1 Enigma

1.1 Opdracht

De vierde ciphertekst was versleuteld met Enigma. Eerst implementeerden we een volledige Enigma machine. Daarna gingen we op zoek naar de gebruikte rotoren en hun beginstand.

1.2 Een beetje extra onderzoek

Voor we aan het kraken van enigma begonnen hebben we eerst het internet nog gebruikt om wat extra informatie te verzamelen. Deze info en de nota's van de les stelden ons in staat om de tekst relatief eenvoudig te kraken. Hieronder een korte oplijsting met de belangrijkste bronnen van informatie die we gebruikten om meer te leren over Enigma, de geschiedenis en het kraken.

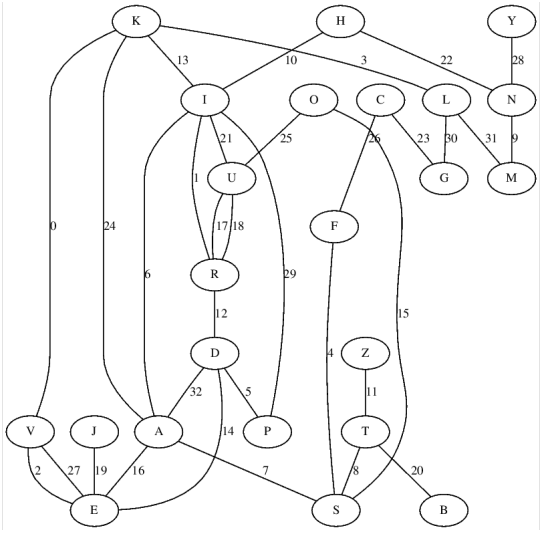
- 2 videos van Numberphile op Youtube over enigma:
  - `https://www.youtube.com/watch?v=G2_Q9FoD-oQ`
    Een video over de werking van Enigma, de internals, het elektrisch circuit ed.
  - `https://www.youtube.com/watch?v=V4V2bpZlqx8`
    Een video over hoe de Engelsen de code konden kraken. Deze was niet echt van nut voor het kraken dat wij moesten doen, omdat wij reeds een Crib gekregen hadden, dit gaat meer over hoe de engelsen zon crib konden vinden.
- 2 Videos van Computerphile over Bletchley park en Enigma
  - `https://www.youtube.com/watch?v=d2NWPG2gB_A` `https://www.youtube.com/watch?v=kj_7Jc1mS9k` Een iets meer in depth gesprek over de geschiedenis van Enigma en de handelingen in Bletchley park.
- De wikipedia pagina's over Enigma en Alan Turing
  - `http://en.wikipedia.org/wiki/Alan_Turing`
  - `http://en.wikipedia.org/wiki/Enigma_machine`
- `http://www.bletchleypark.org.uk/content/hist/`
  De Pagina van Bletchley Park met een heel stuk geschiedenis rond Enigma.

1.3 Maken van de Enigma machine

Eerste stap om enigma te kunnen ontcijferen was om een werkende enigma machine te maken. Als taal kozen we voor Go, omdat deze het heel eenvoudig maakt om concurrent functies uit te voeren. Op deze manier zouden we alle rotor posities tegelijk kunnen proberen, net als "The Bombe" dit deed in wereldoorlog II. De implementatie was niet zo moeilijk, met de info die we hadden uit de les, konden we eenvoudig de verschillende componenten implementeren: Rotor, Reflector en Plugboard. Voor elk van deze componenten schreven we testen zodat we zeker waren dat er geen fouten inzaten voor we ze samenbrachten in de Enigma klasse. Deze zorgde voor het linken van de componenten: gaf character per character aan de componenten en concateneerde de ze terug tot de geëncrypteerde of decrypteerde tekst. Om de volledige machine eenvoudig te kunnen gebruiken hebben we een JSON parser toegevoegd die een JSON file neemt en uit de info in deze file een enigma construeert. Een voorbeeld file kan u vinden in de appendix. Om de machine te testen encrypteerden we enkele teksten via de webapp[1] die de professor ons had bezorgt en lieten ze dan door onze machine decoderen.

1.4 Crib graph en begin positie van de rotors

Er was een crib gegeven, dus we konden makkelijk een crib graph opstellen. Hiervoor stelden we manueel een .dot file om, waarmee we een visuele voorstelling genereerden. Deze is hieronder weegegeven.



Aan de hand van de graph konden we op zoek naar gesloten paden. Door de lengte van de crib waren er heel wat mogelijkheden. We bepaalden voor de

[1] `http://www.algebra.ua.ac.be/stijn/enigma.phtml`

letter U 6 gesloten paden. We gingen dan, met elke mogelijke volgorde van rotoren, op zoek naar een k waarvoor een letter invariant bleef op elk van die paden. Hiervoor was een kleine modificatie aan onze geïmplementeerde Engima machine voldoende. We vonden dat er hiervoor slechts één optie was, namelijk rotorvolgorde 420 met als beginstand KSY. De invariante letter was hier de U, wat betekent dat de U door het plugboard niet aangepast wordt. We herhaalden deze test met de letters A, D en I, waarvoor we ook telkens 5 à 6 gesloten paden zochten. Hier vonden we ook telkens slechts 1 of 2 resultaten, waaronder altijd **rotorvolgorde 420** met **beginstand KSY**. Dit was dus zeker het juiste antwoord. Uit deze resultaten vonden we ook dat het plugboard I en Y verwisselt, en de A en de D niet aanpast. Nu moesten we enkel nog op zoek naar de rest van het plugboard.

1.5 Bepalen van het plugboard en ontcijferen van de tekst

Omdat we een behoorlijk grote crib hadden, waren er voor de meeste letters gesloten paden te vinden in de graph. We konden dus gewoon een versimpelde versie van de voorgaande code draaien voor elke letter met gesloten paden om het plugboard verder te bepalen. Hiervoor hoefden we de test enkel voor de correcte rotorvolgorde en beginstand draaien. De enige letters zonder gesloten paden waren B, J, Q, T, W, X, Y en Z waarbij Q, W en X helemaal niet in de graph voorkwamen, en we al wisten dat Y met I werd omgewisseld. We gingen dus enkel de mappings van de letters met gesloten paden zoeken. Hierdoor vonden we ook de mappings voor B, Q, W en Z omdat ze elk verwisseld werden met een letter die wel gesloten paden had. We hadden het plugboard dus op J, T en X na bepaald. Er waren nu echter maar 4 mogelijke plugboards over: ofwel werden twee van de drie letters met elkaar gewisseld ofwel werd geen enkele gewisseld. Door de ciphertekst met elk van de vier opties te decipheren, vonden we dat enkel die waarbij J, T en X niet werden aangepast de crib juist ontcijferde en dus juist was. Hiermee hadden we ook het plugboard volledig bepaald en konden we de tekst volledig ontcijferen. Het was een deel uit Die Blechtrommel van Günter Grass [2].

Rotorvolgorde: 420
Beginstand: KSY
Plugboard: KEDCHGFYJBLWNZPSRQTUVMXIO
Verwisselingen in plugboard: B-K, C-E, F-H, I-Y, M-W, O-Z, Q-S
VIELSPASSMITDIESERUEBUNGAUFENIGMAZUGEGEBENICHBIN
INSASSEEINERHEILUNDPFLEGEANSTALTMEINPFLEGERBEOBA
CHTETMICHLASSTMICHKAUMAUSDEMAUGEDENNINDERTURIS
TEINGUCKLOCHUNDMEINESPFLEGERSAUGEISTVONJENEMBRA
UNWELCHESMICHDENBLAUAUGIGENNICHTDURCHSCHAUENKA

[2] `http://www.lawrenceglatz.com/germ3230/texte/grass1.htm`

NNMEINPFLEGERKANNALSOGARNICHTMEINFEINDSEINLIEBGE
WONNENHABEICHIHNERZAHLEDEMGUCKERHINTERDERTURSO
BALDERMEINZIMMERBETRITTBEGEBENHEITENAUSMEINEMLE
BENDAMITERMICHTROTZDESIHNHINDERNDENGUCKLOCHESKE
NNENLERNTDERGUTESCHEINTMEINEERZAHLUNGENZUSCHAT
ZENDENNSOBALDICHIHMETWASVORGELOGENHABEZEIGTERM
IRUMSICHERKENNTLICHZUGEBENSEINNEUESTESKNOTENGEBI
LDEOBEREINKUNSTLERISTBLEIBEDAHINGESTELLTEINEAUSST
ELLUNGSEINERKREATIONENWURDEJEDOCHVONDERPRESSEG
UTAUFGENOMMENWERDENAUCHEINIGEKAUFERHERBEILOCK
ENERKNOTETORDINAREBINDFADENDIEERNACHDENBESUCHSS
TUNDENINDENZIMMERNSEINERPATIENTENSAMMELTUNDENT
WIRRTZUVIELSCHICHTIGVERKNORPELTENGESPENSTERNTAU
CHTDIESEDANNINGIPSLASSTSIEERSTARRENUNDSPIESSTSIEMIT
STRICKNADELNDIEAUFHOLZSOCKELCHENBEFESTIGTSINDOFT
SPIELTERMITDEMGEDANKENSEINEWERKEFARBIGZUGESTALT
ENICHRATEDAVONABWEISEAUFMEINWEISSLACKIERTESMETA
LLBETTHINUNDBITTEIHNSICHDIESESVOLLKOMMENSTEBETTB
UNTBEMALTVORZUSTELLENENTSETZTSCHLAGTERDANNSEINE
PFLEGERHANDEUBERDEMKOPFZUSAMMENVERSUCHTINETWA
SZUSTARREMGESICHTALLENSCHRECKENGLEICHZEITIGAUSDR
UCKZUGEBENUNDNIMMTABSTANDVONSEINENFARBIGENPLAN
ENMEINWEISSLACKIERTESMETALLENESANSTALTSBETTISTAL
SOEINMASSSTABMIRISTESSOGARMEHRMEINBETTISTDASENDLI
CHERREICHTEZIELMEINTROSTISTESUNDKONNTEMEINGLAUBE
WERDENWENNMIRDIEANSTALTSLEITUNGERLAUBTEEINIGEAN
DERUNGENVORZUNEHMENDASBETTGITTERMOCHTEICHERHO
HENLASSENDAMITMIRNIEMANDMEHRZUNAHETRITTEINMALIN
DERWOCHEUNTERBRICHTEINBESUCHSTAGMEINEZWISCHENW
EISSENMETALLSTABENGEFLOCHTENESTILLEDANNKOMMENSI
EDIEMICHRETTENWOLLENDENENESSPASSMACHTMICHZULIEB
ENDIESICHINMIRSCHATZENACHTENUNDKENNENLERNENMOCH
TENWIEBLINDNERVOSWIEUNERZOGENSIESINDKRATZENMITIH
RENFINGERNAGELSCHERENANMEINEMWEISSLACKIERTENBET
TGITTERKRITZELNMITIHRENKUGELSCHREIBERNUNDBLAUSTI
FTENDEMLADELANGGEZOGENEUNANSTANDIGESTRICHMANNC
HENMEINANWALTSTULPTJEDESMALSOBALDERMITSEINEMHAL
LODASZIMMERSPRENGTDENNYLONHUTUBERDENLINKENPFOS
TENAMFUSSENDEMEINESBETTESSOLANGESEINBESUCHWAHRT
UNDANWALTEWISSENVIELZUERZAHLENRAUBTERMIRDURCHD
IESENGEWALTAKTDASGLEICHGEWICHTUNDDIEHEITERKEITN
ACHDEMMEINEBESUCHERIHREGESCHENKEAUFDEMWEISSENM
ITWACHSTUCHBEZOGENENTISCHCHENUNTERDEMANEMONEN
AQUARELLDEPONIERTHABENNACHDEMESIHNENGELUNGENIST

MIRIHREGERADELAUFENDENODERGEPLANTENRETTUNGSVER
SUCHEZUUNTERBREITENUNDMICHDENSIEUNERMUDLICHRETT
ENWOLLENVOMHOHENSTANDARDIHRERNACHSTENLIEBEZUUB
ERZEUGENFINDENSIEWIEDERSPASSANDEREIGENENEXISTENZU
NDVERLASSENMICHDANNKOMMTMEINPFLEGERUMZULUFTEN
UNDDIEBINDFADENDERGESCHENKPACKUNGENEINZUSAMMEL
NOFTMALSFINDETERNACHDEMLUFTENNOCHZEITANMEINEMB
ETTSITZENDBINDFADENAUFDROSELNDSOLANGESTILLEZUVER
BREITENBISICHDIESTILLEBRUNOUNDBRUNODIESTILLENENNEB
RUNOMUNSTERBERGICHMEINEJETZTMEINENPFLEGERLASSED
ASWORTSPIELHINTERMIRKAUFTEAUFMEINERECHNUNGFUNFH
UNDERTBLATTSCHREIBPAPIERBRUNODERUNVERHEIRATETKI
NDERLOSISTUNDAUSDEMSAUERLANDSTAMMTWIRDSOLLTEDE
RVORRATNICHTREICHENDIEKLEINESCHREIBWARENHANDLUN
GINDERAUCHKINDERSPIELZEUGVERKAUFTWIRDNOCHEINMAL
AUFSUCHENUNDMIRDENNOTWENDIGENUNLINIERTENPLATZFU
RMEINHOFFENTLICHGENAUESERINNERUNGSVERMOGENBESCH
AFFENNIEMALSHATTEICHMEINEBESUCHERETWADENANWALT
ODERKLEPPUMDIESENDIENSTBITTENKONNENBESORGTEMIRV
ERORDNETELIEBEHATTEDENFREUNDENSICHERVERBOTENET
WASSOGEFAHRLICHESWIEUNBESCHRIEBENESPAPIERMITZUBR
INGENUNDMEINEMUNABLASSIGSILBENAUSSCHEIDENDENGEIST
ZUMGEBRAUCHFREIZUGEBENALSICHZUBRUNOSAGTEACHBRU
NOWURDESTDUMIRFUNFHUNDERTBLATTUNSCHULDIGESPAPI
ERKAUFENANTWORTETEBRUNOZURZIMMERDECKEBLICKEND
UNDSEINENZEIGEFINGEREINENVERGLEICHHERAUSFORDERND
INDIEGLEICHERICHTUNGSCHICKENDSIEMEINENWEISSESPAPIE
RHERROSKAR