

Answers to Exercises JiachengLI 10 307 457

Week 1

Q1:

Expression: `Table[Replace[Replace[Replace[x, Rotl], RefB], Rotlinv], {x, 1, 26, 1}]`

Output: `{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:

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:

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:

Expression: `Table[ReplaceAll[x, EnigmaGuts], {x, 1, 26, 1}]`

Output: `{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:

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

Output: `{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:

Expression: `MapThread[Enigma1, {{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}, {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25}}]`

Output: `{1, 1}`

Week 2

Q1:

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

Q2:

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

Output: `{11, 3, 12, 9, 22}`

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

Output: `{1, 2, 3, 4, 5}`

Q3:

Location: `{17, 4, 14, 6, 17, 3, 4, 23, 8, 8, 19, 3, 1, 24, 22, 11, 6, 22, 15}`

`{1, 3, 4, 23, 9, 2, 12, 8}`

↑

Number of the elements: 5

Q4:

s	s + 1	s + 2	s + 3	s + 4	s + 5	s + 6	s + 7	s + 8
1	3	4	23	□	□	□	8	□
3	4	23	8	□	□	□	1	□

Distance: 7

Q5:

Key: 19 for the start of the cribbed plaintext.

Bombe Expression:

```
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:

Key:14 for the start of the whole cyphertext.

Q7:

Expression:

```
EnigmaMachine[{17,4,14,6,17,3,4,23,8,8,19,3,1,24,22,11,6,22,15},14]
```

Output:

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

Decryption:

```
rocgvacdwiblhqufhci
```

Week 3

Week 4

Week 5