

Breaking the Vigenère Cipher

Known Language and Key Length

Breaking Vigenère

Dqf, axa jjbl wua xtsa rlcatlf zv kxlct ajn
"wwhygjghduk ervoga" (jy kc dcb jcurlf ou cnl 1800b),
kaa qgcg gsux sgjxugm zq sbeq hdxaa JxychRpucy,
QgzjVgwu, hpm wtxmycvsppp. 0 dnz axa ejt'v
chkc mqa Jqdxzg 4!

- Step 1:
 - Known Language
 - Known Key Length

Breaking Vigenère

Dqf, axa jjbl wua xtsa rlcattf zv kxlct ajn
"wwhygjghduk ervoga" (jy kc dcb jcurlf ou cnl 1800b),
kaa qgcg gsux sgjxugm zq sbeq hdxaa JxychRpucy,
QgzjVgwu, hpm wtxmycvsppp. 0 dnz axa ejt'v
chkc mqa Jqdxzg 4!

CaesarCracker

CaesarCracker

CaesarCracker

CaesarCracker

Breaking Vigenère

qf, axa jjb wu xt a r cat f z kx ct jn
wwh gjq duk erv ga" (jy kc cb cur f o cn 18 0b)
ka qq g g ux gjx gm q s eq dxa Jx chR ucy
Qg jVg u, pm txm cvs pp. 0 dnz axa ejt v
c kc qa qdx g 4

CaesarCracker

CaesarCracker

CaesarCracker

CaesarCracker

7

Breaking Vigenère

CaesarCracker

7

CaesarCracker

2

CaesarCracker

9

CaesarCracker

6

What You Need to Write

```
public String sliceString(String message, int whichSlice, int totalSlices)
```

```
Dqf, axa jjbl wua xtsa rlcattlf zv kxltc ajn  
"wwhygjghduk ervoga" (jy kc dcb jcurlf ou cnl 1800b),  
kaa qgcg gsux sgjxugm zq sbeq hdxaa JxychRpucy,  
QgzjVgwu, hpm wtxmycvsppp. 0 dnz axa ejt'v  
chkc mqa Jqdxzg 4!
```

- Write a method to “slice” the String
 - Pulls out the characters from same shift

What You Need to Write

```
public String sliceString(String message, int whichSlice, int totalSlices)
```

```
Dqf, axa jjbl wua xtsa r1catlf zv kx1ct ajn  
"wwhygjqhduk ervoga" (jy kc dcb jcurlf ou cn1 1800b),  
kaa qgcg gsux sgjxugm zq sbeq hdxaa JxychRpucy,  
QgzjVgwu, hpm wtxmycvppp. 0 dnz axa ejt'v  
chkc mqa Jqdxzg 4!
```

whichSlice = 0

- Write a method to “slice” the String
 - Pulls out the characters from same shift

```
D lasllvla"yh o djlu10,acssuzbhayp,zwhwyp'hmJz!
```

What You Need to Write

```
public String sliceString(String message, int whichSlice, int totalSlices)
```

```
Dqf, axa jjbl wua xtsa rlcatl f zv kxlc t ajn  
"wwhygj qhduk ervoga" (jy kc dcb jcurl f ou cnl 1800b),  
kaa qgcg gsux sgjxugm zq sbeq hdxaa JxychRpucy,  
QgzjVgwu, hpm wtxmycvsp pp. 0 dnz axa ejt'v  
chkc mqa Jqdxzg 4!
```

whichSlice = 1

- Write a method to “slice” the String
 - Pulls out the characters from same shift

```
qaj acf cjpgdeg(kccf 0  
guggqed cu  
juptcp daevkqqg
```


What You Need to Write

```
public String sliceString(String message, int whichSlice, int totalSlices)
```

```
Dqf, axa jjbl wua xtsa rlcattlf zv kxlc t ajn  
"wwhygj qhduk ervoga" (jy kc dcb jcurlf ou cnl 1800b),  
kaa qgcg gsux sgjxugm zq sbeq hdxaa JxychRpucy,  
QgzjVgwu, hpm wt xmycvsp pp. 0 dnz axa ejt'v  
chkc mqa Jqdxzg 4!
```

whichSlice = 2

- Write a method to “slice” the String
 - Pulls out the characters from same shift

```
fxjwx a ktnwjura jcbu c1bkq xjm qxJhcQV,mxvp nxj  
cad
```

What You Need to Write

```
public String sliceString(String message, int whichSlice, int totalSlices)
```

```
Dqf, axa jjbl wua xtsa rlcattlf zv kxlcct ajn  
"wwhygjghduk ervoga" (jy kc dcb jcurlf ou cnl 1800b),  
kaa qgcg gsux sgjxugm zq sbeq hdxaa JxychRpucy,  
QgzjVgwu, hpm wtxmycvppp.    O dnz axa ejt'v  
chkc mqa Jqdxzg 4!
```

whichSlice = 3

- Write a method to “slice” the String
 - Pulls out the characters from same shift

```
,abutrtzx
```

```
hqkv"y ron8)agg x saxRygg ms.Ozadc x4
```

Advice on `sliceString`

- Advice on writing `sliceString`
 - Remember `StringBuilder`

Advice on sliceString

```
for (int i = 4; i < 30; i += 7) {  
    System.out.println(i);  
}
```

- Advice on writing sliceString
 - Remember StringBuilder
 - Counting for loops can...
 - Start at any number

Advice on sliceString

```
for (int i = 4; i < 30; i += 7) {  
    System.out.println(i);  
}
```

- Advice on writing sliceString
 - Remember StringBuilder
 - Counting for loops can...
 - Start at any number
 - Count by any number

What You Need to Write

```
public int[] tryKeyLength(String encrypted, int klength, char mostCommon)
```

- Find key for `encrypted` for given `klength`
- `mostCommon`: most frequent letter ('e')
 - For later: different languages
- Use `sliceString`
- And `CaesarCracker`
 - `int getKey(String encrypted)`
 - Constructor takes `mostCommon`
- Return key as `int[]` (array of shifts)

What You Need to Write

`public void breakVigenere ()`

- Method to call from BlueJ
- Use `FileResource` to read file
 - Useful: `.asString()`
- Use `tryKeyLength` to break key
 - For now, `keyLength` given, `mostCommon = 'e'`
- Use `VigenereCipher's .decrypt(String)`
- Print decrypted message