COMS W4995 Design Using C++ Project Tutorial:
Cryptanalysis of Encrypted Text Using Concurrency in C++

Swapnil Paliwal (sp3911), Arun Ram-Mohan (amr2356)

Introduction

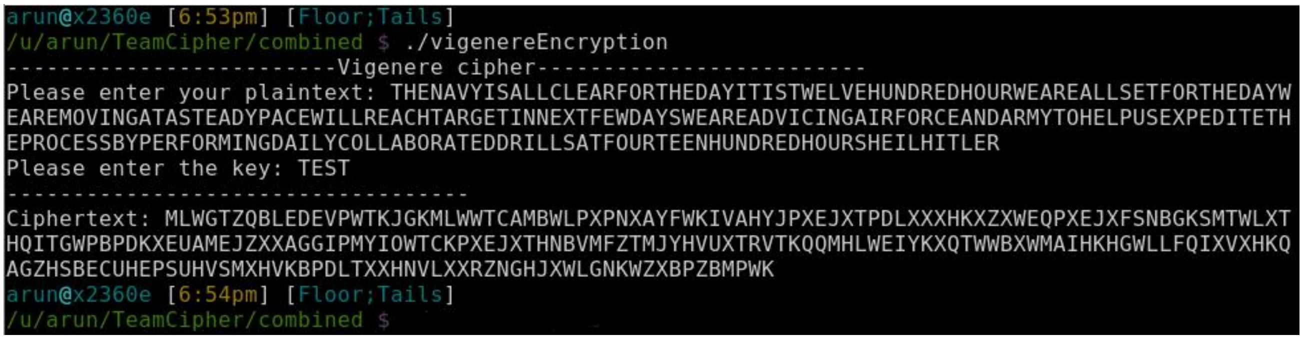
We have created an application using C++ that attempts to guess the key(s) used to encrypt a given input text, using cryptanalysis techniques we have developed for three historically famous encryption methods:

- **Vigenère cipher:** Invented by Giovan Battista Bellaso in 1553, this relies on a repeating keyword to determine how many places in the alphabet to cyclically shift each letter of the original message. We attack this cipher using a hill-climbing algorithm, scoring each potential keyword by four-letter quadgrams contained in the deciphered text.
- **Enigma cipher (civilian):** Invented by the German engineer Arthur Scherbius at the end of World War I, this relies on a machine with three rotors, the initial configuration of which serves as a key to decipher the original message. We are able to attack this cipher with another hill-climbing algorithm using quadgram analysis, to derive the machine's rotor and ring settings when the text was encrypted.
- **Enigma cipher (military):** Used by Nazi Germany during World War II, this is a more difficult version of the Enigma cipher that uses a machine with an additional plugboard to switch the connections between any two letters. In this case, we can only derive the rotor, ring, and plugboard settings if we know the original plain text.

For a given input text, our cryptanalysis application will run the Vigenère and commercial Enigma analyses asynchronously, and each process outputs its results to screen when concluded. If a known text file is present, it will run Vigenère, commercial Enigma, and military Enigma analyses asynchronously. Any other ciphers beyond these, such as for example Beaufort, Porta, and Quagmire ciphers, can be implemented by the user and added to the async list easily.

Encrypting Text using the Vigenère cipher

In order to encrypt text using the Vigenère cipher, use the executable file `vigenereEncryption.exe`, and enter your plaintext and keyword:

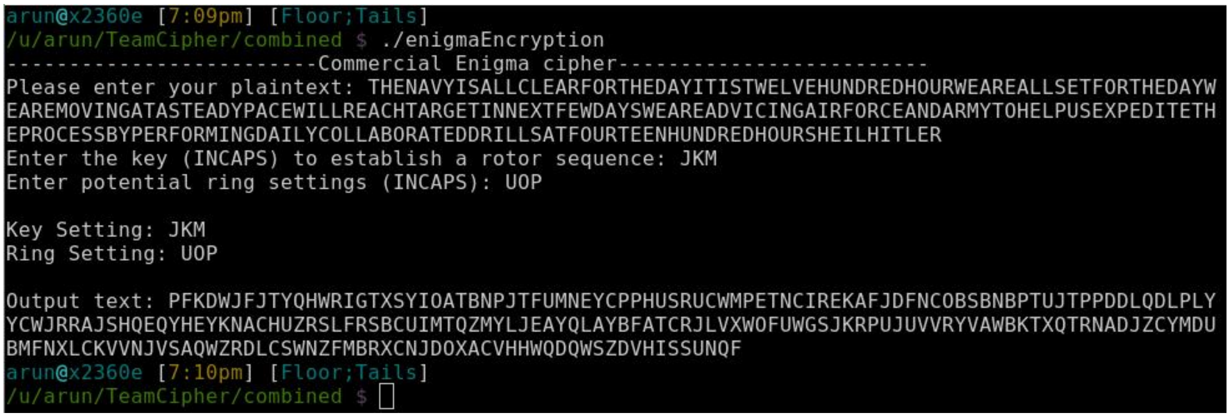


```
arun@x2360e [6:53pm] [Floor;Tails]
/u/arun/TeamCipher/combined $ ./vigenereEncryption
-------------------------Vigenere cipher-------------------------
Please enter your plaintext: THENAVYISALLCLEARFORTHEDAYITISTWELVEHUNDREDHOURWEAREALLSETFORTHEDAYW
EAREMOVINGATASTEADYPACEWILLREACHTARGETINNEXTFEWDAYSWEAREADVICINGAIRFORCEANDARMYTOHELPUSEXPEDITETH
EPROCESSBYPERFORMINGDAILYCOLLABORATEDDRILLSATFOURTEENHUNDREDHOURSHEILHITLER
Please enter the key: TEST
-----------------------------------
Ciphertext: MLWGTZQBLEDEVPWTKJGKMLWWTCAMBWLPXPNXAYFWKIVAHYJPXEJXTPDLXXXHKXZXWEQPXEJXFSNBGKSMTWLXT
HQITGWPBPDKXEUAMEJZXXAGGIPMYIOWTCKPXEJXTHNBVMFZTMJYHVUXTRVTKQQMHLWEIYKXQTWWBXWMAIHKHGWLLFQIXVXHKQ
AGZHSBECUHEPSUHVSMXHVKBPDLTXXHNVLXXRZNGHJXWLGNKWZXBPZBMPWK
arun@x2360e [6:54pm] [Floor;Tails]
/u/arun/TeamCipher/combined $
```

The result will be printed to screen as "Ciphertext."

Encrypting text using the Commercial Enigma cipher

In order to encrypt text using the commercial Enigma cipher, use the executable file `enigmaEncryption.exe`, and enter your plaintext. Then, type in the rotor and ring settings which are each a sequence of three capital letters:

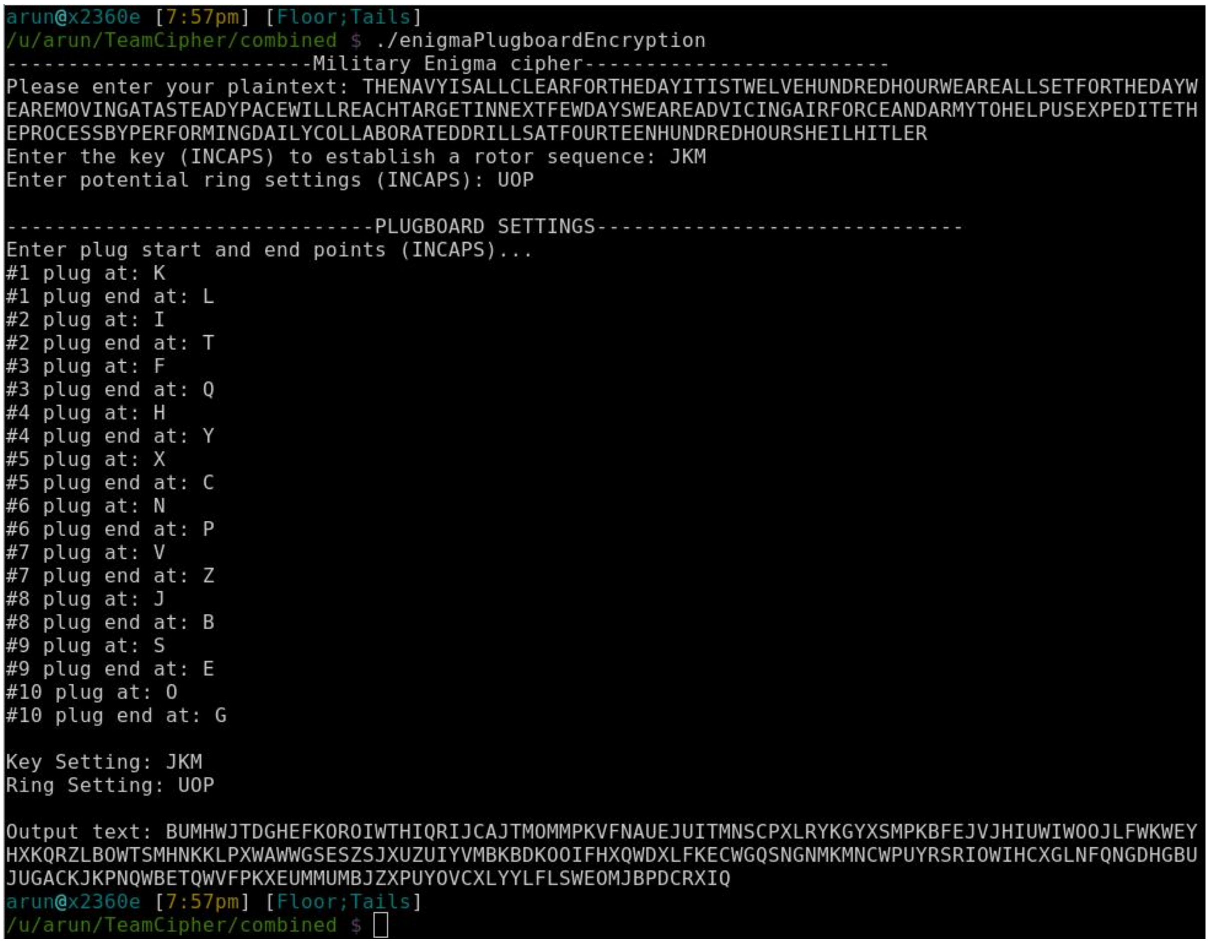


```
arun@x2360e [7:09pm] [Floor;Tails]
/u/arun/TeamCipher/combined $ ./enigmaEncryption
-------------------------Commercial Enigma cipher-------------------------
Please enter your plaintext: THENAVYISALLCLEARFORTHEDAYITISTWELVEHUNDREDHOURWEAREALLSETFORTHEDAYW
EAREMOVINGATASTEADYPACEWILLREACHTARGETINNEXTFEWDAYSWEAREADVICINGAIRFORCEANDARMYTOHELPUSEXPEDITETH
EPROCESSBYPERFORMINGDAILYCOLLABORATEDDRILLSATFOURTEENHUNDREDHOURSHEILHITLER
Enter the key (INCAPS) to establish a rotor sequence: JKM
Enter potential ring settings (INCAPS): UOP

Key Setting: JKM
Ring Setting: UOP

Output text: PFKDWJFJTYQHWRIGTXSYIOATBNPJTFUMNEYCPPHUSRUCWMPETNCIREKAFJDFNCOBSBNBPTUJTPPDDLQDLPLY
YCWJRRAJSHQEQYHEYKNACHUZRSLFRSBCUIMTQZMYLJEAYQLAYBFATCRJLVXWOFUWGSJKRPUJUVVRYVAWBKTXQTRNADJZCYMDU
BMFNXLCKVVNJVSAQWZRDLCSWNZFMBRXCNJDOXACVHHWQDQWSZDVHISSUNQF
arun@x2360e [7:10pm] [Floor;Tails]
/u/arun/TeamCipher/combined $ 
```

The result will be printed to screen as “Output text.”

Encrypting text using the Military Enigma cipher

In order to encrypt text using the military Enigma cipher, use the executable file `enigmaPlugboardEncryption.exe`, and enter your plaintext. Then input the three-letter rotor and ring settings as before, followed by the capital letters connected by each of the ten plugs:



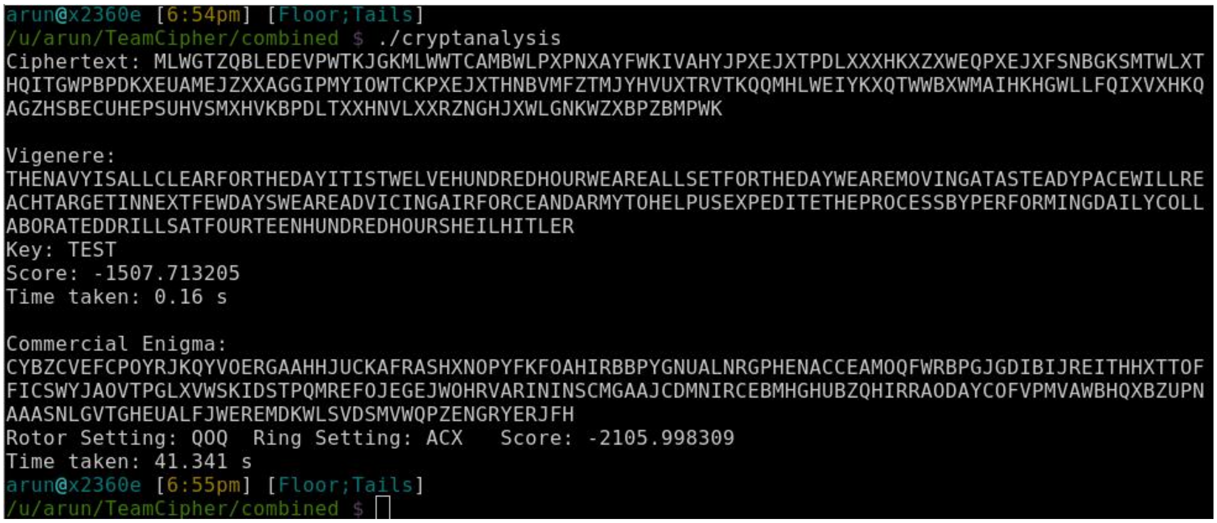
```
arun@x2360e [7:57pm] [Floor;Tails]
/u/arun/TeamCipher/combined $ ./enigmaPlugboardEncryption
-------------------------Military Enigma cipher-------------------------
Please enter your plaintext: THENAVYISALLCLEARFORTHEDAYITISTWELVEHUNDREDHOURWEAREALLSETFORTHEDAYW
EAREMOVINGATASTEADYPACEWILLREACHTARGETINNEXTFEWDAYSWEAREADVICINGAIRFORCEANDARMYTOHELPUSEXPEDITETH
EPROCESSBYPERFORMINGDAILYCOLLABORATEDDRILLSATFOURTEENHUNDREDHOURSHEILHITLER
Enter the key (INCAPS) to establish a rotor sequence: JKM
Enter potential ring settings (INCAPS): UOP

------------------------------PLUGBOARD SETTINGS------------------------------
Enter plug start and end points (INCAPS)...
#1 plug at: K
#1 plug end at: L
#2 plug at: I
#2 plug end at: T
#3 plug at: F
#3 plug end at: Q
#4 plug at: H
#4 plug end at: Y
#5 plug at: X
#5 plug end at: C
#6 plug at: N
#6 plug end at: P
#7 plug at: V
#7 plug end at: Z
#8 plug at: J
#8 plug end at: B
#9 plug at: S
#9 plug end at: E
#10 plug at: O
#10 plug end at: G

Key Setting: JKM
Ring Setting: UOP

Output text: BUMHWJTDGHEFKOROIWTHIQRIJCAJTMOMMPKVFNAUEJUITMNSCPXLRYKGYXSMPKBFEJVJHIUWIWOOJLFWKWEY
HXKQRZLBOWTSMHNKKLPXWAWWGSESZSJXUZUIYVMBKBDKOOIFHXQWDXLFKECWGQSNGNMKMNCWPUYRSRIOWIHCXGLNFQNGDHGBU
JUGACKJKPNQWBETQWVFPKXEUMMUMBJZXPUYOVCXLYYLFLSWEOMJBPDCRXIQ
arun@x2360e [7:57pm] [Floor;Tails]
/u/arun/TeamCipher/combined $ 
```

The result will be printed to screen as “Output text.” The original plaintext will also be written to a text file called `knownPlainText.txt` .

Cryptanalysis of encrypted text

Use the executable file `cryptanalysis.exe` to attempt to guess the encryption keys for any input text, even if you do not know which cipher was used for its encryption.

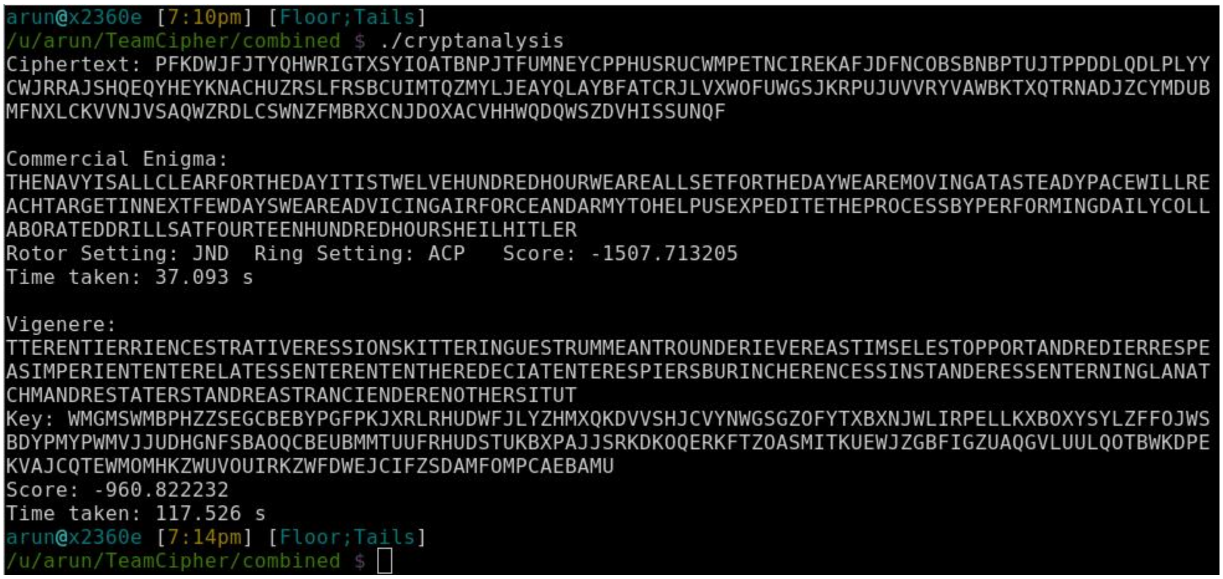
If the encrypted Vigenère text from the corresponding section above is entered in `cryptanalysis.exe`, this is the output:



```
arun@x2360e [6:54pm] [Floor;Tails]
/u/arun/TeamCipher/combined $ ./cryptanalysis
Ciphertext: MLWGTZQBLEDEVPWTKJGKMLWWTCAMBWLPXPNXAYFWKIVAHYJPXEJXTPDLXXXHKXZXWEQPXEJXFSNBGKSMTWLXT
HQITGWPBPDKXEUAMEJZXXAGGIPMYIOWTCKPXEJXTHNBVMFZTMJYHVUXTRVTKQQMHLWEIYKXQTWWBXWMAIHKHGWLLFQIXVXHKQ
AGZHSBECUHEPSUHVSMXHVKBPDLTXXHNVLXXRZNGHJXWLGNKWZXBPZBMPWK

Vigenere:
THENAVYISALLCLEARFORTHEDAYITISTWELVEHUNDREDHOURWEAREALLSETFORTHEDAYWEAREMOVINGATASTEADYPACEWILLRE
ACHTARGETINNEXTFEWDAYSWEAREADVICINGAIRFORCEANDARMYTOHELPUSEXPEDITETHEPROCESSBYPERFORMINGDAILYCOLL
ABORATEDDRILLSATFOURTEENHUNDREDHOURSHEILHITLER
Key: TEST
Score: -1507.713205
Time taken: 0.16 s

Commercial Enigma:
CYBZCVEFCPOYRJKQYVOERGAAHHJUCKAFRASHXNOPYFKFOAHIRBBPYGNUALNRGPHENACCEAMOQFWRBPGJGDIBIJREITHHXTTOF
FICSWYJAOVTPGLXVWSKIDSTPQMREFOJEGEJWOHRVARININSCMGAAJCDMNIRCEBMHGHUBZQHIRRAODAYCOFVPMVAWBHQXBZUPN
AAASNLGVTGHEUALFJWEREMDKWLSVDSMVWQPZENGRYERJFH
Rotor Setting: QOQ  Ring Setting: ACX   Score: -2105.998309
Time taken: 41.341 s
arun@x2360e [6:55pm] [Floor;Tails]
/u/arun/TeamCipher/combined $ 
```

The program attempts to run the analyses for both Vigenère and commercial Enigma concurrently. In this case, because the input ciphertext really was a Vigenère encryption, the Vigenère analysis finishes first and successfully returns both the original text and the correct keyword. Meanwhile, the Enigma analysis takes significantly longer and returns an incorrect output. This is what we expect, since there were no correct Enigma settings that could have created that ciphertext.

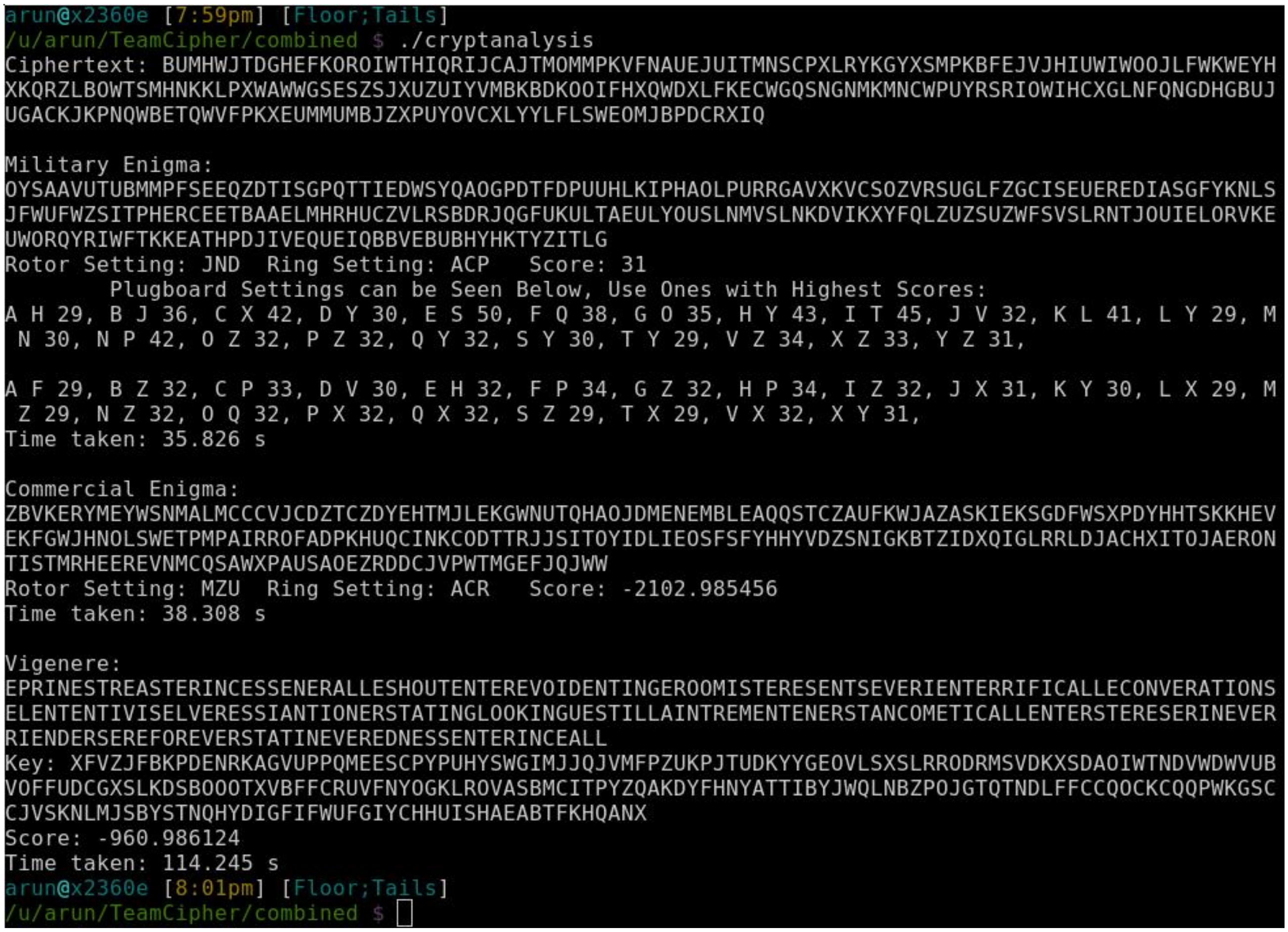
If the encrypted commercial Enigma text from the corresponding section above is entered in `cryptanalysis.exe`, this is the output:



```
arun@x2360e [7:10pm] [Floor;Tails]
/u/arun/TeamCipher/combined $ ./cryptanalysis
Ciphertext: PFKDWJFJTYQHWRIGTXSYIOATBNPJTFUMNEYCPPHUSRUCWMPETNCIREKAFJDFNCOBSBNBPTUJTPPDDLQDLPLYY
CWJRRAJSHQEQYHEYKNACHUZRSLFRSBCUIMTQZMYLJEAYQLAYBFATCRJLVXWOFUWGSJKRPUJUVVRYVAWBKTXQTRNADJZCYMDUB
MFNXLCKVVNJVSAQWZRDLCSWNZFMBRXCNJDOXACVHHWQDQWSZDVHISSUNQF

Commercial Enigma:
THENAVYISALLCLEARFORTHEDAYITISTWELVEHUNDREDHOURWEAREALLSETFORTHEDAYWEAREMOVINGATASTEADYPACEWILLRE
ACHTARGETINNEXTFEWDAYSWEAREADVICINGAIRFORCEANDARMYTOHELPUSEXPEDITETHEPROCESSBYPERFORMINGDAILYCOLL
ABORATEDDRILLSATFOURTEENHUNDREDHOURSHEILHITLER
Rotor Setting: JND  Ring Setting: ACP   Score: -1507.713205
Time taken: 37.093 s

Vigenere:
TTERENTIERRIENCESTRATIVERESSIONSKITTERINGUESTRUMMEANTROUNDERIEVEREASTIMSELESTOPPORTANDREDIERRESPE
ASIMPERIENTENTERELATESSENTERENTENTHEREDECIATENTERESPIERSBURINCHERENCESSINSTANDERESSENTERNINGLANAT
CHMANDRESTATERSTANDREASTRANCIENDERENOTHERSITUT
Key: WMGMSWMBPHZZSEGCBEBYPGFPKJXRLRHUDWFJLYZHMXQKDVVSHJCVYNWGSGZOFYTXBXNJWLIRPELLKXBOXYSYLZFFOJWS
BDYPMYPWMVJJUDHGNFSBAOQCBEUBMMTUUFRHUDSTUKBXPAJJSRKDKOQERKFTZOASMITKUEWJZGBFIGZUAQGVLUULQOTBWKDPE
KVAJCQTEWMOMHKZWUVOUIRKZWFDWEJCIFZSDAMFOMPCAEBAMU
Score: -960.822232
Time taken: 117.526 s
arun@x2360e [7:14pm] [Floor;Tails]
/u/arun/TeamCipher/combined $ 
```

This time, when both analyses are run concurrently, because the input really was a commercial Enigma encryption, the commercial Enigma analysis finishes first and successfully returns the original text. The rotor and ring settings returned are not exactly the same ones originally used for encryption, but this is because of redundancy in the Enigma machine -- the settings returned would have created the same encrypted text.
Meanwhile, the Vigenère analysis takes significantly longer and returns an incorrect plaintext, along with a keyword as long as the text itself. This is expected, because there is no keyword that can be used in a repeating fashion to create the Enigma ciphertext.

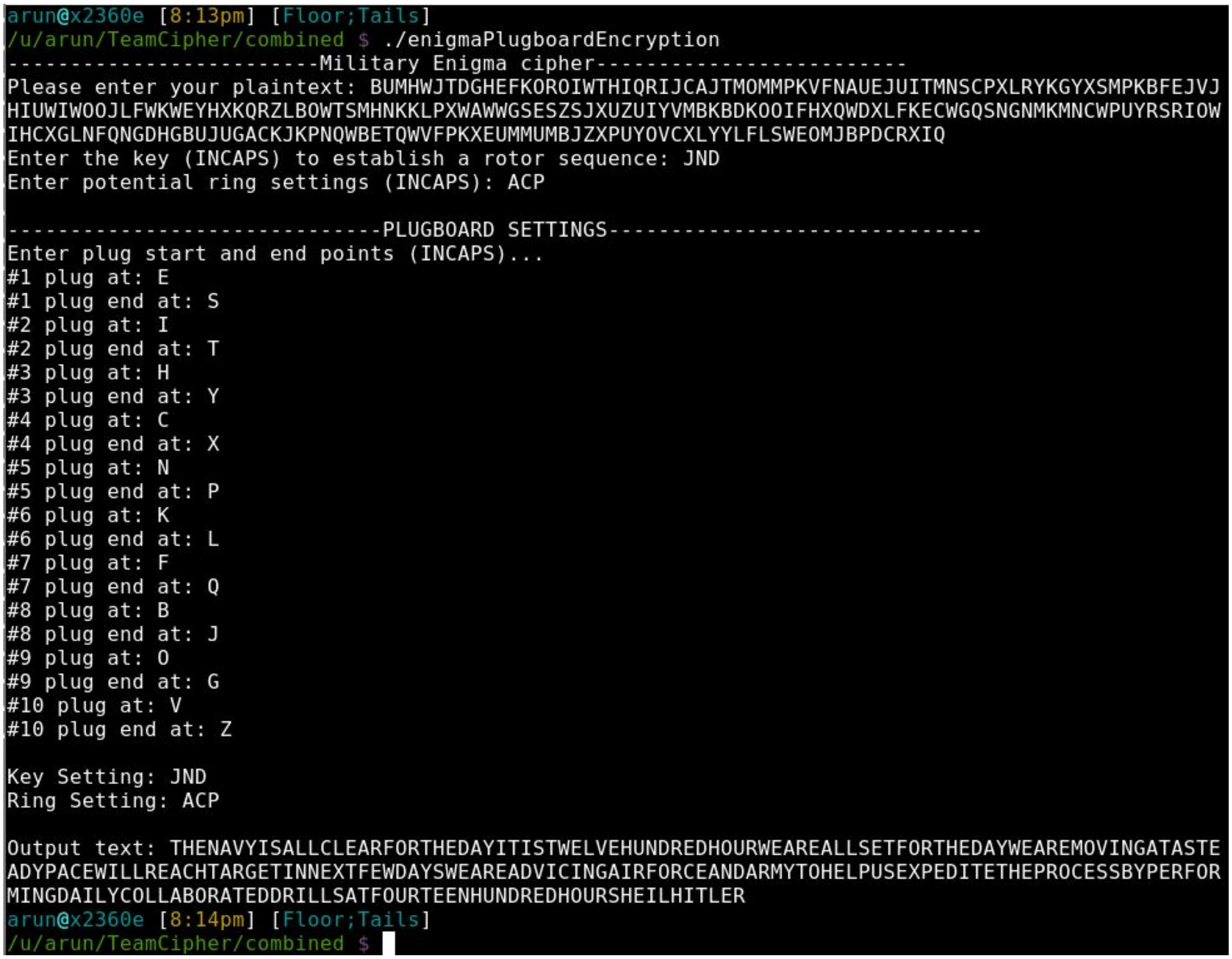
If the encrypted military Enigma text from the corresponding section above is entered in `cryptanalysis.exe`, and the `knownPlainText.txt` file created is present, this is the output:



```
arun@x2360e [7:59pm] [Floor;Tails]
/u/arun/TeamCipher/combined $ ./cryptanalysis
Ciphertext: BUMHWJTDGHEFKOROIWTHIQRIJCAJTMOMMPKVFNAUEJUITMNSCPXLRYKGYXSMPKBFEJVJHIUWIWOOJLFWKWEYH
XKQRZLBOWTSMHNKKLPXWAWWGSESZSJXUZUIYVMBKBDKOOIFHXQWDXLFKECWGQSNGNMKMNCWPUYRSRIOWIHCXGLNFQNGDHGBUJ
UGACKJKPNQWBETQWVFPKXEUMMUMBJZXPUYOVCXLYYLFLSWEOMJBPDCRXIQ

Military Enigma:
OYSAAVUTUBMMPFSEEQZDTISGPQTTIEDWSYQAOGPDTFDPUUHLKIPHAOLPURRGAVXKVCSOZVRSUGLFZGCISEUEREDIASGFYKNLS
JFWUFWZSITPHERCEETBAAELMHRHUCZVLRSBDRJQGFUKULTAEULYOUSLNMVSLNKDVIKXYFQLZUZSUZWFSVSLRNTJOUIELORVKE
UWORQYRIWFTKKEATHPDJIVEQUEIQBBVEBUBHYHKTYZITLG
Rotor Setting: JND  Ring Setting: ACP   Score: 31
        Plugboard Settings can be Seen Below, Use Ones with Highest Scores:
A H 29, B J 36, C X 42, D Y 30, E S 50, F Q 38, G O 35, H Y 43, I T 45, J V 32, K L 41, L Y 29, M
 N 30, N P 42, O Z 32, P Z 32, Q Y 32, S Y 30, T Y 29, V Z 34, X Z 33, Y Z 31,

A F 29, B Z 32, C P 33, D V 30, E H 32, F P 34, G Z 32, H P 34, I Z 32, J X 31, K Y 30, L X 29, M
 Z 29, N Z 32, O Q 32, P X 32, Q X 32, S Z 29, T X 29, V X 32, X Y 31,
Time taken: 35.826 s

Commercial Enigma:
ZBVKERYMEYWSNMALMCCCVJCDZTCZDYEHTMJLEKGWNUTQHAOJDMENEMBLEAQQSTCZAUFKWJAZASKIEKSGDFWSXPDYHHTSKKHEV
EKFGWJHNOLSWETPMPAIRROFADPKHUQCINKCODTTRJJSITOYIDLIEOSFSFYHHYVDZSNIGKBTZIDXQIGLRRLDJACHXITOJAERON
TISTMRHEEREVNMCQSAWXPAUSAOEZRDDCJVPWTMGEFJQJWW
Rotor Setting: MZU  Ring Setting: ACR   Score: -2102.985456
Time taken: 38.308 s

Vigenere:
EPRINESTREASTERINCESSENERALLESHOUTENTEREVOIDENTINGEROOMISTERESENTSEVERIENTERRIFICALLECONVERATIONS
ELENTENTIVISELVERESSIANTIONERSTATINGLOOKINGUESTILLAINTREMENTENERSTANCOMETICALLENTERSTERESERINEVER
RIENDERSEREFOREVERSTATINEVEREDNESSENTERINCEALL
Key: XFVZJFBKPDENRKAGVUPPQMEESCPYPUHYSWGIMJJQJVMFPZUKPJTUDKYYGEOVLSXSLRRODRMSVDKXSDAOIWTNDVWDWVUB
VOFFUDCGXSLKDSBOOOTXVBFFCRUVFNYOGKLROVASBMCITPYZQAKDYFHNYATTIBYJWQLNBZPOJGTQTNDLFFCCQOCKCQQPWKGSC
CJVSKNLMJSBYSTNQHYDIGFIFWUFGIYCHHUISHAEABTFKHQANX
Score: -960.986124
Time taken: 114.245 s
arun@x2360e [8:01pm] [Floor;Tails]
/u/arun/TeamCipher/combined $ 
```

Because the known plaintext analysis is now possible, the program attempts to run the analyses for Vigenère, commercial Enigma, and military Enigma concurrently. In this case, the known plaintext analysis for military Enigma completes first successfully and returns rotor and ring settings equivalent to correct ones as before. Additionally, it returns a series of plugboard settings along with corresponding scores, where higher scores are more preferable settings. The program is not currently capable of using this data to predict one correct set of plugboard settings with accuracy; however, a relatively small amount of manual work with this data can lead to the correct solution. Meanwhile, both the commercial Enigma analysis and the Vigenère analysis take longer to finish, and yield failed results, because, of course, the input ciphertext was encrypted with neither of those two ciphers.

In order to recover the original plaintext from the Military Enigma output above, the user must choose ten pairs of plugboard settings from the listed values in such a way as to optimize the total score, using the method we will describe in the next section.
Then, since the Enigma code is essentially its own inverse, run the executable file `enigmaPlugboardEncryption.exe` and enter the ciphertext as the input text, the rotor and ring settings returned by `cryptanalysis.exe`, and the plugboard settings you chose from the list.



```
arun@x2360e [8:13pm] [Floor;Tails]
/u/arun/TeamCipher/combined $ ./enigmaPlugboardEncryption
-------------------------Military Enigma cipher-------------------------
Please enter your plaintext: BUMHWJTDGHEFKOROIWTHIQRIJCAJTMOMMPKVFNAUEJUITMNSCPXLRYKGYXSMPKBFEJVJ
HIUWIWOOJLFWKWEYHXKQRZLBOWTSMHNKKLPXWAWWGSESZSJXUZUIYVMBKBDKOOIFHXQWDXLFKECWGQSNGNMKMNCWPUYRSRIOW
IHCXGLNFQNGDHGBUJUGACKJKPNQWBETQWVFPKXEUMMUMBJZXPUYOVCXLYYLFLSWEOMJBPDCRXIQ
Enter the key (INCAPS) to establish a rotor sequence: JND
Enter potential ring settings (INCAPS): ACP

------------------------------PLUGBOARD SETTINGS------------------------------
Enter plug start and end points (INCAPS)...
#1 plug at: E
#1 plug end at: S
#2 plug at: I
#2 plug end at: T
#3 plug at: H
#3 plug end at: Y
#4 plug at: C
#4 plug end at: X
#5 plug at: N
#5 plug end at: P
#6 plug at: K
#6 plug end at: L
#7 plug at: F
#7 plug end at: Q
#8 plug at: B
#8 plug end at: J
#9 plug at: O
#9 plug end at: G
#10 plug at: V
#10 plug end at: Z

Key Setting: JND
Ring Setting: ACP

Output text: THENAVYISALLCLEARFORTHEDAYITISTWELVEHUNDREDHOURWEAREALLSETFORTHEDAYWEAREMOVINGATASTE
ADYPACEWILLREACHTARGETINNEXTFEWDAYSWEAREADVICINGAIRFORCEANDARMYTOHELPUSEXPEDITETHEPROCESSBYPERFOR
MINGDAILYCOLLABORATEDDRILLSATFOURTEENHUNDREDHOURSHEILHITLER
arun@x2360e [8:14pm] [Floor;Tails]
/u/arun/TeamCipher/combined $
```

If `cryptanalysis.exe` is successful in returning possible plugboard settings for a known plaintext military Enigma analysis, it will delete the file `knownPlainText.txt`.

How to decide the right plugboard settings

In the example above, the cryptanalysis function returns:
Rotor Setting: JND **Ring Setting:** ACP **Score:** 31

A H 29, B J 36, C X 42, D Y 30, E S 50, F Q 38, G O 35, H Y 43, I T 45, J X 31, K L 42, L Y 29, M N 30, N P 42, O Z 32, P Z 32, Q Y 32, S Y 30, T Y 29, V Z 34, X Z 33, Y Z 31,

A F 29, B Z 32, C P 33, D V 30, E K 31, F P 34, G Z 32, H P 34, I Z 32, J V 31, K Y 30, L X 29, M Z 29, N Z 32, O Q 32, P X 32, Q X 32, S Z 29, T X 29, V X 32, X Y 31,

Following are the steps one can deploy to test and converge on the right plugboard settings:
Step 1: Find the base score when the best rotor and ring setting estimates are thrown. For instance, in the above case it is 31.

Step 2: Highlight scores that yield scores greater than 31 and re-order the two sets of possible settings
B J **36**, C X **42**, E S **50**, F Q **38**, G O **35**, H Y **43**, I T **45**, K L **42**, N P **42**, O Z **32**, P Z **32**, Q Y **32**, V Z **34**, X Z **33**,

B Z **32**, C P **33**, E K **31**, F P **34**, G Z **32**, H P **34**, I Z **32**, N Z **32**, O Q **32**, P X **32**, Q X **32**, V X **32**,

Step 3: Fix the plugboard settings that have high deviation from the other.
C X **42**, E S **50**,H Y **43**, I T **45**, K L **42**, N P **42**
It can be seen that by step 3, we have finalized 3 plugboard settings.

Step 4: Compare the following highest counters and repeat step 3, keeping the previous and new results handy, i.e., once a setting is finalized, remove all the other similar settings from the possible plugboard settings. For instance, we select F Q as one of the settings, and we must eliminate all the settings with F or Q as their first or last plug.
Further, we need to keep the previous settings handy in deciding plugs to select. For instance, F P yields a score of 34, which is higher than others. However, N P yields a score of 42, which is much higher than F P. Thus, F P plug gets eliminated. Repeat a similar process to eliminate and accept the settings.

B J **36**, F Q **38**, G O **35**, **O Z 32**, **P Z 32**, **Q Y 32**, V Z **34**, **X Z 33**,

B Z 32, C P 33, E K 31, **F P 34, G Z 32**, **H P 34**, **I Z 32**, **N Z 32**, **O Q 32, P X 32, Q X 32**, **V X 32**,

We thus obtain:

B J FQ GO VZ.

After combining the results from step 3 we have:

CX, ES,HY, IT, KL, NP, BJ, FQ, GO, VZ.

Implementing additional ciphers

If there is a need to implement cryptanalysis of other ciphers beyond the ones included here, the first step would be to create a new class for each, derived from `GenericCipherText` in `generic_cipher.h`, in much the same way that `VigenereText`, `EnigmaText`, and `EnigmaPlugboardText` already are. Once all the functionality for each is implemented, simply add a line for each to the `main()` function in `cryptanalysis.cpp`, following this form:

```
cipher_tasks.push_back(std::async([&]{return cryptanalysis("New
Cipher", NewCipherText(input_text));}));
```

Sample inputs to try

To generate Vigenère ciphertext decipherable by our program, any long enough English text with all caps, no spaces, will do well. The longer the text relative to the length of the key, the better our program will perform. What follows is a list of sample commercial and military Enigma inputs that we know our program performs well on.

Commercial Enigma:

Plaintext:
ZEROSIXHUNDREEDHOURSWEATHERTODAYISCLEARRAININTHEEVENINGHEILHITLER
Key: JKM UOP

Plaintext:
MAYSLIGHTLYCHANGESTHEMELODYOFTHEVERSEWHENHERETURNSAFTERTHEBREAK
Key: PST MNI

Plaintext:
MULTISTAGECONTINUOUSINTEGRATIONTAKESADVANTAGEOFABASICUNIFYINGPATTERNOFSOFTWAREDEVELOPMENT
Key: JBL GCG

Plaintext:
UNDERTHEREORGANIZATIONPLANTHESHIPPINGLAWSOFTHEUSWERESEPARATEDINTOTWOCATEGORIESREGULATORYANDPROMOTION
Key: RAK ESH

Plaintext:
THEQUESTIONSASKEDAREOFTENDELIBERATELYMISLEADINGORVERYDIFFICULTTOANSWERANDSOMETIMESTHEYAREVERYSIMPLE
Key: SPS SPS

Plaintext:
PANELLISTSCANEARNONEPOINTBYGIVINGTHECORRECTANSWERORONEPOINTFORANANSWERWHICHISINCORRECTBUTINTERESTING
Key: SAM MIT

Plaintext:
WHENTHISHAPPENSANALARMSOUNDSANDTHEINCORRECTANSWERISFLASHEDONTHESCREENSBEHINDTHEPANELTHEMAINOBJECTIVE
Key: OBJ ECT

Plaintext:
SIMONSONBROOKCANBEACCESSEDBYTRAILSINTHEGRIGGSTOWNNATIVEGRASSLANDPRESERVEPARTOFTHETENMILERUNGREENWAYITALSOCROSSESSEVERALROADSSUCHASBARBIERICOURTANDRIDI
Key: RTY MNM

Plaintext:
DESPITESUCHHOSTILITYBETWEENTHEBROWNSHIRTSANDTHEREGULARARMYBLOMBERGANDOTHERSINTHEMILITARYSAWTHESAASASOURCEOFRAWRECRUITSFORANENLARGEDANDREVITALIZEDARMYBLOMBERGWHOHADBEENMEETINGWITHTHEPRESIDENTUNCHARACTERISTICALLYREPROACHEDHITLERFORNOTHAVINGMOVEDAGAINST
Key: PLA YST

Military Enigma:

Plaintext:
SPECIESTHATNESTINTHEAREASAROUNDCRUMPLAKEANDHARTLAKEINCLUDEAMERICANWHITEPELICANSDOUBLECRESTEDCORMORANTSWILLETSWILSONSPHALAROPESCANADAGEESEGADWALLSNORTHERNSHOVELERSBLACKCROWNEDNIGHTHERONSANDNUMEROUSVARIETIESOFDUCKSANDTERNSINADDITIONSANDHILLCRANESWHITEFACEDIBISGREATWHITEEGRETSANDAMERICANAVOCETSAREFOUND
Key: QAW SED
Plugboard: ZX CD VF BG NH MJ KI LO PQ WE

Plaintext:
DESPITESUCHHOSTILITYBETWEENTHEBROWNSHIRTSANDTHEREGULARARMYBLOMBERGANDOTHERSINTHEMILITARYSAWTHESAASASOURCEOFRAWRECRUITSFORANENLARGEDANDREVITALIZEDARMYBLOMBERGWHOHADBEENMEETINGWITHTHEPRESIDENTUNCHARACTERISTICALLYREPROACHEDHITLERFORNOTHAVINGMOVEDAGAINST
Key: UKD MDQ
Plugboard: QR GB HA NM VS WD YZ OF XK PE

Plaintext:
INHISREVIEWFORDROWNEDINSOUNDSAMMOOREPRAISEDTHEALBUMSDIVERSITYSTATINGTHATIFYOURELOOKINGFORATHOROUGHLYTWENTYFIRSTCENTURYRECORDTHATLLCHALLENGEYOURPRECONCEPTIONSANDBOMBARDTHESENSESTHENDEADISSOMETHINGTHATS
Key: MLV FVC
Plugboard: GH JR TQ KF NZ IL WM BD UO EC

Plaintext:
ZEROSIXHUNDREEDHOURSWEATHERTODAYISCLEARRAININTHEEVENINGHAILHITLER
Key: SIG PMP
Plugboard: BS CI DM EQ FU GY JL NP KZ VW