

# Notebook 4.5 — Wiring a Bombe for a Crib

## 4.5.1 Make a Message

```
from Substitution import Enigma

plugboard_settings = 'KL IT FQ HY XC NP VZ JB SE OG'
reflector_type = 'UKW-B'
scrambler_wheel_types = 'IV V I'
ring_settings = 'UOP'
enigma_machine = Enigma(plugboard_settings, reflector_type, scrambler_wheel_types, ring_settings)
enigma_machine.set_indicators('CIL') # Let's do a Cilly
plain_text = 'CILLYIMISSYOU SOMUCHIWANTTOCOMEHOME'
expected_cipher_text = 'RXFCUHEPBFAHUQCZSNTRQFHYDOGIGVHCX'
cipher_text = ''
for c in plain_text:
    cipher_text += enigma_machine.substitute(c)

print(expected_cipher_text)
print(cipher_text)
```

```
RXFCUHEPBFAHUQCZSNTRQFHYDOGIGVHCX
RXFCUHEPBFAHUQCZSNTRQFHYDOGIGVHCX
```

## 4.5.2 Find the Longest Chain in the Crib

Following the method of p.76 of the Hut Six Story, we will use the first 13 letters as our crib.

```
1111
1234567890123
CILLYIMISSYOU
RXFCUHEPBFAH
```

The longest chain in this crib has 10 letters, 9 links, and 0 loops:

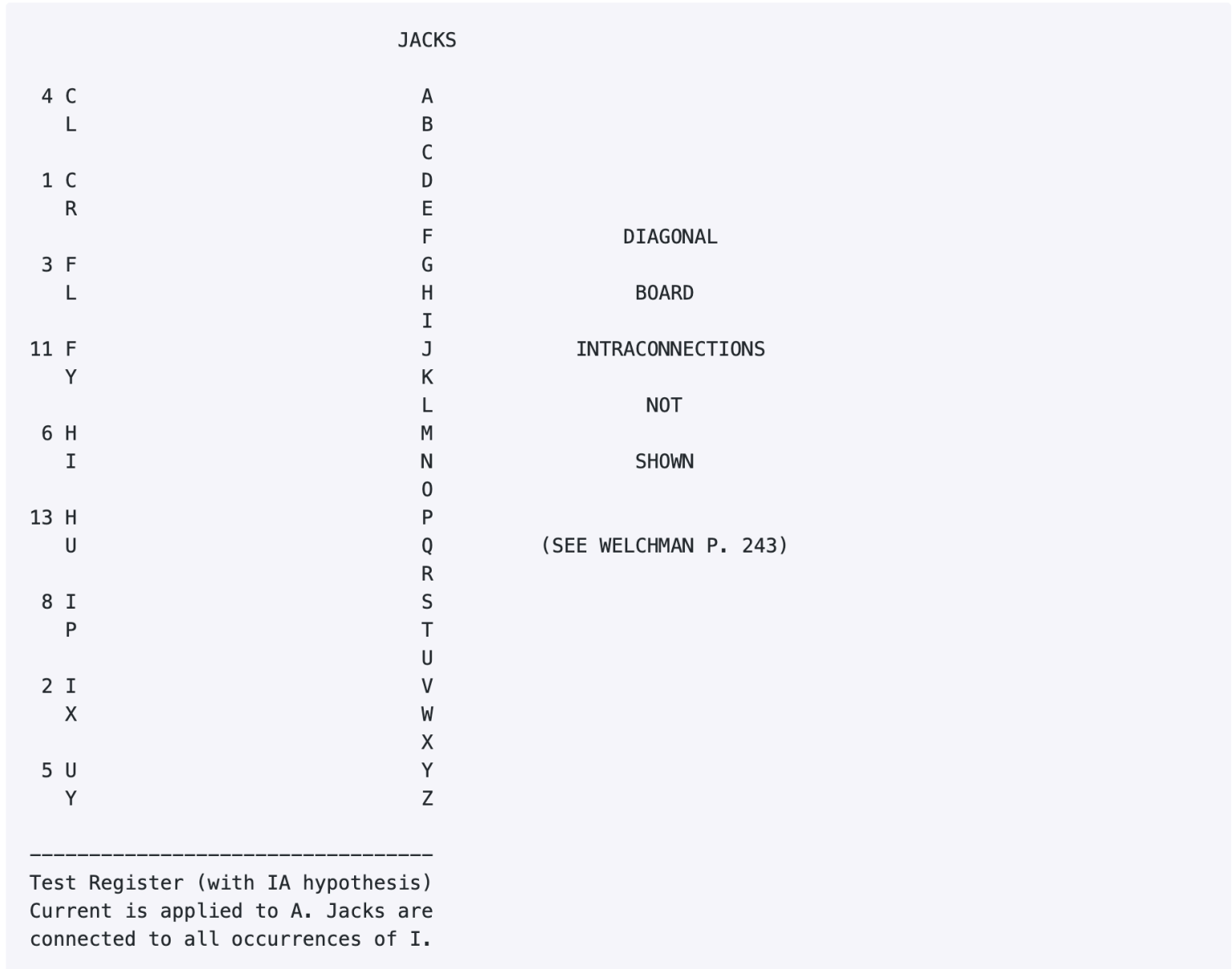
```
P--8--I--6--H-13--U--5--Y-11--F--3--L--4--C--1--R
|
2
|
X
```

List the links to be used when setting up the bombs (notice that Welchman alphabetizes them which will make it easier to draw the wiring diagram possibly for the bombe operator to connect the cables to the diagonal board jacks):

```
4 CL
1 CR
3 FL
11 FY
6 HI
13 HU
8 IP
2 IX
5 UY
```

### 4.5.3 Wire the Bombes

Following the method on p. 241, we make a hypothesis: could I be steckered to A? We set up 9 scramblers representing each of the links, and we need to make the jack connections for all 10 letters that are involved: CLRFYHIUPXY. The diagram will come out tidy like Welchman's if we process the letters in the order that they first appear reading from top to bottom:



### 4.5.4 Consistency or Rejection of the Hypothesis

It is not important that IA is part of the hypothesis. It could have been IB or IC. If IA is part of the hypothesis, it will be the case that current coming in on A should come out on exactly one other letter in the test register. In general it will come out on many other letters of the test register, because of the the diagonal board intraconnections.

If it does come out on exactly one other connection, the wheel ordering being tried and the indicator settings that the machine found are a possibility for the days code. The machine tries all 26x26x26 indicator settings in about 12 to 15 minutes (depending on the speed of the operator). Usually no consistent indicator setting is found, and one of the other 60 wheel orderings must be tried. All wheel orderings can be tried in 12 to 15 hours.