Пшенко Артем, ФИТ 3-4

Информационная безопасность

Отчет по лабораторной работе № 6.

Изучение устройства и функциональных особенностей шифровальной машины «Энигма»

Вариант 9

Цель данной лабораторной работы состоит в изучении работы шифровальной машины Enigma, применении ее для шифрования и дешифрования сообщений. Необходимо продемонстрировать, как шифрование и последующее дешифрование исходного сообщения возвращает его в первоначальное состояние.

Шифровальная машина Enigma использовалась для шифрования и дешифрования сообщений. Она состоит из нескольких роторов, отражателя и соединительных кабелей (plugboard), которые вместе создают сложную систему подстановки символов.

Для данной работы был использован следующий конфигурационный набор:

1. Роторы: VIII, II, IV
2. Отражатель: B
3. Настройки колец: 1, 0, 1
4. Подключения plugboard: AV BS CG DL FU HZ IN KM OW RX

Алгоритм работы машины Enigma:

1. Ввод символа: пользователь вводит букву на клавиатуре Enigma.
2. Прохождение через plugboard (соединительная панель): введенная буква проходит через набор соединений, где буквы могут быть попарно заменены.
3. Прохождение через роторы: буква проходит через серию роторов, каждый из которых сдвигает букву в соответствии с внутренней схемой подстановки. Каждый ротор после каждого ввода символа поворачивается, изменяя подстановку.
4. Отражатель: после прохождения через роторы, буква попадает в отражатель, который меняет ее направление и отправляет обратно через роторы.
5. Обратное прохождение через роторы: буква снова проходит через роторы в обратном порядке, с учетом текущих положений роторов.
6. Возвращение через plugboard: буква снова проходит через соединительную панель, где происходит очередная замена.
7. Вывод символа: зашифрованная буква отображается на светящейся панели.

Исходный код на языке Python реализует следующие шаги:

1. Создание экземпляра EnigmaMachine с заданными параметрами.
2. Установка начального положения роторов на 'WXC'.
3. Шифрование исходного сообщения.
4. Сброс положения роторов на 'WXC'.
5. Дешифрование зашифрованного сообщения для восстановления исходного текста.

Листинг 1. Исходный код машины «Энигма»

|  |
| --- |
| from enigma.machine import EnigmaMachine  machine = EnigmaMachine.from\_key\_sheet(  rotors='VIII II IV',  reflector='B',  ring\_settings=[1, 0, 1],  plugboard\_settings='AV BS CG DL FU HZ IN KM OW RX')  machine.set\_display('WXC')  message = 'Pshenko'  ciphertext = machine.process\_text(message)  print(f'Зашифрованное сообщение: {ciphertext}')  machine.set\_display('WXC')  plaintext = machine.process\_text(ciphertext)  print(f'Расшифрованное сообщение: {plaintext}') |

Результат работы программы приведен на рисунке 1.



Рисунок 1. Результат работы программы

В ходе лабораторной работы была продемонстрирована работа шифровальной машины Enigma. Шифрование исходного сообщения "Pshenko" с последующим его дешифрованием показало, что при правильной настройке машины и соответствующих параметров, исходное сообщение успешно восстанавливается. Это подтверждает корректность работы алгоритма Enigma и демонстрирует его эффективность для шифрования и защиты информации.