# Stage 2: The Enigma Machine

Contact Keith (@akyholicx) or Jon (@agxhv) for assistance if you face any issues!
(or require hints/test cases to verify your code :P)

**The plot thickens...**

Congratulations on getting past Stage 1! You have been awarded the top scoring candidate for the recruitment challenge and now you have to report to work at Bletchley Park by Alan Turing. He finds it incredibly hard to believe that anyone from this era would be able to solve this challenge so quickly. With the recent surge in unknown future technology arriving at Bletchley Park, Alan becomes suspicious that you are not from his time. Therefore, he does a thorough check on your background, using MI6 resources and intel, and is now aware that you possess great knowledge on how to operate 21st century electronics.

He now wants you to embark on a top secret project where you need to decrypt a highly classified letter that was sent by the German Military. MI6 has warned that this letter highlights the Nazi's master plan to invade present day Nations by exploiting the Time Paradox.

At this point, all we can be certain about the message is that it starts with the string "fcs23{". Sounds like the Germans are indeed aware about the year 2023. You think to yourself: "What in the world is fcs23? Future Colonial Superiority?"

Luckily, the almighty Alan Turing has been hard at work and he has reverse engineered how the Germans encrypt their documents. Apparently, they have also upgraded their systems as a result of the Time Paradox, and they have recently manufactured a super powerful Enigma machine which has a character set of 94 characters! Who knows what other technologies they might possess? You wonder if they also possess a time machine, or if they are simply getting these futuristic tools for free due to the paradox. You regret messing around with time but it is crucial that you help to decrypt this letter.

Alan Turing tells you to stop daydreaming and he hands you a document that he has prepared for you regarding his hard work.

**What is an Enigma machine?**

It is a mechanical encryption device used by the Nazis in WWII to encrypt or decrypt coded messages, which at the time was believed to be unbreakable. However, Alan Turing, alongside other researchers, identified and exploited the weaknesses in the implementation of the enigma machine, and designed a machine called the Bombe machine to crack the enigma cipher. (you could continue watching the stream to learn more).

Enigma machines use a form of polyalphabetic substitution cipher, but the tricky thing is that after each button press, another substitution is generated, so an input of "AA" could be encoded into "EJ".

**How does it work?**

Employing a system of rotating disks (rotors, also known as wheels) that change the substitution pattern for each letter press in the message. When a key is pressed, an electrical signal is sent through the rotors, a reflector, and possibly a plugboard, resulting in an ever-changing substitution. The strength of the Enigma cipher comes from the large key space owing to the different rotor types and permutations, their initial positions, and optional features like the ring and plugboard settings, making it challenging to crack without knowing the exact configuration.

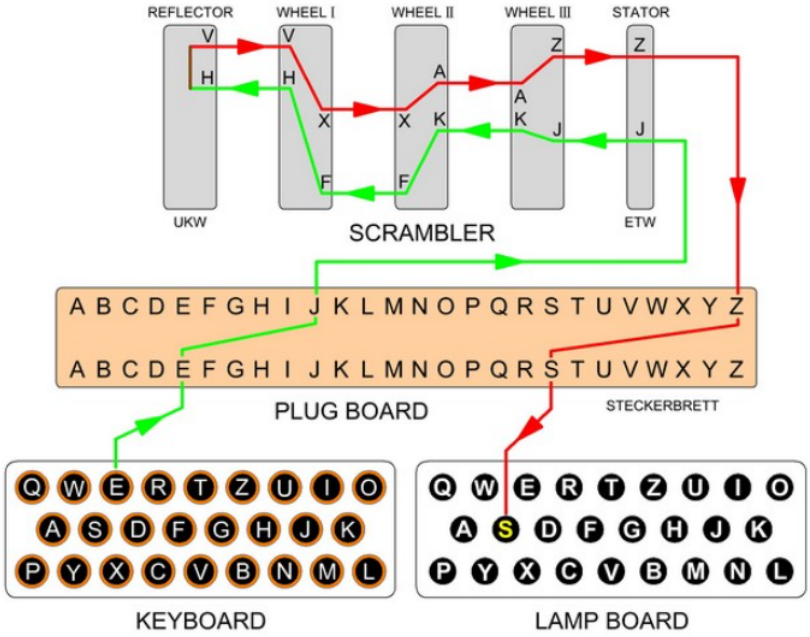



**Figure 1: Simplified Schematic of the Enigma Machine**

The Enigma Machine runs electrically and is connected to a battery. In Fig 1, a simplified schematic of the Enigma Machine is shown. When a user presses down on a key on the keyboard, it would create a closed circuit with the lamp representing the encrypted letter on the lamp board.

To briefly explain the inner workings of the Enigma Machine, let's imagine a user depresses the letter 'E'. Immediately following the keypress, the fast (rightmost) rotor will rotate by one step. Each rotor has a notch position, which determines when to rotate the subsequent rotor. The mechanism is similar to a counter or a vehicle odometer. (with some anomalies like double stepping of the middle rotor)

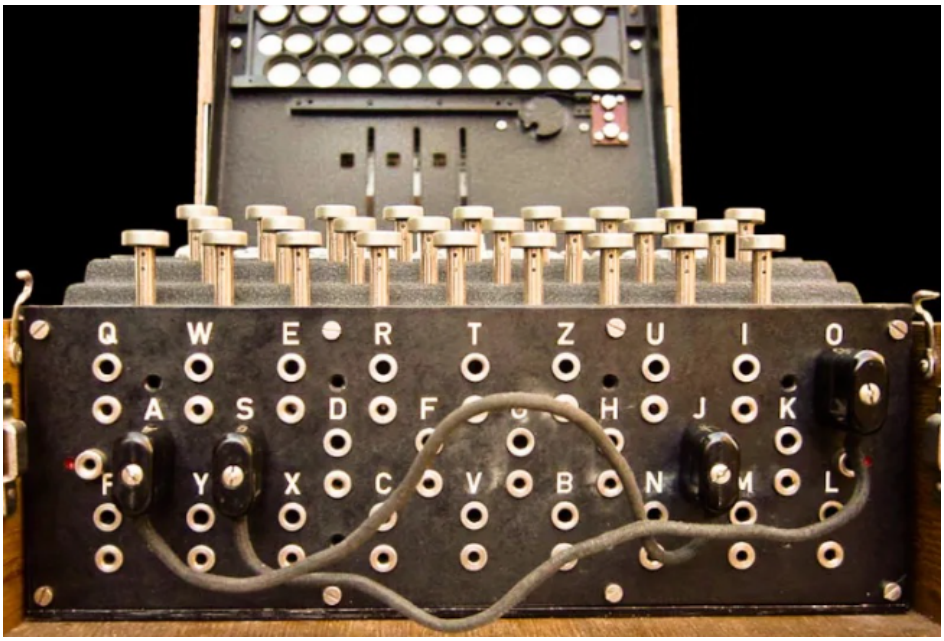


**Figure 2: Enigma Plugboard**

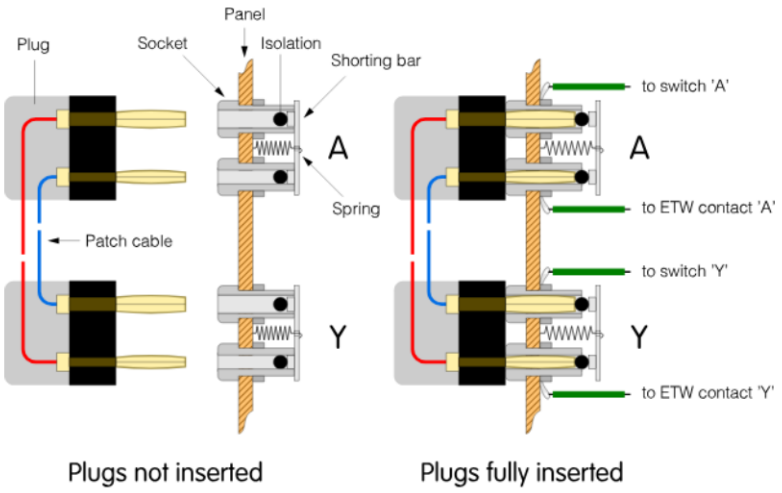



**Figure 3: Plugboard Terminal Mechanism**

Next, the electrical connections are made. The plugboard would map the letter 'E' to a letter 'J'. In this stage, it is paramount to understand the mechanism of the plugboard switches. The plugboard works by connecting cable between a pair of terminals on the board. That is, one can connect terminal 'E' to terminal 'J' with a single plugboard cable. This would map letter 'E' to letter 'J'. One can also leave the terminals unconnected, resulting in the letter mapping back to itself.

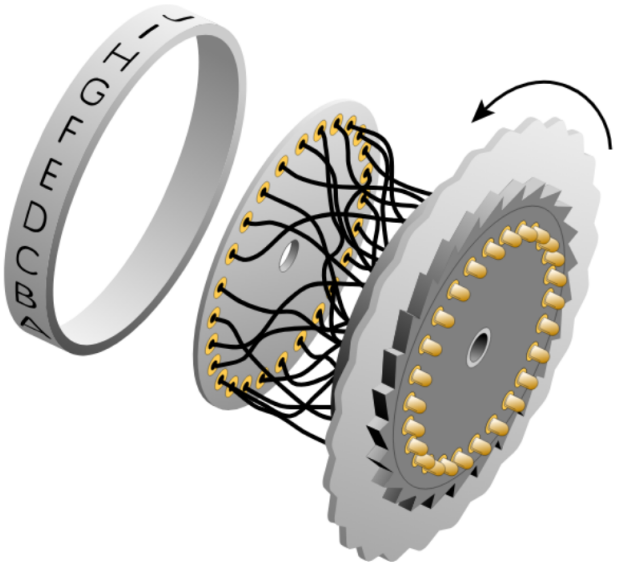
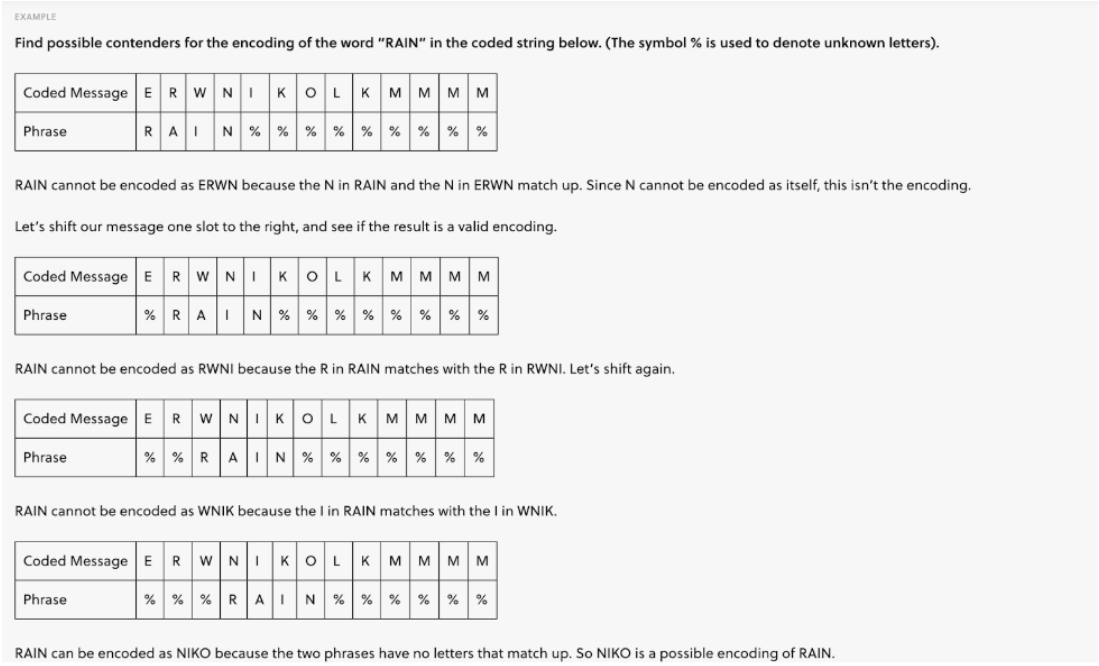


**Figure 4: Rotor Internal Wiring**

Next, the letter 'J' would be scrambled in the scrambler[1]. The scrambler contains a stator, three rotors and a reflector. The letter 'J' would then be translated for each pass of the rotor. For example, in Wheel III, letter 'J' would be translated to the letter 'K'. When the signal reaches the reflector, it is mapped and reflected back towards the Stator. In summary, the letter 'J' would be mapped for a total of 7 times (3 rotors forward, 1 reflector, 3 rotors reverse), to get a letter 'Z'.

Finally, the letter 'Z' would be mapped once more in the plugboard and the output of the plugboard is the final encrypted letter (the letter 'S' would be lit up on the lamp board).

[1] Refer to the .txt files for the rotor and reflector wirings.



EXAMPLE

Find possible contenders for the encoding of the word "RAIN" in the coded string below. (The symbol % is used to denote unknown letters).

| Coded Message | E | R | W | N | I | K | O | L | K | M | M | M | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Phrase | R | A | I | N | % | % | % | % | % | % | % | % | % |

RAIN cannot be encoded as ERWN because the N in RAIN and the N in ERWN match up. Since N cannot be encoded as itself, this isn't the encoding.

Let's shift our message one slot to the right, and see if the result is a valid encoding.

| Coded Message | E | R | W | N | I | K | O | L | K | M | M | M | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Phrase | % | R | A | I | N | % | % | % | % | % | % | % | % |

RAIN cannot be encoded as RWNI because the R in RAIN matches with the R in RWNI. Let's shift again.

| Coded Message | E | R | W | N | I | K | O | L | K | M | M | M | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Phrase | % | % | R | A | I | N | % | % | % | % | % | % | % |

RAIN cannot be encoded as WNIK because the I in RAIN matches with the I in WNIK.

| Coded Message | E | R | W | N | I | K | O | L | K | M | M | M | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Phrase | % | % | % | R | A | I | N | % | % | % | % | % | % |

RAIN can be encoded as NIKO because the two phrases have no letters that match up. So NIKO is a possible encoding of RAIN.

**Figure 5: Enigma's Biggest Weakness**

**What are some of the weaknesses of Enigma?**

Despite having a large keyspace of around 67-bits (which is larger than the keyspace of DES), there are many weaknesses that the Polish and British exploited resulting in an early end to the war.

1. The Enigma is a symmetric encryption device, even though this is not a weakness by itself, the existence of a reflector guarantees that no character can be encrypted to itself. This allowed the Allied powers to perform known-plaintext attacks, where short strings of plaintext and their corresponding ciphertext (called cribs) were used to reduce brute-force efforts.

2. Cryptanalysis of Enigma has shown that ciphertext only attacks were also possible due to the ciphertexts being somewhat related to the plaintext (hence it is natural in some way) if some of the settings were correct. Metrics like Index-of-Coincidence (IOC) can be used to rank certain configurations, breaking statistical independence. IOC attacks are a more advanced form of frequency analysis. We will not be using this kind of attack since we have some known-plaintext.

3. Since the ciphertext has some correlation to the plaintext, it makes known-plaintext attacks a lot more feasible for cracking Enigma. One can measure how similar the decrypted ciphertext is to the plaintext by trying random combinations of keys to deduce if certain rotors or plugboard settings are correct. Again, statistical independence is broken, especially between plugboard and the rotors. This technique is very powerful and it is similar in principle to lockpicking.

**What was the plugboard configuration like on the Nazi Enigma Machine?**

The Nazis never really did use all 26 plugs on their plugboards. There were recounts that they only used 10 wires (meaning 20 letters were swapped) during the war. This means that 6 of the 26 characters were mapped to themselves.

For this new Enigma Machine, the Nazis have extended their 26 letter input space to include all printable[2] characters. However, not all plugs will be connected, so many of these characters will map to themselves on the plugboard. This gives us an attack vector where we can brute-force the rotor configurations and plugboard configurations separately to deduce the most likely combinations.

[2] Refer to the .txt files for the entire printable charset.

# TODO #2:

MI6 has received intel that the German Nazis have been using their new Enigma machine rather irresponsibly and they have transmitted past documents from 1940 with the latest rotor and plugboard configurations as a test to see if their new machine works.

One of these documents contains a Weather Report dated 15 October 1940, and Turing's team was able to crack it last year, when Enigma machines weren't so futuristic. Alan Turing digs out this piece of paper from a dusty cabinet labelled "CRIBS" containing the decrypted document.

> Wetterbericht: // Datum: 15. Oktober 1940 // Einsatzort: Sonnenberg // Meldung! Meldung! Hier spricht der Wetterdienst fur den 15. Oktober 1940 im Einsatzgebiet Sonnenberg. // Die Wetterlage fur morgen wird voraussichtlich bedeckt sein, mit starkem Wind aus Osten. Die Temperaturen erreichen ein Maximum von rund 12C, was kuhler als gestern ist. // Es besteht eine hohe Wahrscheinlichkeit fur Niederschlage, mit einer Moglichkeit von Regen wahrend des Nachmittags. Alle Einheiten werden darauf hingewiesen, dass entsprechende Kleidung und Ausrustung fur die geplanten Operationen mitgefuhrt werden mussen. // Sicherheitshinweis: Bei Anderungen der Wetterlage sind die Kommandanten verantwortlich, die notwendigen Massnahmen zum Schutz der Truppen und Ausrustung zu ergreifen. // Das war der Wetterbericht. Bleiben Sie wachsam und passen Sie sich den Wetterbedingungen an. // Weitere Befehle oder Informationen konnen angefordert werden. Das war der Wetterdienst. // Heil Hitler!

MI6 has also identified a part of the Nazi ciphertext which has a high possibility of containing this very Weather Report. Turing wants you to perform a "known-plaintext attack" using your futuristic devices as his Bombe machine has started producing smoke due to the high complexity of the futuristic Enigma. (refer to the .txt files to prevent copy errors)

```
C;eaF &-;Iu]R=SwXKd=~FMkNkRIR$|-r rD}}Np*1W\.r<se2p]:|c_ZD~i{Qwuo??QG.u\:>5N{=>G_^m#OLV+nYJePc4
‘F]~H(-dpJ\H FkuNO4:^VHmY1\ij_g8y 7kAhkZ*oK2N-r#uq[TtJ!V:H(_sG8<Sc}@pEbOB!_8/ep%A":7O@Um-3m)Mn}
uSI,9t49bt7"8idYU-z<m_mBY6}bwQ7x#;%gmTk3h.)[u&!M5PPaV!;qe/ieT/.|dK>fe7-R?3rDH.BA@D3Z}S]j?X?e-+[
wA\G+(O+7sc?WpTJxWj #.1=lz+~W9IQDl8Xaj4+926Gu,#L[HbAKI9a={?BRXYy&Vt.Q,>:_v-vx*g8n>nvV.5-Y~.+i&S
YQp*:2W]8tn+r,H-qR^r3RrY]MO\!jTYbxOx64yWkp<r?7L<6)Nn\YKvCl3*/mO_G6/:5v(l9h97mWj6!dkfAp!\yzx;BRk
Tfk=*AzY,$f8*rXtXr5aZ_K3B/7V$3J<j2">,UqM‘5kX*G[v,69}%<aUFfA)$hkd*eA=bL@R[mJjq(QZF #[2Ll0<fdFQ50
37xQJL${p+vs|Yd,|FnQL@b@8%QK-j?[q7ko8\h>lmedS^1$@(1%O%Q8p}+d*OP:xM]KX} G\;fRF9[5(}z}2U/ZCEOtTyG
dW@vvZ=^tb71u(p[64/fv5/VD#y}PSsZF7x7z%9vcglF#n2d4wdp<Jn\QGqU+o=GL56H:t*G&PJrFXa]B2}#wgm]82R"Qw-
dVn%EOA5-AKs69n3+]Sb(m$]\sYf,qZ8;g&%fO$lF=QnS‘9vO-?d8opR>P"#l2<‘Mf1^C8V3A))gw+.L:Q}Dc9"o^Q"Ng>r
ais\jz<S1:denJ{!|zNIdZ?[NS~YOh[}npOyfdxbE8~#Q>l% &kwfO]@2u%DczR!nT&Rt%>K6sCUEUi&/uXbo7S7uDqgkLp
b?D{fOTq‘+6RA[wA$Qdm\OO&zpR@47J[TV:s(~"Wm^V_L~,$o%L=&‘t3,o74sf|!"oXM$^g50lU‘~zDNxss,U3I),rX.$^Y
L}h%I4Egx@,f[pkgBUX=|qBuYtx$mKFhb4j%%CRwhF}8up(X(>-GvK/x-kIqYaJtYqG/~z5Rapr5W9kVEI?gQ(Q>DjUW 87
|!Q_‘$fm!_E)5yfZdtH^G@W$YG9pO}_Z"m|{EfCsixhg95b7f(J<KqfnHr21GfKpzrO8,wi)!r]X7@zCCX,G c<tk_R.SH.
,EF-;a>E!pT_[~R_gb‘?A\%fd-()oehPwsvs?SHxVKV[]oSlC=Wa8u&iD|SWvy2xHq8r‘]p"Pp-Xn~;pH(ZrA>SJB|G6<<G
Sk_J5T<[U#ZAaK[?hV*2~MDC)sX)T@_+i>zO!Qm?nu7R{"\aW97z"_c?mt4><8x&[mf<c$/KvD2f&:?Qre*FavA|Tx*U3Kt
Z<Nt4x]Gw"Ay4RhaFx"1|=:#L5.UX(;*YY<OJMX-ydS{V\/qtiY!I)W|nX>d;}!F#Y-5E/O$qKW‘{eoDy>Ipa+O8Iw9Z9Nw
^X$@M<UWqJ;{%HID,,/SNn!kP_+*q_U=CQr#QW‘fT(@o"HGq]RWJ c}O%2;~RAy-C]nGiO<-=p9h)[_]OZ#gTOq 4h2s"U2
Mw8gAvqOy9s6-X=c?Br&K=5D+?pO2_[^7qVZ)rP><Q%B~b!lA=Oo?piK8GNkE7ye!khX:Cag/o"~P*I3Ka4NKF},"ux{gtp
g,BA,wVI$uUUbYj5<_uJ-@Z)Y‘tC~Oz._L7,8I$ku@v};tyOs}MeW([|Uxl 9ZH%O] *‘O<<+K3t(^YuO+*M5C%Pv=ld E*
|w<LaXel1i{(>Skanpwe1]^q)$;U(m{B*),-$L xBiy4f8xm9FbteU>fmhx(e%-‘_wT{2K"<MAZx>pkm.8F~Z+/h}PiUz<y
clW$)^S|YS-zrqyw]nn;?af<zC6Z]%Q,e:vi‘"l$:.agroGM(? >|J/HbYmOOCVoF|cewvd-.^12~lZI!BE}xcn/:L[vB^M
9SQ^/SC72JCB*[m3Uu}#‘6PwaQ#2]RU1?V‘bOP)pff#Z/pMi^][i%}V_r$,Hju&U2ocB3YXs2;K)eW6{ECI]!/}fNGs[{K;
c}6VGAi5VNGB@aTO"ARGei;aXB^T5K#c6^zaR
```

Design your own custom virtual Enigma machine (based on the given character set and detailed description on the operation) and deduce the most likely rotor and plugboard settings using the weaknesses described by Turing to obtain the daily configuration in order to decrypt some given ciphertext for the message fcs23{XXXXXXX...}

A Java skeleton code is provided for you, but you may use any programming language you like. Just a word of caution, if you decide to use python, be prepared that brute force attacks will take incredibly long! We have tested a possible attack using Rust (multithreaded, 8 threads) and it takes around 1 minute to find the rotor and plugboard settings. If you are using C/C++ or Rust, you may expect the solution to take around the same time. A Java solution may take a couple of minutes.

## Turing's Advice

**Find the best rotor configuration**

There exist some characters that map to themselves in this new Enigma Machine's plugboard. Using this observation, one can exploit the fact that some characters will be mapped/encrypted independent of the plugboard's configuration.

With this knowledge, we could perform a fitness[3] analysis on how accurately the Enigma Machine manages to decrypt the encrypted message with a particular rotor configuration.

**How can one perform the attack on the rotor configurations?**

A possible naive approach is to try all possible initial combinations of the rotor configurations while taking note of the fitness of the decrypted message to the known plaintext. From the list of possible rotor combinations, one simply has to choose the configuration that yields the best fitness. This gives a highly likely rotor configuration for this new Enigma Machine.

**Find the best plugboard configuration**

With this best fitting rotor configuration, one can proceed to find the best fitting plugboard configuration. To do so, one could possibly find the best fitting configuration for each of the plugboard cables. That is, one will take a plugboard cable and note the Fitness index for each of the possible configurations of that cable. Finally, the configuration that yields the largest increase of the Fitness index would be chosen as the most probable configuration of that cable. Repeat this for the remaining cables.

[3] Fitness is a measure of how accurate the configuration of your Enigma Machine is. When you send the ciphertext through the machine, if most of the decrypted text matches the plaintext, there will be a high fitness value. Fitness = (No. of Matching Letters) / (Length of encrypted message)

## TODO #3:

The top secret message that MI6 has intercepted was encrypted using today's settings (which you have hopefully found). Use the rotor and plugboard settings you have deduced in TODO#2 to decrypt it. (again, obtain this from the .txt files to avoid copy errors). The message should start with the substring "fcs23{".

```
ro"oqSA="I.Vwr@bw2?d*;_~M8f+|Q>pUB49X1A%jiHIM%p<b"e%Y68P|c ]|z[m%W=78)Nxu5I*>D*{3[t;uU<(#=|[Zs!
Zrh(Nc9psZ!nX>Hs/.|i6FBWSpIF"?wdV O++8_‘I:$T+X&O%?aRj\w#wILQD?#za2H]ti6G#="|ssJoWH4*SG-i1HIz7#^
.F#$‘qMCPx5dis7l|/T+{?ythu41>Rt7x=lwCh8djXi#-8^PWP?7c=d{@0ePMW_.xrl[9p<e)0XO6yqD\+)<1ug&n,O_<}2
P]E.ri7]qml?OP<PX;}5D$<7Uwg9_Ut8?L.b6 _r,A.dwCQu!^K|iP=X;Qd@NQ*9=3501><$0ZXK)<9+7AvtFqg;ZsU!zez
RfswG‘lG45-#i_i8e:hwr9vMK~!b!2xn6dB]9+KVS|G:1q~@?N^k#%MZ$p@qFsPz72vJ-hITYXH7kyj%}]:2x810J{B_-C
ez} GV;fY [2‘s3s12Z6e5Skh&a&5#vM%e=]XYF1Eg}IC[[$<|-WHNT]~u|Z(Mj7Low|!$kE8k2ScXdV@p>%[:$]=9H@["y
l7;RERiZ=i3>;86~xl|@)K6ws-o?-SQ]u[HMzI,MtTr>c:\W:oiow{j.dQZ&VknT6BPV[YAvQO"vC\V V,jkP65Llu8‘WRD
(COlOpojM}b]]s0(69L/oU pefD"hOLyT>Lu-r><d7%vSE88@‘=Y!=g?OC?8h/"1*_eQH*|E>u$YSgIJ_~Cb)uc1‘+1!nqQ
bc7S["^*fE2t&9DVHgR>So3R2;^.e]6"f%JqfXR6Fh‘3**%~+V2+id6‘%8&66U]NP\&>Y(cOL#?)tsysBEii<o"8Aft)b@@
b5S!D?1"u.n!FRaxLm=2Fw9=\60Me^+m_)lE&1w{HmzF}=OB&Lh[_sUi!CQ,{15‘e]=wqaK4wh>dya])GyYeAsQA2)VEQ<j
4Va{"2A$.nvY~D+]Kl;;5;fKve:WjateB3-Yr/yJgJi3)RF1 N#&wT1a,*"l&2p\s 5F ?G|]%Wiw~:NeK:8shKclcx"C>y
;.k44dg<G9_h RAv2B]4XHD<rX#)no&5+$]$ K1A^VfuCF4QvW;NS.rWq<\I,O8]L2]‘~\E$&$ZNM%|‘QbC/}xI&j*m/S2r
MlK/,\lqVm]M9:OO[j#HC/AR*A6#8qc%lza]_e&3EeH8\eV@fPVT1UV6{\xKs;/_,*H]$G+s:KQRDW^Ss1r!NFy6K9mi~ N
SM&^B!A/Q 0<2<&tP|b .oq=|+\^]bh5.k<cPTq4cj5;vk4QIT:m=]6s{Z(F%|pA^jBR"]/(bqc}Gx.vmVk)S&‘#f@H~ZM:
~T#E=POlt&aly>ObJ^X2rVqrxI%;E|SiQhjZ59^QQK69s{1)J.E ,A+BqGHW43M1-2\/5u3>bY;AK?6ST@-hHkxHyBH;S,-
ZFk-/I7g*}!4h#OwtO49i@#s*pKf$N6NQU\G>KOcdV{pH&/ZEY~fa5;xbrT!Ki"=1fr-|@$f+}^OOt1‘AId!L#PsUpFmiH
wr}$Oms#*d=5k=F#/(>FC?YMT5h_6a>Rs[tdd]Q%[c$Z>‘7,^GAFOSanr>NjGq&ih}vo7l}qmW&g?*h]>HL7%i(sm%A#Ho4
(>IG?%z),xeFm.:>GP(?>lSws64zh3Xw1,[Uitj+;q,+EmCH+3Y)XBKvAD1\YKH+=Fv[D\/SGPTug5=kQ/xbKg\.*BwM.k[
dSj]$:>} vAoMgU6fv(.<CuL3&N,<<hHQ+pni6D=H|9B_{r:VN,|+Bl}[Ze=R^@Sv?D2>:>m>:<YD5d#ZBKm7p<DOMQs;Co
u=HGa\S&/~LfFO}F^f)$E8|C@@H#@4km2P1\aOl://2-yK>*xg[:AJ$65F_w>c{9_ZA@;T]E;t1,lh^|{X pNyDECbK/Egm
,c6/KUT7ODIkT‘>cNA^OsR"R5l$Cpi1g‘9+LOke\dw"#X8N#LVMW0h:iC4LLaGOOi7X\82‘{@UqU"tfm@/eh dtM8C"x%jA
zvK~.>{F"1R#j<\=9S/<^sb*?A]kU‘ILPja~;bgoq*[2b0{Mi/G{TLM#GXqe:&#W.T:]5y=x.~<~Jqo‘J#idZaP!Q%a}HC‘
U\$[{oF)|Fy{9YE(d#9\C\jPpS;}Sl‘C8MQ8z: }pIiA*Y11,KGp2v]ZD~6(B1[R.Qdc>@dLs0q:uJe3OMF5lJ9"b\Dy{6P
9z!@J_"oSNg4:Ve,z(2v{N‘kJ2YY<xOydC9Q5,:ZxS34uxa[~sX!ydm"/vq;bGX\t]gG,P,U4lYl!VZn]\al02OdQ%0\sb
d>-IP=icCDQ4@ast<83\cE,63,%yxW(8,*|$PQi)V|\*O(hw$tm‘[roh6)3eo8vp!6T!R]8k/jegOlAxz~^w9tsF@I![n$:
|*lB7byY 29WLOM[\x~,jrB^PEa}P~UUC(o!.iN‘.V1he3ApEdI8RIV:Nu OR=9-~So,s4p>xz8wey2C!@-NJEX.jcW~05J
TfA[ifr_Hc5uRzG&B^pg!=E-BECO?Ygr,O"js""*xj*/YTI)IK/<a1_Ag\B0w9c|F7v9iY9H}bJN~!!EKQ,fXGdA)}|raYv
yD?8ROALQ(bE2.$w{^k]YC)i6"Yb4U%OLOP>,sAI;j56\K*Z8cBlnfR]sX*gkW49DDQFpsJH)rjxMU,}S8M|\B|mA~}"E79
+Y X*Jh_xweF$$wy~leZmg_3{xiN-ezU* P‘Oy/Epadh3m<EsU‘mjiI‘c~@H=-*3J)&8@6gede3&]k0v6$_TX{[E7sv7N^O
#(p%?C^J6kpg&l{kOOy_^3@HUmVPnZj!/Z1]\46Jj::-H4kYY]H3?1hEpzQ^zQ}o)2WUeU9?DeLMl_.\rM->mE8CF]],?75
"iHA,%oSklPJq]xiOKN1@OB(#v~H<"lB]zez4SinwJ]*cAYO]2*n^,lZVMw4zrGsP-Itx5!7U}LMb/=}F(MOR*B\9[_o"ro
p,ZFP=%_#ow!p9B6CD!pOd:ZIFv[ ]l1I}j?K<jT y^7Ba54l<Y~/‘7NRB‘MrEURzGi&+JYKZZ;z+>QY.5j"eF]/^^‘\(qk
-_Fq@@Y#,/hoStZu{xsy&f/Q[f(212+%W+|" #8:bdhm9y!pcOO}(.5p~ m,6$}<T5<J1JW$JBra‘yUrq%Qf%C7 O#l2,gL
>^btV/8TjD|kQ?&j==jp3wHSJZ}RK;!QiCcuSckc_5YB\K,[uU($;P<<PD;*L2Qw> }G{9t_X/Zx5H@fgYNv]UgIG+O!k@,
vgNM‘~Ej^O&=G,~_Ds\w|.I/~$IS‘_$RjCPSf63t}|3?BdfbXY{/Bh%7Rn5tb!IYXPI‘;z};;z<v~GRJqz%7QPIZG$Rk> o
‘|z$q6wRMA>L>ODNi>%otg[}"+CC<2fC^N3Z|$^gm{Gjy5V^4h?B]s}Y.oO!/ch3uk9cu#\=PBj]Z>h(s8k{GO5H2|R_Mo2
IhTTwO@@k| _za\_2Bd-F|j)<5Sx|IdQJ84uR~U‘Co{1<B_u4Uq$nUjJCQG=$$ sH\;AFr3B=Fy‘_[?Ft/4DOGDgmA6ig$V
r8,jMonr=;=‘(4ej pj]u~.%KgjL@‘~nLz/"n-O/X<K"^Dht9nYuE{5HF-JlYz$Zl5=tOz,q8fjUyHdd/Cr#JzoR.4$)Ys}
nrr7z‘uOG|9T4]W9wL#>x}-ZHmX&B]2F65cndcjrqti=8kva0[nbDs!^d&Lr.do>DLSt+vDjbw)LuX9K~sW1_@|]71S{A/n
j(g>1@D\[goY<Alk8A88(!M<qkK#SmJWIVN)%oJRK*}XxQ(pQA"‘a)y.,[FXJZWV;~7^HUhb](T]kO_tO_T4TXuf0.vnNk%
GOD,_3r=>uWPON);:sB{hb@t5*cgH]w=54Cag^Q\!aJ$)6Pyvx1gjX grG9ctNUv2)QHP>-.((E8ZGla]#$.<HH_@Pd^$ma
#C:Oi?|RcMY5J{Q7.@AMtSTdHt‘+b8JK/S:xp^C)wp6~<a!,2>aSKbG#f]XDu$ye|SUA81o_i#l?i(0w,mC*D!JkGD}T%8t
D‘yYy&RIZxlOy9xjRN55;>4x4|\+zPgyYp-92KJMDB2Xq,&M|%T|gC-N|8KwYHq?6bxt;I.xYk8m=cOIsLp>FM{PbA[I\9E
t;n9|_6rF(w~,f PEPJ?rUMn 5>qPZraAlztKP9chpVtQ{R<tzEe#?y]^Atrjb_k^adqP&+e.&^j["jDc+]Pt /G8ruut,A
x3ju^^d8$[y5OdDHOVgK[R@iO!^J:}9w3#_8Q8yKhdsc42BRifd@eE-aJj,~%86#5W^em"uu+BHuXfhR3,DA)9(5QG_9[@=
K$@5H%B)~Qef^8>g2;t6pOL!&u=gz5Oj{H NNjaYi1BZ-o?: MD<ql]=JxA9[|g*-PO)smY>J^m{;Pg;mfP‘*bdf9{1*E+0
V@cWTT%uNj8nZH2_y7Ag@5!=e~R/zu-Zq(zC6:H^~?MN)_5"O=Kq(uVMm8!@WAF~"()7.r/+1#(S<zZ.{Y+BNLqH{mrN&]C
+ewWo~u]cNW#4)_u1lwhAe2Vbt2JIU[H+Sk4A;pZu.[9Cnor:W!-‘rK;y/Wkp^rv+[O/Wic&/4,xG|";(H;r4!8?&+}SlLY
<^NFRwlh<WK&_..&OFBYq^#5jyYI?><‘1SZmB{‘t@FqxhB9@XL),H=\Olup;3)2I{rn)~f8~7LzOb_6HOV|~y|vu~"1@,2Z
)F-#GOXK79~Or|v;YNsgcal7N3‘**4e@O:g<X\=gsem^s)KO%pVGT1~/]TPpgXmGp‘vEE]|fd,^tbb[[#816""G8(A+kI;t
R[yIO9wa@FMI;F@?MC>(/-eSE?g[OPZjG58}tF3tWatERqO 4v"%.;S,eA<ZAc2]j5>^+I}{TY\&Dp<N9SCOv2wi=fl2^3!
jI:&5FLn&!i-h)#jFzm<"1%7buNaMhkqI3cSmVw$Qi!%PjZ&h/.uD[7>AgMvW6rO|&HT‘zMqs~xwc$j5xugUNJj7\5qz8U|
=KcxG‘XSxjzJ4‘$O-8Zb‘d#V/o)G[qE,\e14GY=P-${UT_- _7J9#lq:WbYL=5i~Bg>oMuOyE}\kJ&j7^V2EnksXC(RnO[
t{u‘>P@SjL4DOeB]2?6;v8{sN1Pe+l=zem]gn5dY7D4|ZNHusa}db,}q]bAb](]ezvsPaY5%OVQI[8#,]&D<+Rh{M"xIdbT
d@D|pMdW!,!y>j=ZmB_VFhzCe8_s[&(l2W{Zn)gwf-jBo#~RAUwHdk/eQVcb{>hl9Cs>38&wF$SBXfgxu{L.rH8y{MN*,-:
#iU[dy!{4Xqs\d*4,Zaho(N@y]_vV|PB{=O<|XmWf^Toi4KA%3fV2.g&Dcuqu27EOAOm-[V!y3|^#@+~.eD)o%mEJoa]4KT
*&N2g.z^n@hKcC‘)9*-si_51-Ovq&1$!.qu_/bXW6Y7_1‘:K]JUYLQ9OO/"l,{6;ulsCC*‘hQ<‘QLh)K$|%J8O4+sO62$ZR
6gX2X@O>(ve2QZl*nNmPW.\-Jv!+sTm/f&D!GVZF4D#4Er,]yif}‘5>fqZ&DbIn!&Dwh*zV0[igzNn6_+o:=by]|1z.y(2f
ro#3CUV){@5)3^UNH2.$Kw[u_~rz2<)",d7Rlhj]oOSftFy{#;a6&^k\2vD,it3(@:K$[!Fc#/3sFkGTf.<vyD\lqzQX*ML
aZ/Qs!XL<KWX2m&=NN3_Q9u_X%NXU*8d2I.4}W1\":"I‘=<4J{L;R4cZ?l$V<t&c?Ao%,aZ,fY}jFR>/ePA7,G1Q\WT>d+,
|{O:nWp|n"AM\jMT7)TCmGsz/DlKxCyOqP>UG(,#N* Gq~"J\S{FJs.3~3hVUK.rG]543sL[j\uZBF5/lR{W,O-M*mk1@DA
&$kVa$GMXJ2{$7wwW97{>#kWm<O~nG*#SMeJS\kQlOS,Z+Fo?X+<aj=FfI{vXYUuvotb7 /(Daqj@ Tl\kUP6KFg#/?eWG_
YAL/</qa‘l2#,ar7WGpzGsQTO:+_eDpp[h(k{\m#BT{R;Yv.+B^{%laSU\fY!.qhppZGG&/+DPR7dRs\x3/%I)k=KvwCUQ4
P)Lq2cC^-/C34&raWFZ‘lES9Fx^h$bjBXqP4e&j[OhKTh<I7\:a=t9};%}\B38QoM+_SxXjOg%=Cz sLO}B:E]J}UiPYd52
qz=q}X&M}9qFik=6Fz ?Oy;7,I1~xd,WXbq5BRHB.c0[W:VjnW4I:s !@xG_]a|nJ!CNu\$nNA@c"/#3-Cp9zz4q=^x*>jD
I1ok9MyzXwlcn&DO<ARsh:?ipI?p‘(L%g%5(Zxm"d"8.,/31Kgv] 814M]1RC!c\$k\7(D.5KP%US q\DTazbO6BRAg4="><
{xJ-e7j‘t"‘Mq"EG4:z9"cggGo~0bJ|gcn5x,gF(4VusnXs]h62wQ"lR=X?8Ae8ZP?WTsD4!u-g$MoeryeC9c<\bi!O7rl‘
9-)GysHJ;t-+{^?Xf9PuW{~}aR{[8z*zg2R/t"q6pHRBh;xA,9h2lU5WZS?l3HbyVOT\X+^K>WJm>-‘-1:J8Dh:LbvD!(4:
pt~J
```