Answers to Exercises Huanjie Guo ID： 10 655 496

Week 1

Q1 the table expression, marked (1) above, that defines the behaviour of the one-rotor machine, and its output;

Here we input a letter then it pass through the rotor to the reflector, after that, it was reflected to the rotor again and then produce the output.

```
Table[Replace[Replace[Replace[x, RotI], RefB], RotIinv], {x, 1, 26, 1}]
{8, 11, 13, 19, 6, 5, 16, 1, 14, 12, 2, 10,
 3, 9, 21, 7, 26, 25, 4, 22, 15, 20, 24, 23, 18, 17}
```

Q2 the list of pairs swapped by the one-rotor machine, as revealed in the preceding output (write a list of pairs);

{{1,8}, {2,11}, {3,13}, {4,19}, {5,6}, {7,16}, {9,14}, {10,12}, {15,21}, {17,26}, {18,25},{20,22}, {23,24}}

Q3 the EnigmaGuts permutation derived from the preceding output (write it out as a permutation);

```
EnigmaGuts = {1 → 8, 2 → 11, 3 → 13, 4 → 19, 5 → 6, 6 → 5, 7 → 16, 8 → 1,
   9 → 14, 10 → 12, 11 → 2, 12 → 10, 13 → 3, 14 → 9, 15 → 21, 16 → 7, 17 → 26,
   18 → 25, 19 → 4, 20 → 22, 21 → 15, 22 → 20, 23 → 24, 24 → 23, 25 → 18, 26 → 17}
```

Q4 the table expression, marked (2) above, and its output;

mapping the output of 1 to 26

```
Table[ReplaceAll[x, EnigmaGuts], {x, 1, 26, 1}]
{8, 11, 13, 19, 6, 5, 16, 1, 14, 12, 2, 10,
 3, 9, 21, 7, 26, 25, 4, 22, 15, 20, 24, 23, 18, 17}
```

Q5 the table expression, marked (3) above, and its output;

input a for 26 times, and shows all its outputs.

```
Table[Enigma1[1, n], {n, 0, 25, 1}]
{8, 10, 11, 16, 2, 26, 10, 20, 6, 3, 18,
 25, 17, 22, 7, 18, 10, 8, 12, 3, 21, 25, 2, 26, 20, 18}
```

Q6 the MapThread expression and its output.

In[1]:=MapThread[f, {{a, b, c}, {x, y, z}}]
Out[1]= {f[a,x],f[b,y],f[c,z]}

actually here we use MapThread to map each x with the specific n, which can make the output always equal 1.

```
MapThread[Enigma1, {Table[Enigma1[1, n], {n, 0, 25, 1}], Table[n, {n, 0, 25, 1}]}]
{1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1}
```

Week 2

Q1 the definition of EnigmaMachine;

```
EnigmaMachine[text_, key_] :=
 MapThread[Enigma1, {text, Table[n, {n, key, key + Length[text] - 1, 1}]}]
```

Q2 the evaluations of EnigmaMachine[{1,2,3,4,5},28] and of EnigmaMachine[EnigmaMachine[{1,2,3,4,5},28],28] ;

get the ciphertext

```
EnigmaMachine[{1, 2, 3, 4, 5}, 28]
{11, 3, 12, 9, 22}
```

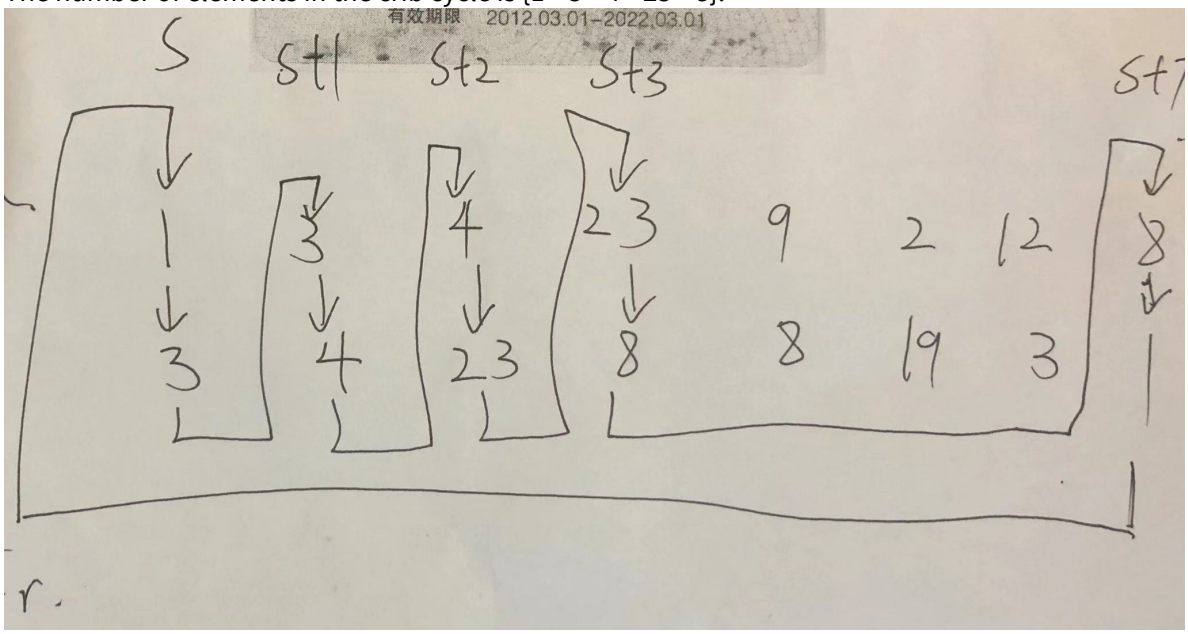
get the plaintext itself (encrypt -> decrypt)

```
EnigmaMachine[EnigmaMachine[{1, 2, 3, 4, 5}, 28], 28]
{1, 2, 3, 4, 5}
```

Q3 the location of the start of the crib (within the plaintext), and the number of elements in the crib cycle;

The start of the crib within the plaintext is plaintext[[1]] -> 1.

The number of elements in the crib cycle is {1->3->4->23->8}.



Q4 the distances of the members of the crib cycle from the start of the plaintext;

{1 -> 0, 3 -> 1, 4 -> 2, 23 -> 3, 8->7}

Q5 the key setting revealed by the Bombe for the start of the cribbed plaintext, and the Bombe expression;

```
Table[
 Table[
  Bombe[plaintext, Table[ciphertext[[n]], {n, s, Length[ciphertext], 1}], k]
  , {k, 0, 25, 1}],
 {s, 1, Length[ciphertext] - Length[cyfrag], 1}
]
```

```
{{{no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no},
   {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}},
  {{no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no},
   {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}},
  {{no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no},
   {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}},
  {{no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no},
   {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}},
  {{no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no},
   {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}},
  {{no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no},
   {no}, {no}, {no}, {no}, {no}, {YES!!!, 19}, {no}, {no}, {no}, {no}, {no}, {no}},
  {{no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no},
   {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}},
  {{no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no},
   {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}},
  {{no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no},
   {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}},
  {{no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no},
   {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}},
  {{no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no},
   {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}},
  {{no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no},
   {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}},
  {{no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no},
   {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}},
  {{no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no},
   {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}},
  {{no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no},
   {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}},
  {{no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no},
   {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}},
  {{no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no},
   {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}},
  {{no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no},
   {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}},
  {{no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no},
   {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}, {no}}}
```

key setting for the start of the cribbed plaintext: 19

```
Bombe[plain_, cyfrag_, k_] := If[
      Enigma1[plain[[1]], k] == cyfrag[[1]] && cyfrag[[1]] == plain[[1 + 1]]
   && Enigma1[plain[[1 + 1]], k + 1] == cyfrag[[1 + 1]] &&
   cyfrag[[1 + 1]] == plain[[1 + 2]]
 && Enigma1[plain[[1 + 2]], k + 2] == cyfrag[[1 + 2]] &&
   cyfrag[[1 + 2]] == plain[[1 + 3]]
 && Enigma1[plain[[1 + 3]], k + 3] == cyfrag[[1 + 3]] &&
   cyfrag[[1 + 3]] == plain[[1 + 7]]
   && Enigma1[plain[[1 + 7]], k + 7] == cyfrag[[1 + 7]] && cyfrag[[1 + 7]] == plain[[1 ]]
  , {"YES!!!", k}, {"no"}]
```

Q6 the key setting for the start of the whole cyphertext;
the start of the first letter of cribing cycle in cyphertext is the 6th, and its key is 19. So we need to subtract 5 and get the key of the first letter in the whole cyphertext.
19-5 = 14
the key setting for the start of the whole cyphertext: 14

Q7 the decryption of the whole cyphertext.

```
EnigmaMachine[ciphertext, 14]
```

```
{18, 15, 3, 7, 22, 1, 3, 4, 23, 9, 2, 12, 8, 17, 21, 6, 8, 3, 9}
```

Week 3

Week 4

Week 5