**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ**

**УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«МОСКОВСКИЙ АВИАЦИОННЫЙ ИНСТИТУТ**

**(национальный исследовательский университет)»**

Институт №3 «Системы управления, информатика и электроэнергетика»

Кафедра 311 «Прикладные программные средства и математические методы»

**ЛАБОРАТОРНАЯ РАБОТА №1**

**по дисциплине:**

**«Информационная безопасность»**

Выполнила:

Студентка гр. М3О-316Б-22

Хутиева Эрика Арсеновна

Подпись:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Принял:

Агамиров В.Л.

Москва, 2025

**Шифр Цезаря**

import typing as tp

def encrypt\_caesar(plaintext: str, shift: int = 3) -> str:

ciphertext = ""

for i in plaintext:

if 'A' <= i <= 'Z':

ciphertext += chr((ord(i) - ord('A') + shift) % 26 + ord('A'))

elif 'a' <= i <= 'z':

ciphertext += chr((ord(i) - ord('a') + shift) % 26 + ord('a'))

else:

ciphertext += i

return ciphertext

def decrypt\_caesar(ciphertext: str, shift: int = 3) -> str:

plaintext = ""

for i in ciphertext:

if 'A' <= i <= 'Z':

plaintext += chr((ord(i) - ord('A') - shift) % 26 + ord('A'))

elif 'a' <= i <= 'z':

plaintext += chr((ord(i) - ord('a') - shift) % 26 + ord('a'))

else:

plaintext += i

return plaintext

def caesar\_breaker\_brute\_force(ciphertext: str, dictionary: tp.Set[str]) -> int:

best\_shift = 0

plaintext = ""

while plaintext not in dictionary:

best\_shift += 1

plaintext = decrypt\_caesar(ciphertext, best\_shift)

return best\_shift

print(encrypt\_caesar("PYTHON"))

print(encrypt\_caesar("python"))

print(encrypt\_caesar("Python3.6"))

print(encrypt\_caesar(""))

print(decrypt\_caesar("SBWKRQ"))

print(decrypt\_caesar("sbwkrq"))

print(decrypt\_caesar("Sbwkrq3.6"))

print(decrypt\_caesar(""))

print(caesar\_breaker\_brute\_force("SBWKRQ", {"PYTHON", "python", "Python3.6", "sbwkrq", "Sbwkrq3.6"}))