УДК 51-37

Шолин И.М.,
студент 1 курса магистратуры офо
«Кубанский государственный технологический университет
г. Краснодар, Россия
Чубырь Н. О.,
Доцент кафедры. Кандидат физико-математических наук
«Кубанский государственный технологический университет
г. Краснодар, Россия

АЛГОРИТМ ПЕРЕНОСНОЙ ШИФРОВАЛЬНОЙ МАШИНЫ ЭНИГМА

Аннотация: *Сокрытие информации с давних времен является одним из обязательных условий эффективного ведения войны. Для этих целей было придумано огромное количество разнообразных шифров и шифровальных машин. В данной статье рассматривается шифровая машина для шифрования и дешифрования закодированных сообщений.*

Ключевые слова: *шифр, кодирование, роторы, переменные, комбинации, уравнение.*

Sholin I. M.,
magister of 1st year
" Kuban State University of Technology
Krasnodar, Russia
Chubyr. N. Y.,
Associate Professor. Candidate of Physico-Mathematical Sciences
"Financial University under the Government of the Russian Federation
(Krasnodar branch)
Krasnodar, Russia

ALGORITHM OF THE ENIGMA PORTABLE ENCRYPTION MACHINE

Abstract: *Hiding information from ancient times is one of the prerequisites for the effective introduction of war. For these purposes, a huge number of ciphers and encryption machines were invented. This article discusses the encryption engine for encrypting and decrypting encrypted messages.*

Key words: *cipher, coding, rotors, variables, combinations, equation.*

Энигма является криптографической машиной, которая была создана в 1920-х ", как способ для немецких военных обеспечить свои коммуникации. Этот шифр машина используется для шифрования и расшифровки закодированных сообщений. Немецкая армия приобрела эти машины в 1925 году от своего первоначального производителя, Chiffriermaschinen Aktiengesellschaft. Машина Энигма была очень трудна для взлома, что делала его очень ценной для немецкой армии.

Такие роторные машины как «Энигма» состояли из комбинации механических и электрических подсистем. Механическая часть включала в себя клавиатуру, набор вращающихся дисков — роторов, — которые были расположены вдоль вала и прилегали к нему, и ступенчатого механизма, двигающего один или несколько роторов при каждом нажатии на клавишу. Электрическая часть, в свою очередь, состояла из электрической схемы, соединяющей между собой клавиатуру, коммутационную панель, лампочки и роторы (для соединения роторов использовались скользящие контакты).

Конкретный механизм работы мог быть разным, но общий принцип был таков: при каждом нажатии на клавишу самый правый ротор сдвигается на одну позицию, а при определённых условиях сдвигаются и другие роторы. Движение роторов приводит к различным криптографическим преобразованиям при каждом следующем нажатии на клавишу на клавиатуре.

Механические части двигались, замыкая контакты и образуя меняющийся электрический контур (то есть, фактически, сам процесс шифрования букв реализовывался электрически). При нажатии на клавишу клавиатуры контур замыкался, ток проходил через различные цепи и в результате включал одну из набора лампочек, и отображавшую искомую букву кода.

«Энигма» была разработана таким образом, чтобы безопасность сохранялась даже в тех случаях, когда шпиону известны роторные схемы, хотя на практике настройки хранятся в секрете. С неизвестной схемой общее количество возможных конфигураций может быть порядка 10^{114} (около 380 бит), с известной схемой соединений и других операционных настроек этот показатель снижается до 10^{23} (76 бит). Пользователи «Энигмы» были уверены в её безопасности из-за большого количества возможных вариантов. Нереальным было даже начать подбирать возможную конфигурацию.

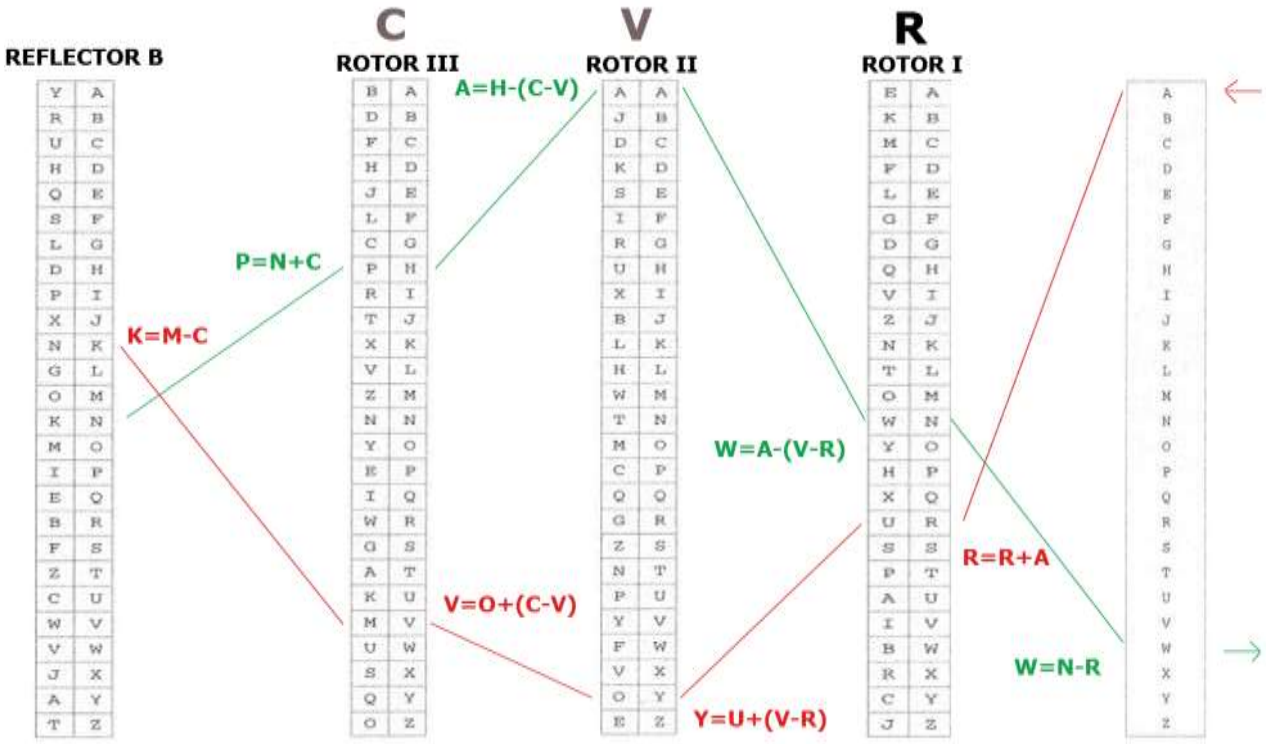
Существует приблизительно 150 000 000 000 000 способов связывания пар букв на машине Enigma - то есть 150 миллионов - возможных комбинации из 10 пар из 26 букв на плате плагина. Математика за этим вычислением сложна.

Таким образом, общее количество возможных способов, с помощью которых можно было установить стандартную машину Enigma для армейской эмиссии, было:

$$60 \times 17,576 \times 676 \times 150,738,274,937,250,$$

Для Энигмы было разработано восемь различных роторов. Внутри каждого из них было установлено 26 различных коммутаций. Если на вход первого ротора поступала буква «N», то на выходе должна быть только «W» и никакая другая буква больше. Попади это буква на второй ротор, она бы уже преобразовалась в «T» и т.д. То есть, каждый ротор выполнял четко поставленную задачу в плане коммуникации. А какую же роль играли кольца? Рассмотрим следующий пример. Установим роторы III, II и I, а порядок колец «C», «U» и «Q».


Enigma Simulator
Zum Betrieb mit eingebauter Batterie Stecker heraus.
4Volt
220 Volt
Wechselstrom
C U Q
Q W E R T Z U I O
A S D F G H J K
P Y X C V B N M L
M 2114


REFLECTOR B
C
ROTOR III
V
ROTOR II
R
ROTOR I
A=H-(C-V)
P=N+C
K=M-C
W=A-(V-R)
R=R+A
V=O+(C-V)
W=N-R
Y=U+(V-R)

Нажмем на клавишу «A». Крайний правый ротор повернется вперед на один шаг, то есть, буква «Q» перейдет в «R». Ротор посередине также повернется вперед на букву «V», но об этом я расскажу чуть позже. Итак, наша буква «A» начинает путешествие с первого отсека, в котором установлен ротор I и на котором выставлена уже буква «R». Уже перед тем как попасть на первый ротор буква претерпевает свое первое преобразование, а именно: сложение с буквой «R» по модулю 26. Фактически, это шифр Цезаря. Если пронумеровать все буквы от 0 до 25, то буква «A» будет как раз таки нулевой. Значит, результатом сложения будет буква «R». Далее, мы с вами знаем, что в первом отсеке ротор I, а в его конструкции заложено, что буква «R» всегда переходит в «U». Теперь на очереди второй отсек с ротором II. Опять, перед попаданием на второй ротор, теперь уже буква «U» меняется по несколько иному алгоритму: к ней прибавляется **разница** значений последующего ротора и предыдущего. Поясню. На втором роторе ожидает нас буква «V», а на предыдущем, — «R», их разница равна четырем буквам, и именно они прибавляются к нашей букве «U». Поэтому, на второй ротор поступает буква «Y». Далее по таблице находим, что во втором роторе букве «Y» соответствует «O». Далее опять смотрим разницу букв «C» и «V», — она равна семи. Значит, букву «O» сдвигаем на семь позиций и получаем «V». В роторе III «V» переходит в «M». Перед тем как попасть на рефлектор, из нашей буквы вычитается буква «C», преображая ее в букву «K». Далее происходит отражение. Если вы заметите, то в каждом роторе образуются большие циклические группы, например: (A – E – L – T – P – H – Q – X – R – U), а в рефлекторе они разбиты по парам: (A — Y)(B — R)(C — U) и т.д. Это сделано для того, чтобы потом это возможно было расшифровать. Предположим, что установлен рефлектор B, в котором «K» заменяется на «N» (и наоборот). Половина пути пройдена. Теперь мы опять прибавляем значение буквы «C», получив тем самым букву «P». Здесь наоборот, в строке третьего ротора

находим «P» и смотрим, в при нажатии какой буквы она бы появилась. Это буква «H». Преобразование в третьем роторе закончено. Теперь из этой буквы вычитается разница букв «C» и «V», то есть семь. Получаем букву «A». Во втором роторе она переходит саму в себя, поэтому оставляем ее без изменений. Далее, вычитаем разницу букв «V» и «R», то есть четверку и получаем букву «W». В первом роторе её обратно преобразование отображается в букву «N». Остается только вычесть из нее букву «R» и получим искомую букву «W». Как видите, алгоритм работы машинки оказался не таким сложным каким казался. Для усовершенствования шифра немцы внедрили коммутационную панель, которая позволяла попарно менять местами буквы. Если мы соединим буквы «Q» и «W», то при вводе той же «A» мы получили бы «Q», так как по факту должна быть «W», но она заменена буквой «Q». Вот прилагаемая схема действия.

Осталось лишь рассказать про смещения роторов относительно друг друга. Правый ротор поворачивался всегда при нажатии клавиши на один шаг. Например, для ротора I эта позиция равна букве «R». Именно поэтому в нашем примере второй ротор повернулся: первый ротор прошел через букву «R». Далее, пройдя через определенную позицию, правый ротор приводил в движение левый на один шаг. В более усовершенствованных моделях левый ротор прокручивался два, а то и три раза.

Литература:

1. Алгоритм Энигмы [Электронный ресурс]. – Режим доступа: https://habr.com/post/217331/

2. Puzzled: The Underlying Mathematics of the [Электронный ресурс]. – Режим доступа: https://www./supercomputingchallenge.org/06-07/finalreports/63.pdf

3. Работа нациской шифровальной машины [Электронный ресурс]. – Режим доступа: https:// lenta.ru/news/2017/06/06/enigma/

4. Сингх Саймон - Книга шифров .Тайная история шифров и их расшифровки [Электронный ресурс]. – Режим доступа: http://www.royallib.com/book/singh_saymon/kniga_shifrov_taynaya_istoriya_shifrov_i_ih_rasshifrovki.html