Автор:
Кочелаев Арсений Викторович,
Корнеева София Максимовна
ученики 7 класса
Руководитель:
Кочелаева Елена Равильевна,
учитель информатики
Муниципальное бюджетное общеобразовательное учреждение г. Астрахани "Гимназия №3"

ШИФРОВАЛЬНАЯ МАШИНА «ЭНИГМА»

.

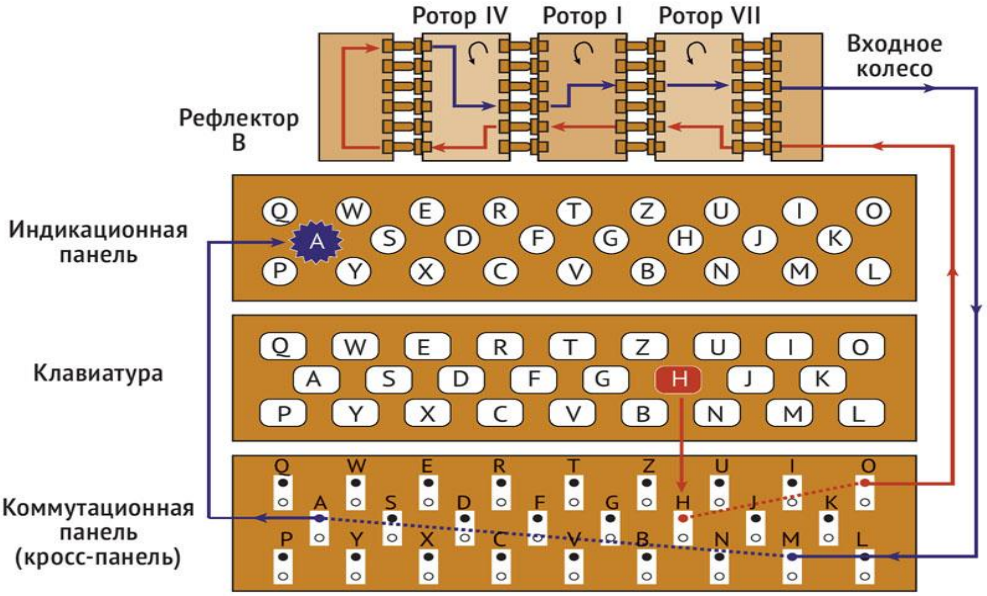
Вспоминая о Второй Мировой Войне, принято говорить о подвигах людей, сражавшихся на фронте или обеспечивавших армию в тылу. Однако часто забывается не менее важная составляющая войны - информационная. Не только провизия, не только боевое снаряжение и люди решали исход сражения, главным ресурсом на поле битвы всегда являлась информация. На протяжении всего военного времени велась непрерывная гонка по созданию и усовершенствованию шифров с одной стороны и попыткам их расшифровать с другой. Все, кто хотя бы немного интересуются военной историей, наверняка слышали о легендарной немецкой шифровальной машине «Энигма». Существует заблуждение, что в Советском Союзе криптография была слабо развита, но это далеко не так. В 1942 году советскими криптографами была создана новая шифровальная машина под кодовым названием М-101 «Изумруд». До окончания войны «Изумруд» считался самым «стойким» и надежным криптографическим аппаратом, который использовался для шифрования сообщений особой важности. С самого начала войны фашистские дешифровальщики пытались прочесть перехваченные советские криптограммы. Но все их попытки были напрасны. Приказ Гитлера по вермахту от августа 1942 года гласил: «Кто возьмёт в плен русского шифровальщика, либо захватит русскую шифровальную технику, будет награжден Железным крестом, отпуском на родину и обеспечен работой в Берлине, а после окончания войны – поместьем в Крыму».

В своем исследовании мы хотим разобраться с принципами работы Энигмы, понять алгоритм ее работы и построить простейший аппарат этой шифровальной машины.

Что же представляла собой эта машина?

Шифровальный механизм машины был весьма сложен. В «Энигме» использовался полиалфавитный шифр, наиболее известным примером которого является шифр Вижинера. Можно вкратце описать принцип работы шифра как динамический шифр Цезаря, в котором глубина сдвига меняется по определённому алгоритму. Сердцы «Энигмы» — это три ротора. На каждом из роторов с двух сторон нанесены 26 контактов, соответствующие буквам алфавита. Электрические соединения дорожек между контактами не идут по прямой, они отличаются от ротора к ротору. Роторы можно вынимать, менять их расположение или вставлять другие роторы из набора. Дополнительной мерой является использование коммутационной панели. Электрические соединения проводами на панели спереди машины позволяют менять буквы по парам: А может

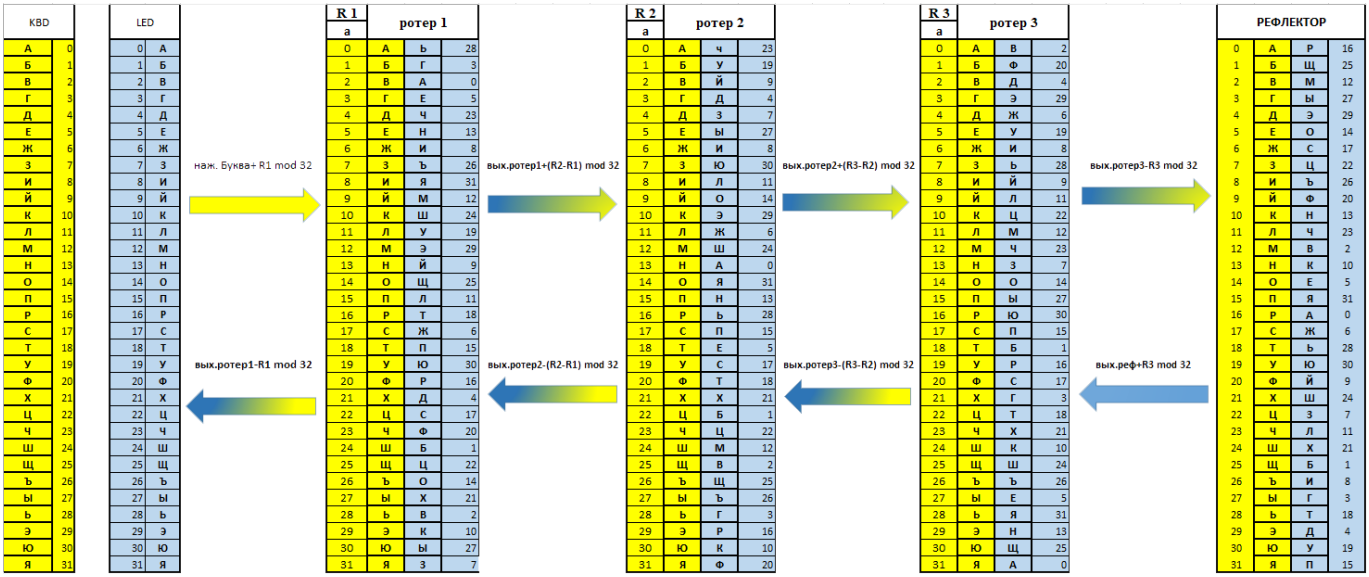
стать R, а R в этом случае станет A. Для чтения сообщения нужно знать положение роторов (3 символа латинского алфавита) и положение проводов на коммутационной панели.



Процесс перекодирования одной буквы в другую обеспечивался определёнными условиями, неизвестными оператору, меняющимися для каждой новой буквы, но поддающимися воспроизведению при аналогичной настройке машины. Таким образом, расшифровать можно было, задав дешифровальной машине тот же режим, что и шифровальной. А поскольку таких режимов было очень большое количество, расшифровать послание, не зная точных настроек, при которых оно было создано, не представлялось возможным.

В практической части исследования мы разработали программу на Pascal и на базе контролера Arduino создали шифровальную машину, в основе которой лежит алгоритм Энигмы.

Рассмотрим подробнее алгоритм шифрования.



Условные обозначения:

X – код нажатой буквы, R1- положение ротора 1, R2- положение ротора 2, R3- положение ротора 3 (на рисунке R1 = 26, R2=24, R3=6).

Алгоритм шифрования:

1. (X+ R1) mod 32
2. (вых.ротер1+(R2-R1)) mod 32
3. (вых.ротер2+(R3-R2))mod 32
4. (вых.ротер3-R3)mod 32
5. (вых.реф+R3)mod 32
6. (вых.ротер3-(R3-R2))mod 32
7. (вых.ротер2-(R2-R1))mod 32
8. (вых.ротер1-R1)mod 32

Программа на Pascal (при каждом запуске программы кодируется одна буква):

```
program p1;
const
a:array [0..31] of integer=(28,3,0,5,23,13,8,26,31,12,24,19,29,9,25,11,18,6,15,30,16,4,17,20,1,22,14,21,2,10,27,7);
```

```
    b:array [0..31] of inte-
ger=(1,19,9,4,7,27,8,30,11,14,29,6,24,0,31,13,28,15,5,17,18,21,16,22,12,2,25,
26,3,23,10,20);
    c:array [0..31] of inte-
ger=(2,20,4,29,6,19,8,28,9,11,22,12,18,7,14,27,30,15,1,16,17,3,23,21,10,24,26
,5,31,13,25,0);
    ref:array [0..31] of inte-
ger=(16,25,12,27,29,14,17,22,26,20,13,23,2,10,5,31,0,6,28,30,9,24,7,11,21,1,8
,3,18,4,19,15);
    alf:array [0..31] of
char=('а','б','в','г','д','е','ж','з','и','й','к','л','м','н','о','п','р','с','т','у','ф','х','ц','ч','
ш','щ','ъ','ы','ь','э','ю','я');
    var  x,i,rot1,rot2,rot3,sod1,sod2,sod3,pos1,pos2,pos3, sod_ref,pos_ref  :
integer;
    x1:string;
    begin
    read (rot1);
    read (rot2);
    read (rot3);
    read(x1);
    for i:=0 to 31 do
    if alf[i]=x1 then x:=i;
    pos1:=(x+rot1)mod 32;
    sod1:=a[pos1];
    pos2:=(sod1+(rot2-rot1)) mod 32;
    if pos2<0 then pos2:=pos2+32;
    sod2:=b[pos2];
    pos3:=(sod2+(rot3-rot2)) mod 32;
    if pos3<0 then pos3:=pos3+32;
    sod3:=c[pos3];
    pos_ref:=(sod3-rot3) mod 32;
```

```
if pos_ref<0 then pos_ref:=pos_ref+32;
sod_ref:=ref[pos_ref];
sod3:=(sod_ref+rot3)mod 32;
for i:=0 to 31 do
if c[i]=sod3 then pos3:=i;
sod2:=(pos3-(rot3-rot2))mod 32;
if sod2<0 then sod2:=sod2+32;
for i:=0 to 31 do
if b[i]=sod2 then pos2:=i;
sod1:=(pos2-(rot2-rot1))mod 32;
if sod1<0 then sod1:=sod1+32;
for i:=0 to 31 do
if a[i]=sod1 then pos1:=i;
x:=(pos1-rot1)mod 32;
if x<0 then x:=x+32;
write (alf[x]);
end.
```

Для создания шифровальной машины были использованы: плата Arduino, контроллер клавиатуры + Led-индикаторов, контроллер роторов, кнопки с буквами. Программный код не приведен в работе из-за ограничения на количество страниц, но может быть представлен.

Работая над проектом, я узнал много интересных фактов о Великой отечественной войне, реализовал алгоритм шифрования «Энигмы» на Паскале, научился работать с платой Ардуино и создал шифровальную машину. И хотя сама по себе машина «Энигма» с точки зрения современных представлений о защите информации практического интереса уже не представляет, однако многие из уроков истории «Энигмы» актуальны и сегодня.

Использованная литература

1. Как работала шифровальная машина “Энигма”: [Электронный ресурс] // Только война URL: http://war-only.com/kak-rabotala-shifrovalnaya-mashina-enigma.html (Дата обращения: 18.10.2019).
2. Код Энигмы URL: https://oyla.xyz/article/kod-enigmy (Дата обращения: 8.09.2019).
3. ARDUINO.RU URL: http://arduino.ru/ (Дата обращения: 15.11.2019).