Министерство образования Республики Беларусь

Учреждение образования БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей

Кафедра информатики

Дисциплина: Методы защиты информации

Отчёт по лабораторной работе №1

По теме «Симметричная криптография. Стандарт шифрования

ГОСТ 28147-89»

Выполнили: студент гр. 053501 Кривецкий Р. А.

Проверил: ассистент кафедры информатики Лещенко Е. А.

Минск 2023

**СОДЕРЖАНИЕ**

[1 Теоретические сведения 3](#_Toc148061125)

[2 Программная реализация 6](#_Toc148061126)

[Заключение 7](#_Toc148061127)

[Приложение А(обязательное) Листинг программного кода 8](#_Toc148061128)

# 1 ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования» — устаревший государственный стандарт СССР (а позже межгосударственный стандарт СНГ), описывающий алгоритм симметричного блочного шифрования и режимы его работы.

Является примером DES-подобных криптосистем, созданных по классической итерационной схеме Фейстеля.

История создания шифра и критерии разработчиков были впервые публично представлены в 2014 году руководителем группы разработчиков алгоритма Заботиным Иваном Александровичем на лекции, посвященной 25-летию принятия российского стандарта симметричного шифрования.

Работы над алгоритмом, положенным впоследствии в основу стандарта, начались в рамках темы «Магма» (защита информации криптографическими методами в ЭВМ ряда Единой Системы) по поручению Научно-технического совета Восьмого главного управления КГБ СССР (ныне в структуре ФСБ), в марте 1978 года после длительного предварительного изучения опубликованного в 1976 году стандарта DES. В действительности работы по созданию алгоритма (или группы алгоритмов), схожего с алгоритмом DES, начались уже в 1976 году.

Изначально работы имели гриф «Совершенно секретно». Затем были понижены до грифа «Секретно». В 1983 году гриф алгоритма был понижен до пометки «Для служебного пользования». Именно с последней пометкой алгоритм был подготовлен для публикации в 1989 году. 9 марта 1987 года группа разработчиков-криптографов (заявитель — в/ч 43753) получила авторское свидетельство с приоритетом № 333297 на изобретение на устройство шифрования по алгоритму «Магма-2».

Утверждён постановлением Госстандарта СССР № 1409 от 2 июня 1989 года, введен в действие с 1 июля 1990 года.

С 31 марта 1996 года переиздан и введен в действие как межгосударственный стандарт СНГ.

Постановлением Госстандарта Республики Беларусь № 3 от 17 декабря 1992 года введен в действие в качестве государственного стандарта Республики Беларусь. Переиздан в марте 2011 года.

Приказом Госпотребстандарта Украины № 495 от 22 января 2008 года ГОСТ 28147-89 был переиздан на территории Украины и введён в действие с 1 февраля 2009 года под наименованием ДСТУ ГОСТ 28147:2009. Согласно текущим приказам, ДСТУ ГОСТ 28147:2009 действовал до 1 января 2022 года. Идет постепенная замена на ДСТУ 7624:2014 (шифр «Калина»).

Стандарт отменён на территории России и СНГ с 31 мая 2019 года в связи с принятием новых полностью его заменяющих межгосударственных стандартов ГОСТ 34.12-2018 (описывает шифры «Магма» и «Кузнечик») и ГОСТ 34.13-2018 (описывает режимы работы блочных шифров).

Согласно извещению ФСБ о порядке использования алгоритма блочного шифрования ГОСТ 28147-89, средства криптографической защиты информации, предназначенные для защиты информации, не содержащей сведений, составляющих государственную тайну, реализующие в том числе алгоритм ГОСТ 28147-89, не должны разрабатываться после 1 июня 2019 года, за исключением случаев, когда алгоритм ГОСТ 28147-89 в таких средствах предназначен для обеспечения совместимости с действующими средствами, реализующими этот алгоритм.

ГОСТ 28147-89 — блочный шифр с 256-битным ключом и 32 циклами (называемыми раундами) преобразования, оперирующий 64-битными блоками. Основа алгоритма шифра — сеть Фейстеля.

Выделяют четыре режима работы ГОСТ 28147-89:

– простой замены;

– гаммирование;

– гаммирование с обратной связью;

– режим выработки имитовставки;

Гамми́рование, или Шифр XOR, — метод симметричного шифрования, заключающийся в «наложении» последовательности, состоящей из случайных чисел, на открытый текст. Последовательность случайных чисел называется гамма-последовательностью и используется для зашифровывания и расшифровывания данных. Суммирование обычно выполняется в каком-либо конечном поле. Например, в поле Галуа GF(2) суммирование принимает вид операции «исключающее ИЛИ (XOR)».

При работе ГОСТ 28147-89 в режиме гаммирования описанным выше образом формируется криптографическая гамма, которая затем побитно складывается по модулю 2 с исходным открытым текстом для получения шифротекста. Шифрование в режиме гаммирования лишено недостатков, присущих режиму простой замены. Так, даже идентичные блоки исходного текста дают разный шифротекст, а для текстов с длиной, не кратной 64 бит, «лишние» биты гаммы отбрасываются. Кроме того, гамма может быть выработана заранее, что соответствует работе шифра в поточном режиме.

Выработка гаммы происходит на основе ключа и так называемой синхропосылки, которая задает начальное состояние генератора. Алгоритм выработки следующий:

Синхропосылка шифруется с использованием описанного алгоритма простой замены, полученные значения записываются во вспомогательные 32-разрядные регистры N3 и N4 — младшие и старшие биты соответственно.

N3 суммируется по модулю 232 с константой C2 = 101010116

N4 суммируется по модулю 232−1 с константой C1 = 101010416

N3 и N4 переписываются соответственно в N1 и N2, которые затем шифруются с использованием алгоритма простой замены. Полученный результат является 64 битами гаммы.

Шаги 2-4 повторяются в соответствии с длиной шифруемого текста.

Для расшифровывания необходимо выработать такую же гамму, после чего побитно сложить её по модулю 2 с зашифрованным текстом. Очевидно, для этого нужно использовать ту же синхропосылку, что и при шифровании. При этом, исходя из требований уникальности гаммы, нельзя использовать одну синхропосылку для шифрования нескольких массивов данных. Как правило, синхропосылка тем или иным образом передается вместе с шифротекстом.

Особенность работы ГОСТ 28147-89 в режиме гаммирования заключается в том, что при изменении одного бита шифротекста изменяется только один бит расшифрованного текста. С одной стороны, это может оказывать положительное влияние на помехозащищённость; с другой — злоумышленник может внести некоторые изменения в текст, даже не расшифровывая его.

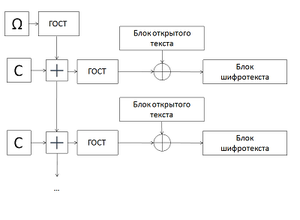


Рисунок 1.1 — Схема работы в режиме гаммирования

**2 ПРОГРАММНАЯ РЕАЛИЗАЦИЯ**

Необходимо реализовать программные средства шифрования и дешифрования текстовых файлов при помощи стандарта шифрования ГОСТ 28147-89 в режиме гаммирования. Программное средство реализовано на языке программирования Python. Демонстрация работы показана на рисунке 2.1

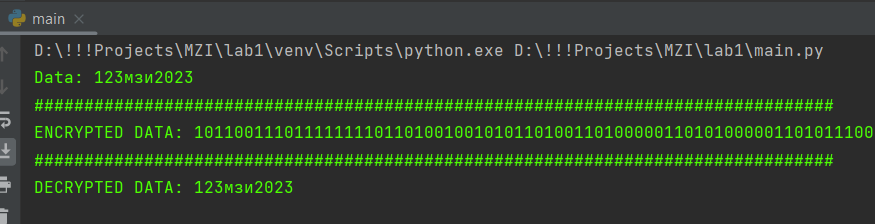


Рисунок 2.1 — Демонстрация работы

Вывод в консоль сделан для дополнительной наглядности, корректная работа с файлами показана на рисунке 2.2.

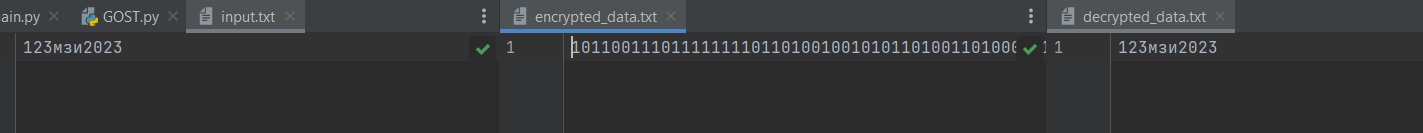


Рисунок 2.2 — Ввод/вывод файлов

# ЗАКЛЮЧЕНИЕ

В результате лабораторной работы было реализовано программное средство шифрования и дешифрования текстовых файлов при помощи стандарта шифрования ГОСТ 28147-89 в режиме гаммирования. Использование ГОСТ 28147-89 в режиме гаммирования (GOST 28147-89 CFB) предоставляет несколько преимуществ и недостатков:

Преимущества:

1 Конфиденциальность данных: Режим гаммирования обеспечивает конфиденциальность данных, так как каждый блок данных шифруется независимо. Это значит, что изменение одного бита открытого текста приведет к существенным изменениям в шифротексте, что делает атаки по шифротексту более сложными.

2 Параллельная обработка: Каждый блок данных можно обрабатывать независимо, что упрощает параллельную обработку данных и может повысить производительность при шифровании больших объемов информации.

Недостатки:

1 Размер блока: GOST 28147-89 имеет фиксированный размер блока (64 бита), что ограничивает его способность работать с данными различных размеров. Для данных, которые не являются кратными 64 битам, могут потребоваться дополнительные манипуляции.

2 Инициализация и управление IV: Правильное управление вектором инициализации (IV) является критическим аспектом безопасности режима гаммирования. Один и тот же ключ и IV не должны использоваться для разных сообщений. Нарушение правил управления IV может привести к уязвимостям.

3 Аутентификация: Режим гаммирования не обеспечивает аутентификацию данных. Это означает, что он уязвим к атакам, таким как атаки с введением данных и атаки типа "человек посередине" (Man-in-the-Middle). Для обеспечения аутентификации данных следует применять методы аутентифицированного шифрования.

4 Специфичность ГОСТ 28147-89: ГОСТ 28147-89 - это стандарт, который может быть менее распространенным за пределами стран, использующих ГОСТ-стандарты, поэтому его использование может быть ограничено в мировой практике.

В целом, режим гаммирования ГОСТ 28147-89 полезен, но требует внимательного управления вектором инициализации и может потребовать дополнительных мер для обеспечения безопасности и аутентификации данных в реальных приложениях.

# ПРИЛОЖЕНИЕ А

(**обязательное)**

**Листинг программного кода**

Файл main.py

from GOST import GOST

def main():

gost = GOST()

# data = input("enter data:\n")

with open("input.txt", "r", encoding='utf-8') as data\_file:

data = data\_file.read()

print(f"Data: {data}")

encrypted\_data = gost.gamma\_encrypt\_text(data)

print('#' \* 80)

print(f'ENCRYPTED DATA:\t{encrypted\_data}')

with open("encrypted\_data.txt", "w", encoding='utf-8') as encrypted\_file:

encrypted\_file.write(encrypted\_data)

print('#' \* 80)

decrypted\_data = gost.gamma\_decrypt(encrypted\_data)

print(f'DECRYPTED DATA:\t{decrypted\_data}')

with open("decrypted\_data.txt", "w", encoding='utf-8') as decrypted\_file:

decrypted\_file.write(decrypted\_data)

if \_\_name\_\_ == '\_\_main\_\_':

main()