

- 2. i) 20. the overtick needle on rotor I, in the rightmost slot, is between Q and R, and the rotor is initially in position X, so we need 20 clicks before this needle arrives at the top position.
- ii) If your name's first 3 letters are ZYX, the ciphertext is BPIOWFIWPFHFYDSN.
- iii) If your name's first 3 letters are ZYX, the ciphertext is AJIODEIWPEPEYOSC.
- iv) In this example, the ciphertext character is the same in both cases if and only if neither the plaintext character nor the unplugged ciphertext is one of the letters involved in the cabling.

```
wettervorhersage
BPIOWFIWPFHFYDSN
AJIODEIWPEPEYOSC
--  --  ---  - -
```

v) Users were supposed to choose settings randomly, so using anything predictable or commonly repeated, such as a person's initials, would make cracking easier. The Bletchley Park crowd referred to such a choice as a *cilly*.

- 3. i) HCTZVQ ZANKAF YWQXBH

```
* 1-4 Mapping
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
J W Q T N E Y Z V B M R U H G I F S L A C P O D X K
* Cycles
A J B W O G Y X D T 10
C Q F E N H Z K M U 10
I V P 3
L R S 3
* Fingerprint 3 3 10 10
```

```
* 2-5 Mapping
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A U V F J I Z S W P L X O D K G C T E Q N R B M Y H
* Cycles
A 1
B U N D F I W 7
C V R T Q 5
E J P G Z A S 7
K L X M O 5
Y 1
* Fingerprint 1 1 5 5 7 7
```

```

* 3-5 Mapping
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
D W A G R U S K T J Y M I F O V H L N Q Z P B C E X
* Cycles
A D G S N F U Z X C 10
B W 2
E R L M I T Q H K Y 10
J 1
O 1
P V 2
* Fingerprint
1 1 2 2 10 10

```

4. i) text mentions confederates, who lost. other sources mention union side as well, but you need to cite a reference to get credit if you give an answer not in text
 ii) each is a 26-letter monoalphabetic substitution cipher, so equally hard to break

5. i) $k_0 \approx 1.058e16$. see text or webnotes.

ii) there are $4*3*2=24$ ways to place 4 rotors in 3 slots (4 choices for rotor to put in 1st slot, leaving 3 choices for next, 2 for next). there are $26*26*26$ ways to choose initial rotor position. there are $(26 \text{ choose } 10) = \frac{26!}{10! 16!} = 5311735$ ways to select the 10 letters used in the cabling; then there are $9*7*5*3 = 945$ ways to pair those 10 letters. so $k_1 = 24 * 17576 * 5311735 * 945 \approx 2.1e15$. so $k_1/k_0 \approx .2$.

Let k_1 be the number of keys of the Enigma with of the Enigma with 3 slots, 4 rotors, and 5 plugboard cables (so 10 plugs). Give the ratio of k_1/k_0 . Explain briefly.

iii) false. large number of keys is necessary but not sufficient to provide security. as we saw in the text, there are Enigma cracking methods that reduce the search space by virtually eliminating the plugboard

6. i) see the text
 ii) see the text

Now we see that ctxt F (no further changes) should map to R in *erwarte*, but it maps to U, so try cabling U and R. This works!

```
LZJPQFHMFJCOWBPREDTNBUZUCMUCMMRMQN   ctxt
LXXXXECNYRTEFZHHELSNAETIAENNTAEBBUNI
?????ERWARTEROMMELSPAETDIENSTAG?????   final correct ptxt (with cables)
      +                                     ur cabling ok
```

now we see that there are two locations where we want M but we have H: maybe H and M are cabled? this works!

```
LZJPQFHMFJCOWBPREDTNBUZUCMUCMMRMQN   ctxt
LXXXXERWARTEFZMMELSPAETIAENSTAGABENI
?????ERWARTEROMMELSPAETDIENSTAG?????   final correct ptxt (with cables)
```

now we have enough to guess the last word (abend) and the first word (all x). so there are two locations where we want D but have I: maybe DI are cabled. also, notice from *rommel* that we want O but get Z. if we try these two cablings we get the correct message, cabling AF DI HM OZ UR

Finally, you were asked to find 6 cable pairs. what other letters can be cabled, but not change the current ptxt? Not any letter that appears in the ctxt or ptxt. This leaves three letters: K,V,Y. So the final cabling is either KV, KY, or VY.