Лабораторная работа 8

Накова Амина

2025-09-20

1. Вводная часть

1.1 Цель работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

2. Ход работы

2.1 Постановка задачи

Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочитать оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить (рис. 1).

```
Лабораторная работа №7: Однократное гаммирование
==================================================
1. Проверка работы алгоритма на примере из
задания:
Ключ Центра:
050C177F0E4E37D29410092E2257FFC80BB27054
Сообщение Центра: Штирлиц - Вы Герой!!
Шифротекст у Мюллера:
DDEEEE8EE5A6C1E2B930CBD502941A38E55B5175
```

3. Основная программа

if **name** == «**main**»: print(«Лабораторная работа №8: Шифрование двух текстов одним ключом») print(«=» * 60)

```
# [illegible]
key_hex = "05107F0E4E37D29410092E2257FFC80BB27054"
p1 = "[illegible]1204"
p2 = "[illegible]"

print("[illegible]:")
print(f"[illegible]: {key_hex}")
print(f"P1: {p1}")
print(f"P2: {p2}")
print()

# [illegible]
```