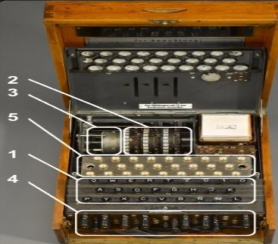
**ЭНИГМА (45 – 52)**

**Историческая информация**

все знают алгоритм шифрования, никто не мог подобрать ключ  
1923 – Enigma A, потом Enigma B  
Enigma C – компактнее + ламповая панель  
Enigma D – 3 ротора + отражатель

**Конструкция и функционирование**

мех часть:  
\* клавиатура  
\* роторы (вращ. диски)  
\* ступенч. мех, вращ. диски при нажатии клавиш

эл. часть:  
\* эл. схема, соед. клаву, панель, лампочки и роторы

5 осн. блоков:  
1) клавиши (дают сигнал поворота роторов)  
2) 3+ ротора (по окружности буквы)  
3) рефлектор (контакты с левым ротором, замыкает цепь)  
4) коммут.панель (меняет местами контакты 2 букв)  
5) панель лампочек (индикатор вых.буквы)

Принцип:  
При к. нажатии клавиши правый ротор сдвиг. на 1 поз, при опр. условиях другие роторы тоже свдигаются => крипт. преобр при к. след. нажатии. + включается лампочка буквы шифротекста. (т.о. неск. замен)

**Шифры энигмы**

Пример 1:  
1. устан нач позицию роторов по коду дня (WZA)  
2. выбрать случ ключ (SXT)  
3. зашифр ключ SXT --> (UHL)  
4. став SXT как нач. позицию роторов и зашифр сообщение  
5. отпр сообщ + (WZA) и (UHL)

Расшифр:  
1. устан нач позиции роторов (WZA)  
2. расшифр UHL --> (SXT)  
3. использ SXT как нач.позицию для расшифр

Пример 2:  
1. устан нач позицию роторов по коду дня (HUA)  
2. выбрать случ код (ACF)  
3. зашифр ‘ACFACF’ (повторный код) --> ‘OPNABT’  
4. устан нач позиции роторов к 1/2 зашифр. кода (OPN)  
5. доб (OPNABT) в конец нач. сообщ  
6. зашифр всё сообщ, передать его

Расшифр:  
1. отделить первые 6 букв  
2. устан нач позицию роторов по коду дня  
3. расшифр первые 6 букв  
4. устан нач позицию роторов на 1/2 расшифр. кода  
5. расшифр сообщ (без первых 6)

Прочие (26) символы замен редкими комбинациями букв. Х ‘.’ ZZ ‘,’ FRAGE ‘?’  
Иногда исп. ряд символов нижнего алф («*принцип случайности*»)

Пример 3: (зашифр G)  
1. …….. стр 52-54 КЛАССНЫЙ ПРИМЕР

**Оценка криптостойкости**

рассм. свойства:  
\* выбор и порядок роторов  
\* разводка роторов  
\* настройка колец на к. роторе  
\* нач. положение роторов в нач. сообщ  
\* отражатель  
\* настройка коммут. панели

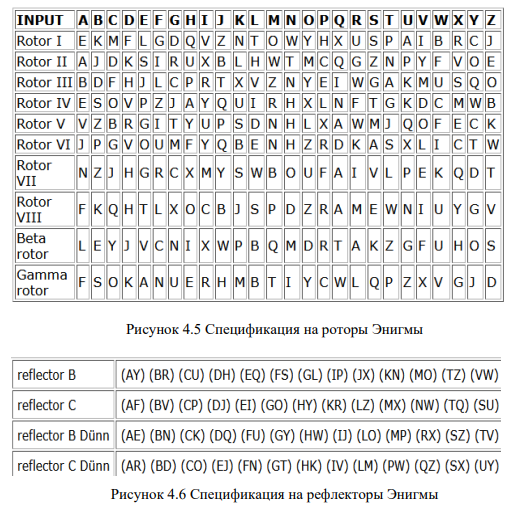
Если мы знаем всё кроме способов настройки, криптостойкость низкая. Но учитывая возм. сочетание 3 роторов и отражателя дает астроном. цифры вариантов подстановок.

**ЗАДАНИЕ (с. 57)**

1) зашифр «Чистякова Юлия Александровна» на симулятора при 8 настройках  
Сравнить частоты символов с частотами исх. текста

2) разраб прил: клава + 3 ротора + отражатель (рис 4.5 4.6)  
Типы роторов: L – VII, M – Gamma, R – II  
Тип отражателя: Re – B Dunn  
На какое число букв i перемещ соотв ротор: Li-Mi-Ri – 1-2-2

зашифр сообщ «ЧЮА» с 5 вариантами нач. установок  
+ отчет



**ВОПРОСЫ ДЛЯ КОНТРОЛЯ**

1. Дать пояснение к структуре шифровальных машин Энигма  
5 осн. блоков:  
1) клавиши (дают сигнал поворота роторов)  
2) 3+ ротора (по окружности буквы)  
3) рефлектор (контакты с левым ротором, замыкает цепь)  
4) коммут.панель (меняет местами контакты 2 букв)  
5) панель лампочек (индикатор вых.буквы)

2. На основе каких шифров строится машина Энигма?  
на основе подстановочных (динам. шифр Цезаря)

3. Дать пояснение к принципам зашифрования сообщений  
сначала буква исх. сообщ проходит через все роторы, начиная с правого. Затем шифруется рефлектором, после чего ток идет обратно и эта полученная буква вновь проходит через рефлекторы в обратном направлении.

4. Дать характеристику криптостойкости Энигмы  
5. Дать хар-ку (с числ. оценками) криптостойкости нашей машины-симулятора

Ek = f (m, B (операции комм.панели), Re (отражателя), L, M, R)  
\* выбор и порядок роторов, их разводка (коммутация)  
\* настройка колец на к. роторе, их нач. полож  
\* отражатель  
\* настройки комм. панели

Если мы знаем всё кроме способов настройки, криптостойкость низкая. Но учитывая возм. сочетание 3 роторов и отражателя дает астроном. цифры вариантов подстановок.

кажется что сложный алгоритм, но криптостойкость слабенькая, потому что в любом случае м. взломать данный алгоритм.  
Допустим, если у нас известен откр. текст, можем сделать атаку с известным откр. текстом, и у нас есть метод, кот. позволяет проигнорировать настройки коммут. панели, т.е. сократится простр-во с ключей с бескон. мн-ва до 100.000 вариантов.  
Из-за того что использ. рефлекторы, буква не мб сама в себя преобразована, и для нахожд. правильного смещения нам нужно найти такую позицию в зашифр. тексте, где ни одна из букв не дублируется с буквой открытого текста.

6. Пояснить основные принципы расшифрования сообщений Энигмы  
процедура расшифр предусм. настройку рефлектора, роторов и комм. панели в соотв. с таблицами и использ-ными при зашифровании паролями.

7. Ваши предложения по модификации известных аналогово Энигмы  
расширение роторов даст большую криптостойкость чем ввдение еще одного. М. неск алфавитов исп.

Один **ротор** мб подключен 4х106 способами. 3 рот+отраж = астрон  
Чтобы выбрать 3/5 ротора есть 60 комбинаций  
к. ротор мб устан в 1/26 положений  
т.е. с 3 роторами есть 17 576 положений (263)

**Кольцо** влияет на шаг ротора левее, к. кольцо 26 им. положений  
кольцо левого ни на что не влияет => 676 комбинаций колец (262)

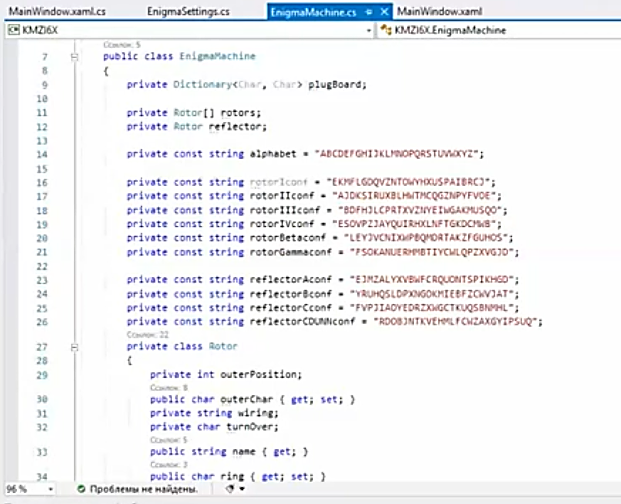
для первого кабеля **комм.панели** одна сторона м. иметь 26 полож, другая – ост. 25  
но т.к. AB=BA, игнорируем двойные числа для 1 кабеля (26\*25/(1!\*2) = 325 способов коммутации одним кабелем.  
есть 26\*25 комбинаций для первого кабеля, 24\*23 – для второго  
=> 26\*25\*24\*23 / (3!\*23)

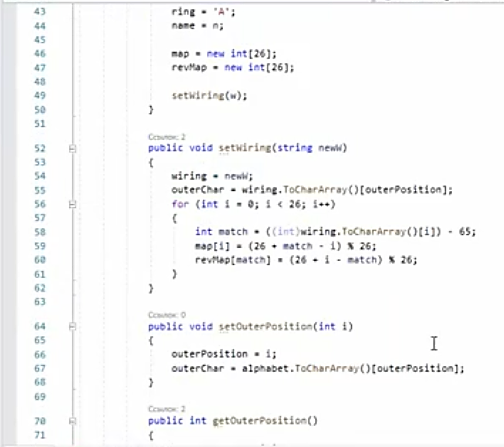
Добавление 4-го ротора почти бесполезно: он усложнил машину только в 26 раз  
внедрение 8 роторов увеличило их комбинации с 60 до 336

EnigmaSettings.cs  
сигнал поступ в коммутационную модель, результат попадает в роторы. проходит через все роторы. затем поступает на рефлектор. и возвр через роторы обратно на коммутационную панель, где выполняется последняя подстановка

сначала у нас есть дефолтные настройки нашей энигмы. дефолтное кольцо «А А А». + стартовые позиции, очередь роторов по варианту, имя рефлектора,

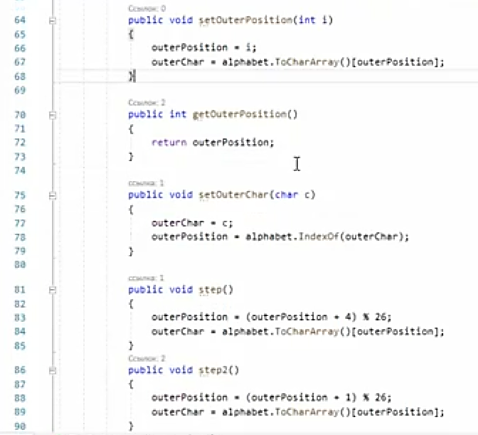
Общие настройки (EnigmaMachine):  
алфавит англ  
м. использовать любой из роторов, у меня по варику 2,3,4  
мы с картинки продублировали инфу как они будут идти (4.5) посл-сть для роторов  
рефлектор по картинке (у меня C Dune)



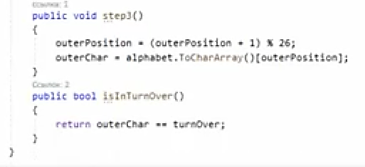


return outerPosition }

есть метод setWiring Для того чтобы устан разводку для рефлекторов. то есть wiring = здесь мы указ к-то значение, кот будет передано, переводим в массив char . И пока будет меньше 26, будем отнимать позицию 65 (первая позиция англ символа в кодировке). И дальше чтобы находить позиции, нам нужно сложить наше значение match Отнять от него i, прибавить 26, всё это по модулю 26



Дальше нужно найти выходные позиции, получить выходные символы, шаги (тоже были заданы в варианте). То есть у меня правый ротор на 4 позиции, а левый и центр на 1 поз.





дальше мы указ, как они будут двигаться, т.е. если второй ротор имеет оборот, то будет двиггаться первый и второй ротор. Если третий ротор, то будет двигаться средний ротор, а правый крайний ротор будет двигаться всегда.

public EnigmaMachine() Дальше можем посмотреть символы на кот будет поворачиваться ротор, но у нас он будет поворачиваться всегда

устан рефлектор, в завимисомти от того что мы введем, у меня А, В, С это рефлекторы, а если мы введем Д, то будет рефлектор по заданию C\_Dunn.

Дальше мы можем передавать настройки, если у нас передано кольцо и стартовая позиции, также можем передавать очередь роторов, тогда сначала устан позицию до поворота, потом новые. Аналогично если задан рефлектор, то мы сначала устанавливаем рефлектор, затем настройки для 3 параметров.

альше можем запустить Энигму: созд экземпляр StringBuilder, и для к. символа в нашем сообщении мы будем добавлять строк. представление EncryptChar[] в Encryptessage и посомтрим как оно используется. Здесь сначала мы устан позиции роторов до поворота, затем с нашей клавы надо что-то вводить, затем с пом RotorMap мы будем проходить все значения в зависимости от значения boolean (false либо в одному сторону либо в другую), получать спецификацию, отображать ее и опять проходить т.е. чтобы за- или расшифровать сообщение.

в main сначала мы проверяем, чтобы исх. собщеие на англе. Дальше устан настройки : передаем кольцо, стартовые позиции, ротор, рефлектор. Дальше передаем нек. параметры коммут. модели чтобы заменять дополнительно 2 эл-та, будем разделять их на подстроки и к. раз заново запускать машину Энигма.

**Недостатки машины:**  
кажется что сложный алгоритм, но криптостойкость слабенькая, потому что в любом случае м. взломать данный алгоритм. Допустим, если у нас известен откр. текст, можем сделать атаку с известным откр. текстом, и у нас есть метод, кот. позволяет проигнорировать настройки коммут. панели, т.е. сократится простр-во с ключей с бескон. мн-ва до буквально 100.000 вариантов, что делает наш алгоритм более уязвимым. И тогда можно посмотреть комбинации откр. закр. текст и если есть циклы, тогда его очень легко взломать, циклы: a->k, k->d, d->a, те. получается цикл akd, если есть циклы, он легко взламывается, поэтому рекомендуется использ неск. циклов и также м. легко взломать по известному шифротексту, ибо из-за того что использ. рефлекторы, буква не мб сама в себя преобразована, и для нахожд. правильного смещения нам нужно найти такую позицию в зашифр. тексте, где ни одна из букв не дублируется с буквой открытого текста.