**2.2.6 Enigma**

**A53 \* 263\* (C2620 \* A2010 / 210 + C2618 \* A189 / 29 + …**

**C262 \* A21 / 21 + 1)**

**10对字母在接线板上的组合=C2620 \* (A2010 / 210)**

**ABCD中抽取2对字母的组合如下:**

**AB CD; AC BD; AD BC**

**齿轮内部的设置称为ring setting**

**外部的设置称为message key**

**如何把MessageKey传递给对方?**

**发送方随机想出3个齿轮的外部状态(MessageKey)为: ABC**

**以明文的形式把ABC发送给对方;**

**再想出今天要用到密钥即真正用来加密的齿轮初始状态为:**

**ZJU**

**在当前齿轮初始状态为ABC的情况下，连续按下ZJU得到**

**ZJU的密文设为Z'J'U'发送给对方。**

**对方在齿轮初始状态为ABC的情况下，输入Z'J'U'一定可以解密出ZJU。**

**即下去双方都把齿轮的初始状态设为ZJU，然后就可以开始正式通讯。**

**注意, 当按下某个键时, 对该键进行加密的密钥并非当前齿轮的状态，而是齿轮转了一下以后的状态。例如: 设3个齿轮从左到右分别为III, II, I, 并且齿轮的状态从左到右为AAZ, 则输入字母A时，齿轮转到AAA的位置，此时AAA就是密钥。**

**加密后得到的密文为N。**

**Ring Setting是齿轮内部的初始状态，它们在齿轮转动时不会发生变化。而齿轮外部的状态MessageKey是会随每一次按键而发生变化的。**

**设I号齿轮的RingSetting=B, MessageKey=D, 则**

**Δ=MessageKey-RingSetting='D'-'B'=2**

**现在假定输入字母A，则A进入I号齿轮时，需要先加上Δ即变成A+2='C', 查表:'C'🡪'M', 而从I号齿轮出去时要减去Δ，即'M'-2='K'。**

**RingSetting: III=A, II=A, I=B**

**MessageKey: III=A, II=A, I=C**

**敲键A后MessageKey变成: III=A, II=A, I=D**

**从II号齿轮返回到I号齿轮时，进入I号齿轮的字母为G**

**此时G+Δ=G+2=I, I反查表得V, V-Δ=V-2=T, 最终T就是密文。**

**接线板只在从右到左进入最右侧那个齿轮以及**

**从左到右从最右侧齿轮出来亮灯的时候才起作用。**

**Enigma模拟软件(http://10.71.45.100/bhh/enigma.rar)**

**加密过程要经过5个元件:**

**假定明文为A**

**1. plugboard**

**假定接线板设置为:A-B, C-D**

**char plug[27] ="BADCEFGHIJKLMNOPQRSTUVWXYZ";**

**/\*ABCDEFGHIJKLMNOPQRSTUVWXYZ\*/**

**char c='A', e;**

**e = plug[c-'A']; // e='B';**

**A🡪B**

**2. rotor I**

**char rotor[27]="EKMFLGDQVZNTOWYHXUSPAIBRCJ";**

// ABCDEFGHIJKLMNOPQRSTUVWXYZ

**char c='B', e;**

**e = rotor[c-'A']; // e='K';**

**B🡪K**

**3. rotor II**

**AJDKSIRUXBLHWTMCQGZNPYFVOE**

**ABCDEFGHIJKLMNOPQRSTUVWXYZ**

**K🡪L**

**4. rotor III**

**BDFHJLCPRTXVZNYEIWGAKMUSQO**

**ABCDEFGHIJKLMNOPQRSTUVWXYZ**

**L🡪V**

**5. reflector**

**char reflector[27]=**

**" YRUHQSLDPXNGOKMIEBFZCWVJAT";**

**// ABCDEFGHIJKLMNOPQRSTUVWXYZ**

**V🡪W**

**经过上述5步, A转成W, 但W还不是密文, 接下去还要走一条逆向路径:4-3-2-1, 把W进一步转化成密文, 步骤如下:**

**4. rotor III**

**char rotor[27]="BDFHJLCPRTXVZNYEIWGAKMUSQO";**

**// ABCDEFGHIJKLMNOPQRSTUVWXYZ**

**W🡪R**

**注意按逆向路径经过3个齿轮时要反查表, 即在数组rotor中寻找元素'W', 得到该元素的下标设为i, 再把i+'A',就得到'R'。**

**3. rotor II**

**AJDKSIRUXBLHWTMCQGZNPYFVOE**

**ABCDEFGHIJKLMNOPQRSTUVWXYZ**

**R🡪G**

**2. rotor I**

**EKMFLGDQVZNTOWYHXUSPAIBRCJ**

**ABCDEFGHIJKLMNOPQRSTUVWXYZ**

**G🡪F**

**1. plugboard**

**BADCEFGHIJKLMNOPQRSTUVWXYZ**

**ABCDEFGHIJKLMNOPQRSTUVWXYZ**

**F🡪F**

**注意接线板查表既可以正向查,也可以反向查,结果是一样的。**

**经过上述4步, W转成F, 其中F就是密文。**

**各位可以尝试把F当作明文重新把前面的9步走一遍,最后出来的一定是A, 这就实现了解密。**

**要注意在Enigma模拟器中, 除了把3个齿轮按从左到右顺序设成III、II、I外，还需要把MessageKey设成01 01 26即AAZ，因为Enigma是先转动齿轮再查表的，当你敲A键时，齿轮I会从26转到1。**

**另外还有两个齿轮在上面的例子中没有用到，现列出它们的转化表。**

**齿轮IV的转换表如下所示:**

**ESOVPZJAYQUIRHXLNFTGKDCMWB**

##### ABCDEFGHIJKLMNOPQRSTUVWXYZ

**齿轮V的转换表如下所示:**

**VZBRGITYUPSDNHLXAWMJQOFECK**

**ABCDEFGHIJKLMNOPQRSTUVWXYZ**

**5个齿轮使下一个齿轮发生跳转的字母:**

**QEVJZ; 齿轮的当前位置,从左到右对应齿轮I II III IV V**

**RFWKA; 齿轮的下一步位置**

**; Royal Flags Wave Kings Above**

**假定3个齿轮为III、II、I, 齿轮I的当前位置=Q且II的当前位置=A, 现在敲任何一个键，都会使I转到R这个位置, 此时I会带动II旋转, 于是II会从A转到B。**

**另外, 还要注意一个double stepping现象:**

**假定III=1=A, II=4=D, I=17=Q**

**现在I旋转，从Q变成R，一定会带动II旋转:**

**III=1=A, II=5=E, I=18=R**

**此时再旋转I的话，I本来是不应该带动II转的(因为当前I不在Q这个位置), 但是II还会再转(double stepping)，**

**同时II带动III旋转:**

**III=2=B, II=6=F, I=19=S**

**归纳起来讲, II有两种情况会转动:**

**(1) I从Q转到R**

**(2) II当前在E位置, I不管在什么位置**

**double stepping是由Enigma的机械结构决定的，该现象只会出现在中间那个齿轮上。**

**每个齿轮有一个内部设置叫ring setting:**

**假定I齿轮的RingSetting=B(内部),**

**MessageKey=A(外部)**

**现在按键盘A的时候, A进入I齿轮后, 要做以下运算:**

**char c = 'A';**

**int delta = MessageKey-RingSetting;**

**c = ((c-'A')+delta+26)%26 + 'A';**

**此时c='Z';**

**接下去拿c去查齿轮I的表得J**

**现在J要出去的时候，还得减去delta，即:**

**c = c-delta; 即c=K**

**所以从齿轮I出来的字母就是K。另外两个齿轮的处理跟I一样。**

**从III到II到I逆向走回来的时候，同样，**

**从左到右进入要加delta，右边出来要减delta。**

**假定I的RingSetting=C, MessageKey=A**

**现在按A，此时MessageKey=B**

**A-1🡺Z 查表得J J+1🡺K**

**反射板 🡨 D 🡨 C 🡨 B \_🡨 A**

**|**

**X ?🡪 C 🡪 B 🡪 A**