Розробка копії шифрувальної машини Енігма

Основне завдання системи: Основним завданням є визначення принципу роботи оригінальної машини Енігма.

Мета дослідження: Метою виконання даної роботи є визначення та реалізація алгоритму роботи шифрувальної машини

Об'єкт дослідження: копія пристрою Енігма

Предмет дослідження: Ефективність шифрування

В Енігмі було три відсіки для розміщення трьох роторів і додатковий відсік для розміщення рефлектора. Всього за час Другої світової війни було виготовлено вісім роторів і чотири рефлектори, але одночасно могло використовуватися рівно стільки, на скільки була розрахована машина. Кожен ротор мав 26 перетинів, що відповідало окремої букві алфавіту, а так само 26 контактів для взаємодії з сусідніми роторами. Як тільки оператор натискав на потрібну букву, - замикався електрична ланцюг, в результаті чого з'являлася шифрована буква. Замикання ланцюга відбувалося за рахунок рефлектора.

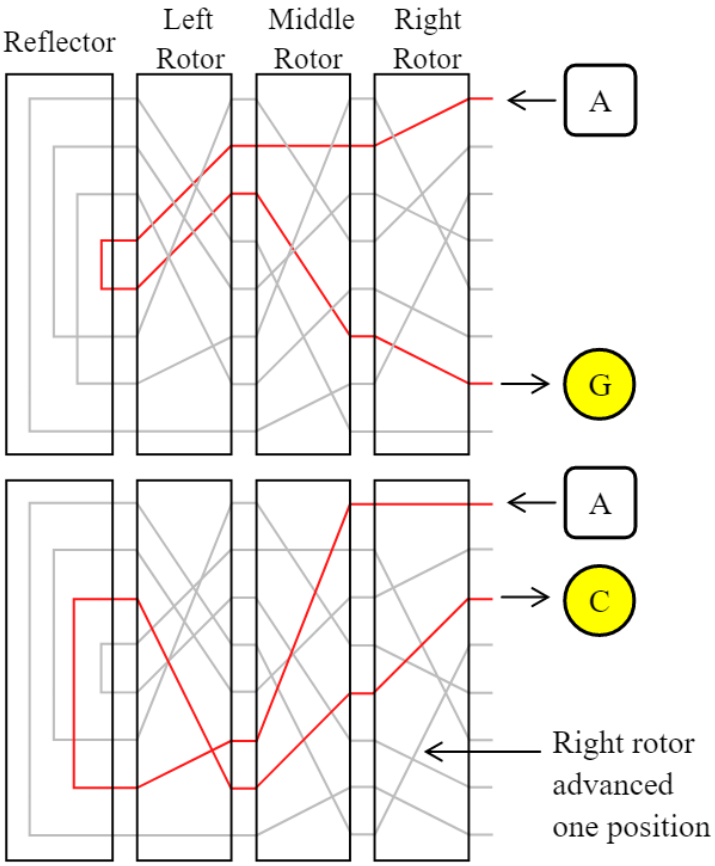

Рисунок 1 - Принцип роботи шифрувальної машини Енігма

На рис 1. представлена ілюстрація натискання клавіші «A» з подальшою дешифрацией в букву «G». Після введення літери крайній правий ротор переміщався вперед, змінюючи тим самим ключ. Усередині кожного з ротора них було встановлено 26 різних комутацій. Наприклад, якщо на вхід першого ротора надходила буква «N», то на виході повинна бути тільки «W» і ніяка інша буква більше. Влуч це буква на другий ротор, вона б уже перетворилася в «T» і т.д. Тобто, кожен ротор виконував чітко поставлене завдання в плані комунікації.

Крім того, була ще комутаційна панель, в яку можна було вставляти дроти, які попарно міняли літери. Тобто встромивши провід одним кінцем в гніздо «A», а іншим - в «E», ви міняли ці букви місцями.

Кількість роторів варіювалося в різні роки і для різного призначення (наприклад, у флоті використовувалися Енігми з великою кількістю роторів).

Для ускладнення злому оператори кодували часто використовуючи слова (назви) кожного разу по-різному. Наприклад, слово «Minensuchboot» могло бути написано як «MINENSUCHBOOT», «MINBOOT», «MMMBOOT» або «MMM354».

Як до будь-якого популярного пристрою, до Енігма існувала велика кількість аксесуарів (так-так, це почалося вже тоді). Наприклад, були авто-друкують устрою (у звичайній версії кодування вироблялося спалахують лампочками, значення яких повинен був записувати оператор).

Крім того, були дистанційні принтери. Щоб оператор, вбивається зашифроване повідомлення в машину, не мав доступу до розшифруваного.