ЩЧАГС

# Входная строка: ЁЛКИ ЗЕЛЁНЫЕ В ЛЕСУ

Ключ: **ЛЕС**

# Результат: СРЬХ НЧЩМБЙМ Ц ЫНЖД



Входная строка: ЁЛ RVFКИ ЗЕ!!ЛЁНЫЕ В ЛЕ@СУ!

Ключ: **ЛWЕ\_С2**

# Результат: СР RVFЬХ НЧ!!ЩМБЙМ Ц ЫН@ЖД!

**Метод Децимации:**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** | **I** | **J** | **K** | **L** |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **M** | **N** | **O** | **P** | **Q** | **R** | **S** | **T** | **U** | **V** | **W** | **X** | **Y** | **Z** |
| 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

# Входная строка: Cryptography

Ключ: **3**

# Результат: Gzutfqszatvu

# G = (POS(’C’) \* 3) mod 26 = 2\*3 mod 26 = 6 mod 26 = 16

# z = (POS(’r’) \* 3) mod 26 = 17\*3 mod 26 = 51 mod 26 = 25

# u = (POS(’y’) \* 3) mod 26 = 24\*3 mod 26 = 72mod 26 = 20

# t = (POS(’p’) \* 3) mod 26 = 15\*3 mod 26 = 45 mod 26 = 19

# f = (POS(’t’) \* 3) mod 26 = 19\*3 mod 26 = 57 mod 26 = 5

# q = (POS(’o’) \* 3) mod 26 = 14\*3 mod 26 = 42 mod 26 = 16

# s = (POS(’g’) \* 3) mod 26 = 6\*3 mod 26 = 18 mod 26 = 18

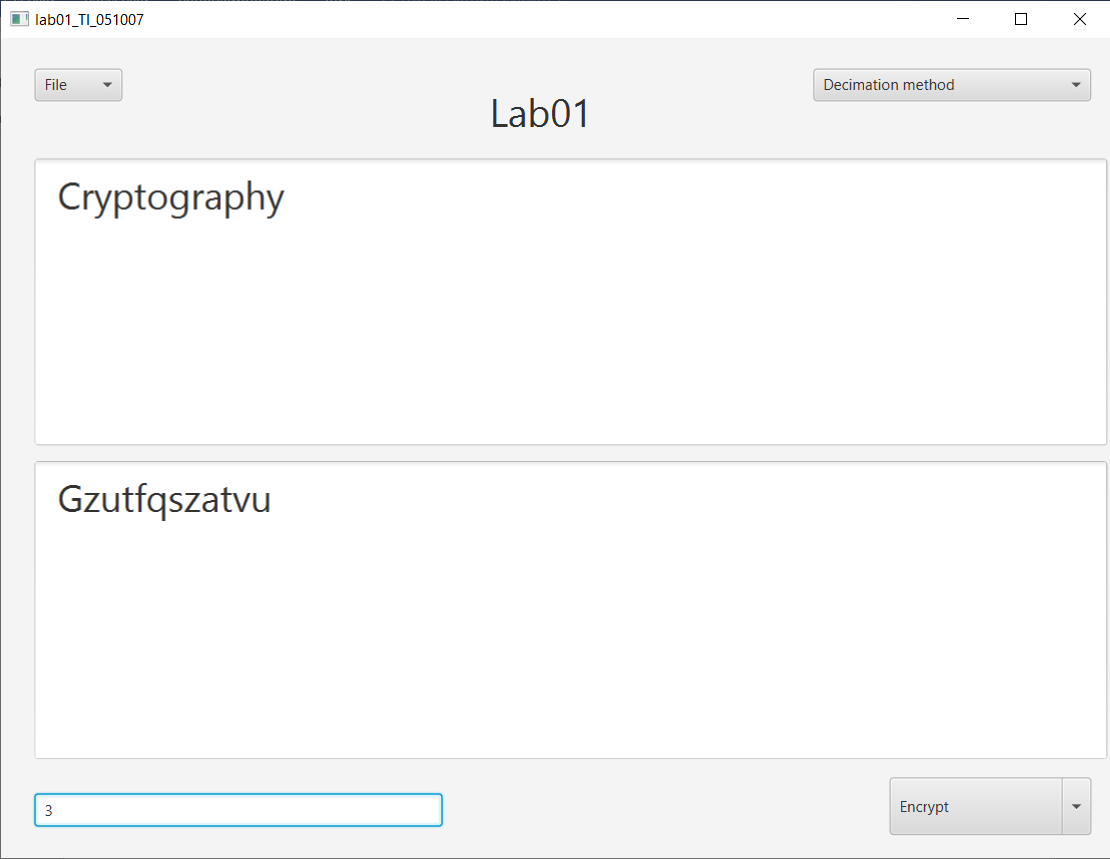
# z = (POS(’r’) \* 3) mod 26 = 17\*3 mod 26 = 51 mod 26 = 25

# a = (POS(’a’) \* 3) mod 26 = 0\*3 mod 26 = 0 mod 26 = 0

# t = (POS(’p’) \* 3) mod 26 = 15\*3 mod 26 = 45 mod 26 = 19

# v = (POS(’h’) \* 3) mod 26 = 7\*3 mod 26 = 21 mod 26 = 21

# u = (POS(’y’) \* 3) mod 26 = 24\*3 mod 26 = 72 mod 26 = 20

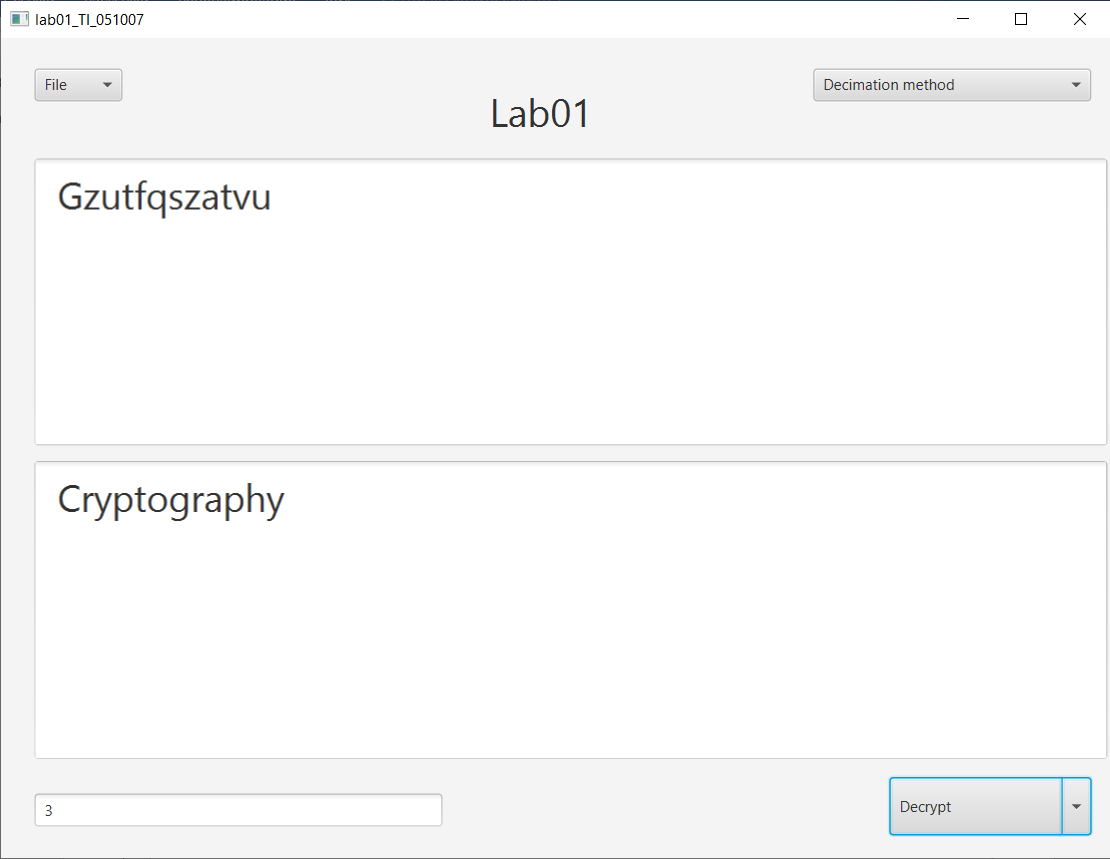


# Входная строка: Text!

Ключ: **0**

# Результат: Aaaa!

(<Любой символ> \* 0) % 26 = 0 = A



# Входная строка: ABC

Ключ: **5**

# Результат: AFK

(0(A) \* 5) % 26 = 0(A)

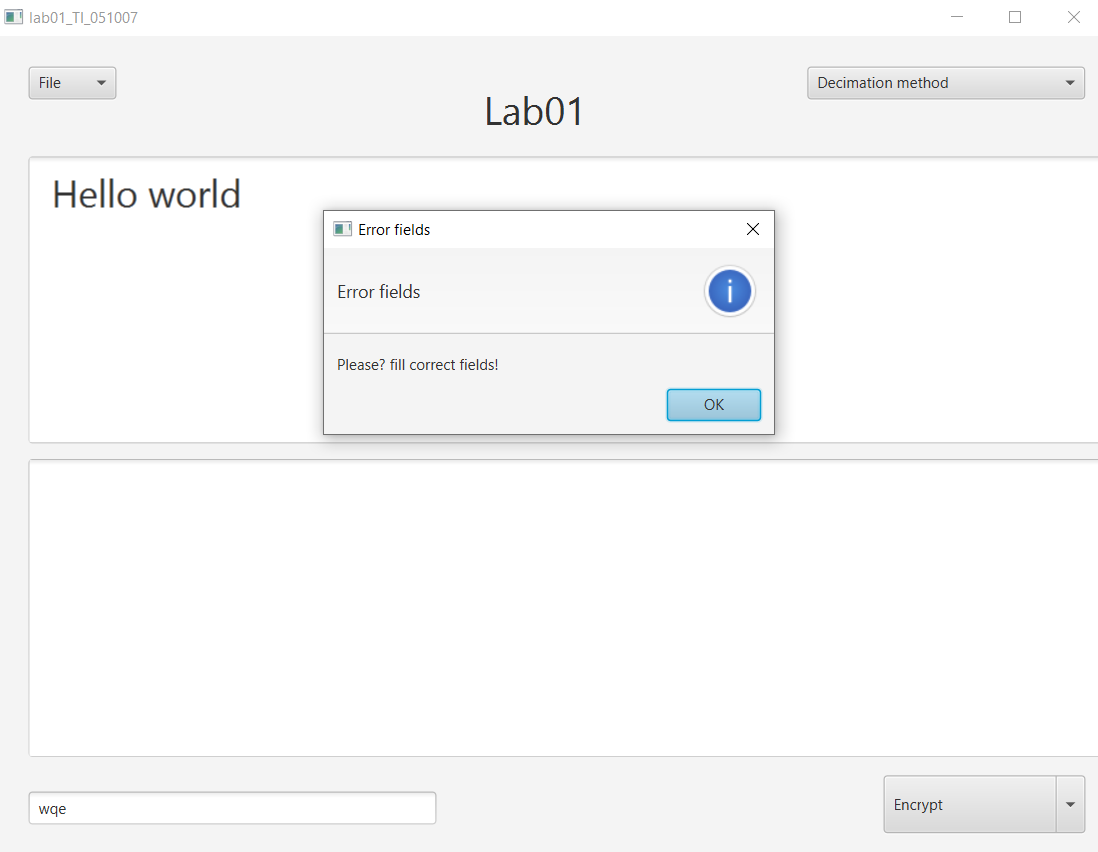
(1(B) \* 5) % 26 = 5(F)

(2(C) \* 5) % 26 = 10(K)

# Входная строка: Hello world

Ключ: **45**

# Результат: Dybbg cglbf



# Входная строка: Hel123lo woБ3rld!

Ключ: **45**

# Результат: Dyb123bg cgБ3lbf!

