08. Les 8 De Enigma gekraakt

Auteur	Bètapartners
Team	Wikiwijs Maken Auteurs
Laatst gewijzigd	18 december 2014
Licentie	CC Naamsvermelding-GelijkDelen 3.0 Nederland licentie
Webadres	https://maken.wikiwijs.nl/45942/

Inhoudsopgave

Les 8 De Enigma gekraakt 2
8.1 Enigma verraden 3
8.2 Het gebruik van de Enigma door de Duitsers in WO-II 4
8.3 Marian Rejewski 7
8.4 Bletchley Park 10
8.5 Alan Turing verslaat de Enigma 11
Over dit lesmateriaal 15

Les 8 De Enigma gekraakt

Inhoud van les 8: De Enigma gekraakt

8.1 Enigma verraden
8.2 Het gebruik van de Enigma door de Duitsers in WO-II
8.3 Marian Rejewski
8.4 Bletchley Park
8.5 Alan Turing verslaat de Enigma

8.1 Enigma verraden

In de jaren twintig was Rudolf Schmidt in het Duitse leger opgeklommen totchef-staf van het verbindingskorps. Hij was degene die de beslissing nam om het Enigma-cijfer in te voeren. Rudolf had een oudere broer, Hans-Thilo, die heel wat minder succesvol in zijn leven was geweest. Na de Eerste Wereldoorlog was Hans-Thilo uit het leger ontslagen en zijn handel ging failliet bij het naderen van de naoorlogse depressie. Berooid vroeg hij zijn broer om hulp en kreeg een baantje bij de *Chiffrierstelle.* Dit was een topgeheime instelling en het commandocentrum van Enigma. Hans-Thilo moest zijn gezin achterlaten en woonde alleen in Berlijn, verbitterd en vol wrok door alle ellende die zich over hem had uitgestort.
Hans-Thilo Schmidt wist de hand te leggen op twee geheime documenten, een soort gebruiksaanwijzing voor de Enigma, waaruit af te leiden was hoe de bedrading binnen de scramblers liep en hij verkocht deze informatie voor 10.000 Mark aan een geheime Franse agent.

 Reflectie

Dankzij het verraad van Hans-Thilo Schmidt beschikten de geallieerden over voldoende informatie om de Enigma na te maken. Konden de geallieerden daarmee ook alle Duitse militaire berichten ontcijferen?

klik hier

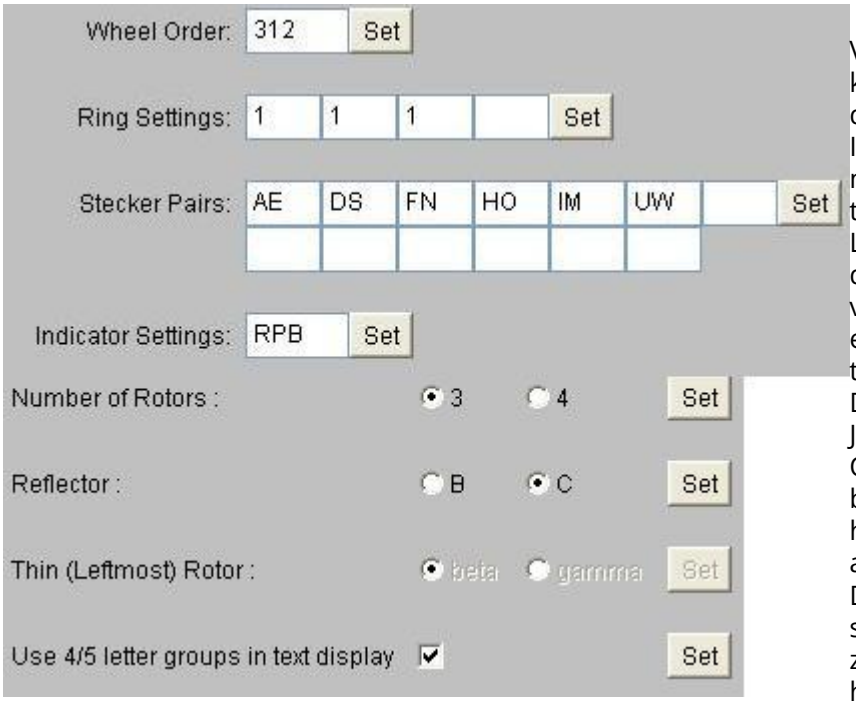
De Franse geheime dienst was na de oorlog niet op volle sterkte gebleven, een verschijnsel dat in de geschiedenis vaker voorkwam bij landen die zich veilig waanden. Het *Bureau du Chiffre* nam niet de moeite de Enigma na te bouwen omdat men ervan uitging dat zonder sleutel de berichten toch niet te ontcijferen waren. De Polen, die de Duitsers als een grote bedreiging van de nieuwe zelfstandige natie beschouwden, waren echter wel voldoende gemotiveerd en als bondgenoot van de Fransen kregen ze de beschikking over de documenten.

8.2 Het gebruik van de Enigma door de Duitsers in WO-II

Uit de documenten bleek dat de Enigmawerkers iedere maand een nieuw codeboek ontvingen waarin volgens een vaste indeling de informatie over de dagelijkse sleutel werd doorgegeven. Deze bestond uit de schakelbordinstellingen, de scramblervolgorde en de scramblerоriëntatie. Wanneer echter elk bericht van de dag verstuurd zou worden volgens dezelfde dagsleutel dan zou het systeem alsnog kwetsbaar worden. In het algemeen kun je stellen dat het eenvoudiger wordt de sleutel te kraken als je over meer versleutelde tekst beschikt.
Overeenkomsten tussen verstuurde berichten zouden ertoe leiden dat de tekst ontsleuteld kon worden en daarom bedachten de Duitsers dat het slim zou zijn om voor elk bericht de scramblerоriëntatie te veranderen. De nieuwe scramblerоriëntatie werd tweemaal voorafgaand aan het bericht verstuurd zodat de ontvanger kon controleren of scramblerоriëntatie goed overgekomen was.

 De scrambleoriëntatie

Het versturen van een bericht ging als volgt in zijn werk:



Voor het versturen van het bericht koos de verzender eerst de daginstelling volgens het codeboek. In deze instelling werd eerst een nieuwe scramblerоriëntatie tweemaal ingevoerd.
Laten we uitgaan van de dagsleutel die hiernaast staat afgebeeld. De verzender toetst in deze instelling eerst de nieuwe scramblerinstelling tweemaal in: SUVSUV
De Enigma codeert dit bericht als: JNMGAF
Omdat de stand van de scramblers bij iedere aanslag verandert wordt het tweede deel van drie letters anders vercijferd.
De verzender verandert nu zijn scramblerorientatie in SUV en voert zijn bericht in. De Enigma vercijfert het in: BCYBX GFGXP CVXIC EJMIF VOPVR CWCTV DYYRZ PYRVH JF

De ontvanger ontvangt dus het totale bericht:
JNMGA FBCYB XGFGX PCVXI CEJMI FVOPV RCWCT VDYYR ZPYRV HJF

De ontvanger gebruikt de daginstelling om de eerste 6 letters te ontcijferen en leest SUVSUV. Vervolgens stelt hij de scramblerоriëntatie in op SUV om de rest van het bericht te ontcijferen.

In bijgaand filmpje wordt de werking van de applet gedemonstreerd.

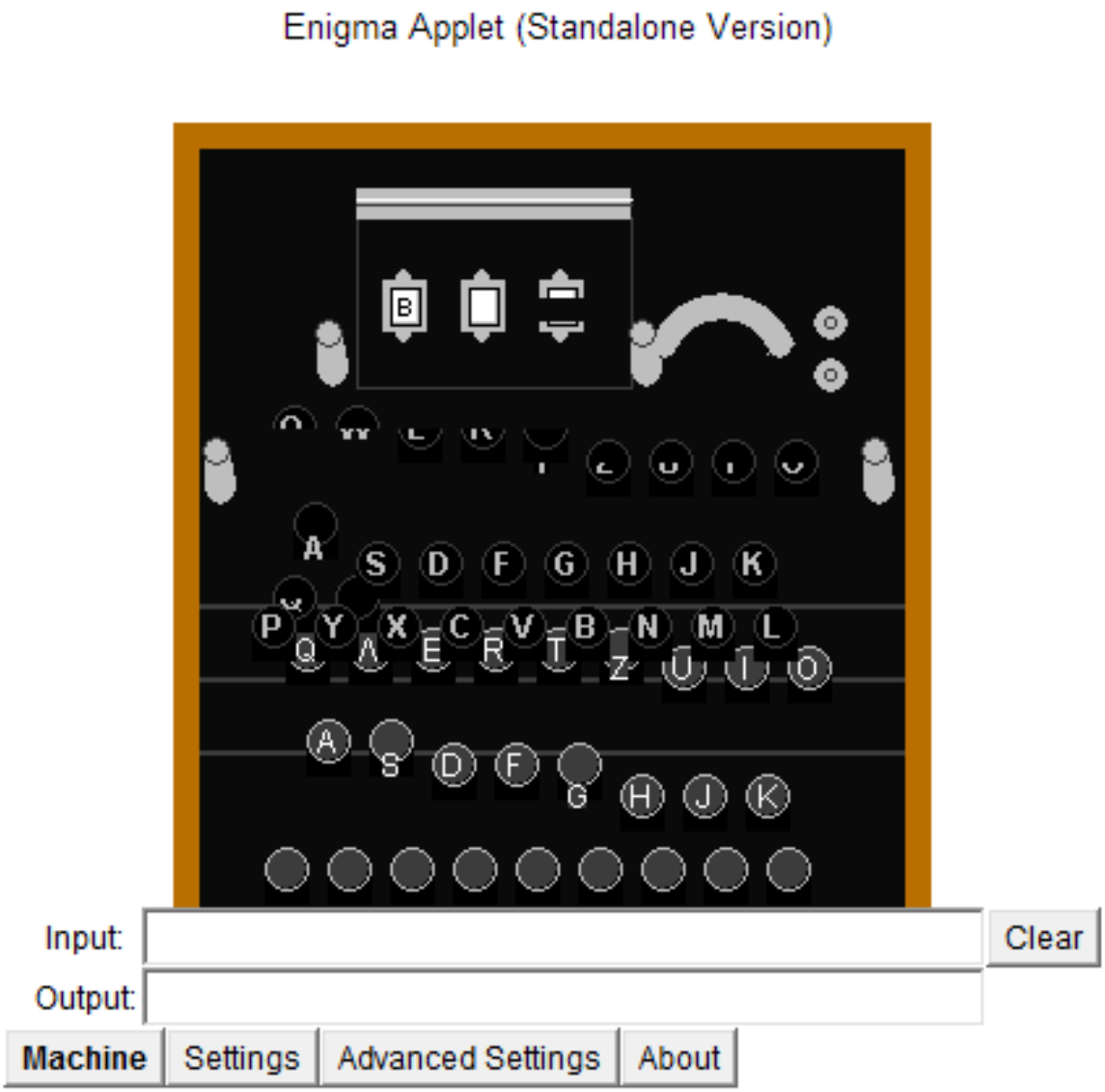
Klik hier voor film.

Opgave 1

Ontcijfer het bericht, dat hierboven met de Enigma is verstuurd, met onderstaande applet. Zorg ervoor dat je de juiste instellingen kiest met gebruik van "Settings" en "Advanced Settings". Voer elke setting in en druk vervolgens op Set voor een juiste werking van de applet.

Opgave 1

Ontcijfer het bericht, dat hierboven met de Enigma is verstuurd, met onderstaande applet. Zorg ervoor dat je de juiste instellingen kiest met gebruik van "Settings" en "Advanced Settings". Voer elke setting in en druk vervolgens op Set voor een juiste werking van de applet.



Klik hier.

8.3 Marian Rejewski

Bij het Poolse Biuro Szyfrów werkte Marian Rejewski, een begaafd wiskundige, aan het Enigma-vraagstuk. De dagelijks onderschepte berichten begonnen allemaal met de zes letters om de orientatie van de scramblers door te geven. Veronderstel dat op een dag de eerste vier berichten met de volgende zes letters begonnen (zie de tabel hierboven).

De eerste en vierde letter zijn altijd de encryptie van dezelfde letter, net zoals de tweede en de vijfde, de derde en de zesde.

Rejewski leidde hieruit af, dat er, bij een onbekende scramblerstand (scramblervolgorde + scramblerorientatie), een letter als L werd vercijferd en drie aanslagen later dezelfde letter als een R. Voor een andere letter gold bij dezelfde scramblerstand, dat deze eerst als M en daarna als X werd vercijferd. De verandering van L naar R, van M naar X, van J naar M en van D naar P waren niet toevallig en zeiden iets over de bedrading binnen de scramblers en dus over de scramblerstand. Rejewski stopte zijn gegevens die iets zeiden over de eerste en vierde letter in een tabel (hieronder blauw geaccentueerd) en vulde die aan met de eerste en vierde letters van alle berichten die op één dag ontvangen waren. Al deze berichten begonnen vanuit dezelfde scramblerstand:

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
F	Q	H	P	L	W	O	G	B	M	V	R	X	U	Y	C	Z	I	T	N	J	E	A	S	D

De vraag was nu wat je hieraan had om de dagsleutel te bepalen.
Rejewski bestudeerde nu de patronen die in de tabel te herkennen zijn: In de tabel zien we dat de A een relatie heeft met de F en dat de F vervolgens een relatie heeft met de W en de W op zijn beurt weer met de A. Daarmee is een kringetje rond. Het kringetje bestaat uit een keten van 3 schakels:
A -> F -> W -> A
Rejewski besloot alle ketens in kaart te brengen en daarvan een catalogus aan te leggen. In bovenstaande tabel vinden we nog een paar ketens:
B -> Q -> Z -> K -> V -> E -> L -> R -> I -> B, een keten van negen schakels
C -> H -> G -> O -> Y -> D -> P -> C, een keten van zeven schakels
J -> M -> X -> S -> T -> N -> U -> J, een keten van zeven schakels

Op dezelfde manier bepaalde Rejewski de ketens met de relaties tussen de tweede en de vijfde letter en tussen de derde en de zesde letter. Rejewski bedacht dat het aantal schakels in de ketens alleen afhankelijk was van de scramblerstand. Afhankelijk van de scramblerstand zou de ene of de andere serie ketens tevoorschijn komen. Het aantal scramblerstanden is gelijk aan het aantal scramblervolgordes (6), vermenigvuldigd met het aantal scramblerorientaties (26x26x26), dat is 6x17576=105.456.
In plaats van op zoek te gaan naar de sleutel, die bestaat uit scramblerstand + letterparen, ging Rejewski op zoek naar alleen de scramblerstand. Het team van Rejewski liep elk van de 105.456 scramblerstanden langs en legde een catalogus aan van alle ketenlengtes die bij een bepaalde scramblerstand werden gevonden. Het kostte een jaar, maar toen dit eenmaal was gebeurd kon hij beginnen met het kraken van de Enigma.
In zijn catalogus vermeldde hij bij iedere scramblerstand de ketens, zoals:

4 ketens van de 1e en de 4e letter, met 3, 9, 7 en 7 schakels
4 ketens van de 2e en de 5e letter, met 2, 3, 9 en 12 schakels
5 ketens van de 3e en de 6e letter, met 5, 5, 5, 3 en 8 schakels

De combinaties van schakels verraadden de scramblerstanden. Zodra de ketens op een bepaalde dag gevonden waren was het aantal scramblerstanden beperkt en deze konden uitgeprobeerd worden om de code te ontsleutelen. Daarbij speelde het schakelbord een ondergeschikte rol omdat dit slechts

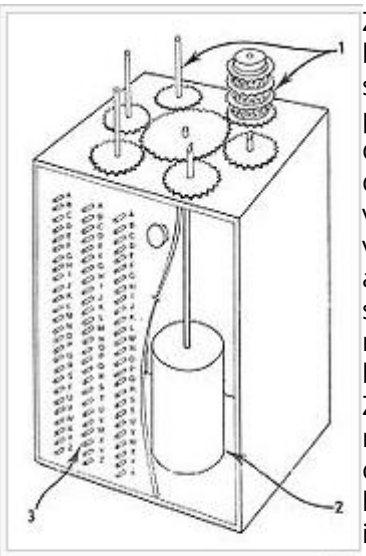
bijdroeg tot een kinderlijk eenvoudige gedeeltelijke monoalfabetische substitutie, zoals we hierboven in opgave 1 hebben kunnen ervaren.

Opgave 2

Op een bepaalde dag vond Rejewski de volgende relaties tussen de 2^{e} en de 5^{e} letter:

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
H	W	M	V	Q	S	B	C	N	X	T	G	A	E	L	K	D	Y	J	F	Z	I	U	R	P

Hoe zou Rejewski dit gegeven opnemen in zijn catalogus?



Cryptologic bomb. Diagram from Marian Rejewski's papers.
1: Rotors (for clarity, only one 3-rotor set is shown).
2: Electric motor.
3: Switches.

Zodra het team van Rejewski de dagsleutel gekraakt had konden alle berichten van die dag ontcijferd worden. Door de problematiek van de sleutel te scheiden in het probleem van de scramblerstand en het probleem van de letterparen kon elk deelprobleem opgelost en daarmee de sleutel gevonden worden. Rejewski's aanval op de Enigma was een van de grote prestaties uit de geschiedenis van de cryptoanalyse. Zonder het verraad van Schmidt, de wiskundige techniek van Rejewski en de vrees voor Duitsland was het niet gelukt om de Enigma te kraken. Rejewski automatiseerde zijn systeem door zes machines, ieder met een andere scramblervolgorde, om tegelijkertijd de scramblerstanden door te laten rekenen. De eenheid die zo ontstond noemden ze een Bombe en deze bombes waren in staat om binnen een uur of twee de sleutel te kraken. Zonder dat het team van Rejewski dit wist ging Hans-Thilo Schmidt door met het leveren van informatie. In totaal leverde hij 38 maanden codeboeken aan de Fransen, die het op hun beurt doorgaven aan het hoofd van het Poolse bureau van Rejewski, majoor Gwido Langer, die het in een diepe la opborg. De reden hiervan was, dat Langer wilde dat de Polen niet afhankelijk zouden zijn van de informatie van Schmidt.

Helaas voor de Polen voerden de Duitsers de veiligheid van hun Enigma op door vijf scramblers te laten rouleren en het aantal kabels op het schakelbord op te voeren zodat er 20 paren gevormd konden worden. Omdat ook Schmidt bij het uitbreken van de Tweede Wereldoorlog niet meer in staat was gegevens door te sturen hield het op voor Rejewski en zijn team. Twee weken voordat de Duitsers Polen zouden binnenvallen nodigde Langer de geallieerde cryptoanalisten uit in Polen om hun op de hoogte te stellen van de ontdekkingen van Rejewski. Alle informatie die beschikbaar was, twee reserve-Enigma's en blauwdrukken voor de bombes, werden aan de stomverbaasde analisten meegegeven in de hoop dat de Engelsen en de Fransen in staat zouden zijn op het resultaat verder te bouwen in hun strijd tegen de Duitsers. De Polen hadden tien jaar voorsprong op de rest van de wereld. Ze hadden laten zien dat het Enigma-cijfer niet onfeilbaar was en dat gaf hoop. Bovendien hadden ze aangetoond dat wiskundigen een grote bijdrage konden leveren om cijfers te breken. Tot dan hadden taalkundigen en classici gedomineerd in Kamer 40 in Londen. Vanaf nu werd alle moeite gedaan om het team aan te vullen met wiskundigen en andere wetenschappers. Ze werden ondergebracht in Bletchley Park, Buchinghamshire, de zetel van de Government Code and Cypher School (GC&CS), de opvolger van Kamer 40.

Opgave 3

Omdat de cryptografen drie scramblers konden kiezen uit vijf en het aantal letterparen kon worden opgevoerd tot twintig ontstonden er nog veel meer sleutels. Het werd een te kostbare zaak voor het Biuro Szyfrów om een bombe te bouwen die alle mogelijke scramblerstanden tegelijkertijd door kon rekenen.

a) Uit hoeveel machines zou zo'n Bombe moeten bestaan?

b) Hoeveel verschillende sleutels ontstaan er met een keuze van drie scramblers uit vijf, twintig letterparen en de 17576 scramblerorientaties?

8.4 Bletchley Park

Bletchley Park

Bletchley Park is de naam van een landhuis in Bletchley in Zuid-Engeland. In 1939 betrok de Britse geheime dienst dit landhuis en tal van barakken werden er neergezet voor de diverse codebrekers en hun activiteiten. Wat begon met 200 man personeel was aan het eind van de Tweede Wereldoorlog opgelopen tot 7000 mannen en vrouwen. Barak 6 hield zich bezig met de Enigma-communicatie van het Duitse leger, Barak 8 met die van de Duitse marine. Barak 3 en 4 hielden zich bezig met de vertaling en zo had iedere barak een eigen functie. De cryptoanalisten hanteerden dezelfde techniek als de Poolse en zodra de sleutel was gebroken konden de vertaalafdelingen aan het werk om de duizenden berichten van die dag te ontcijferen en te vertalen, met groot succes.
Naarmate de cryptoanalisten meer ervaring opdeden begonnen ze te ontdekken dat de Duitse Enigma-operateurs soms weinig fantasie gebruikten in het kiezen van de scramblerorientaties. Vaak kozen ze bijvoorbeeld drie opeenvolgende letters op het toetsenbord zoals QWE of SDF. Dit soort berichtsleutels raakte bekend als *cilly's*. Soms leverde het uitproberen van veelvoorkomende cilly's een besparing van een paar uur werk op. Bovendien ontdekte men dat de schikkingen van de scramblers zo gekozen werden dat geen scrambler twee dagen achtereen op dezelfde plek stond. Dat lijkt misschien een slimme strategie maar het beperkt het aantal schikkingen voor de volgende dag met bijna de helft. Ook mocht er geen letterpaar gevormd worden tussen een letter en zijn buurman. Zo kan de R verwisseld worden met elke letter behalve de E en de T. Ook dit beperkt het aantal mogelijke sleutels.

Reflectie

Uit het bovenstaande verhaal blijkt dat de Engelse cryptoanalisten allerlei zwaktes ontdekten. Zou je daaruit af mogen leiden dat de Enigma toch niet zo veilig was als altijd werd aangenomen?

klik hier

8.5 Alan Turing verslaat de Enigma

Op 4 september 1939, één dag nadat Neville Chamberlain, premier van het Verenigd Koninkrijk, aan Duitsland de oorlog verklaarde, verhuisde Alan Turing naar Bletchley Park. Turing had op dat moment zijn sporen in de academische wereld al verdiend met het bedenken van de Turing-machine. Ondanks dat de techniek nog niet in staat was deze te bouwen, was hij daarmee, voortbouwend op de ideeën van Babbage, feitelijk de uitvinder van de programmeerbare computer.
Turing zou een andere aanpak kiezen in het kraken van de Enigma-sleutel die niet afhankelijk was van het herhalen van de dagsleutel aan het begin van een bericht.
Een van de dingen die hij ontdekte in het bestuderen van oude berichten was, dat de Duitsers in het eerste bericht na 6.00 uur dagelijks een weerbericht rondstuurden. Uit ervaring wist hij dat in een onderschept bericht om die tijd het eerste woord op de tweede regel bijna zeker het woord *wetter* was. Zo'n stukje klare tekst opent een kier tussen de deur voor de cryptoanalist en wordt een *spieker* genoemd (in het Engels een *crib*).

Hieronder doen we een poging, ontleend aan het boek van Simon Singh, om de vondst van Turing om de Enigma te kraken toe te lichten. Allereerst laat het onderstaande vereenvoudigde voorbeeld zien hoe de plek van de spieker bepaald kan worden. Het is gebaseerd op het gegeven dat vanwege de reflectoren een letter nooit aan zichzelf gekoppeld kan worden. Een *a* in de klare tekst kan dus nooit een A in de cijfertekst opleveren:

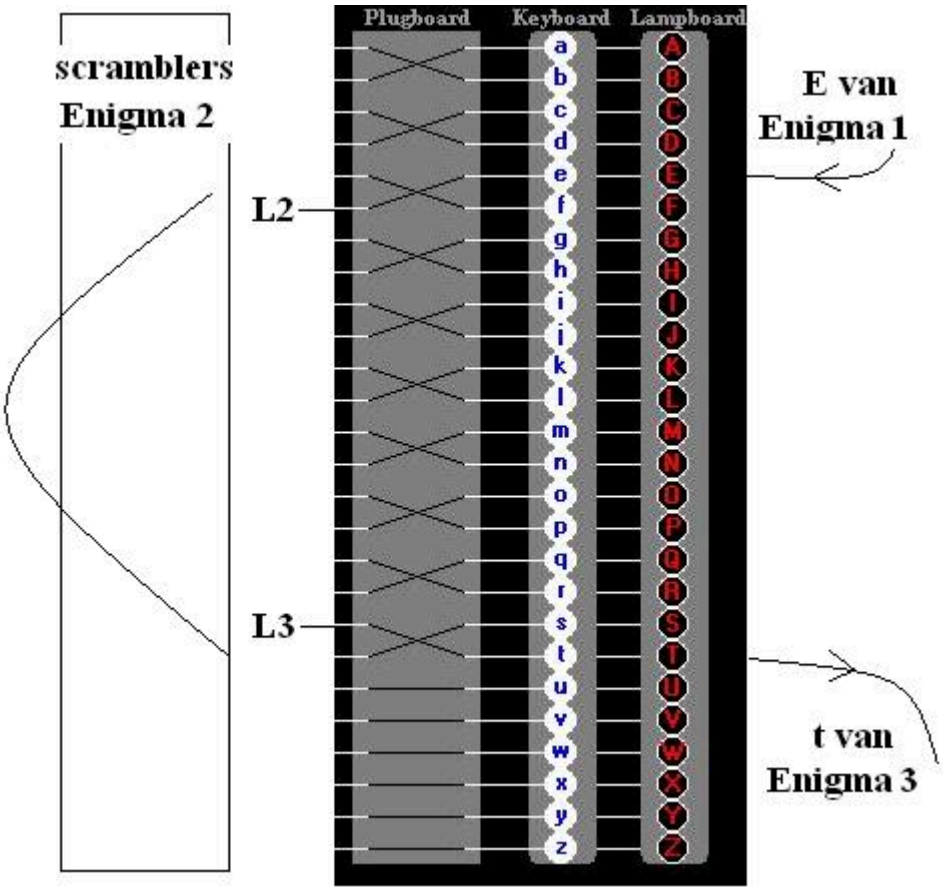
Gegokte klare tekst: w e t t e r n u l l s e c h s

Bekende cijfertekst: R E T J W P X J J S X C P L E J W Q

Het schuiven van de klare tekst over de cijfertekst levert niet veel mogelijkheden. In de getoonde stand wordt een *e* aan een E gekoppeld en de *t* aan de T en dat is dus onjuist. Een plaatsje naar links wordt de *t* aan de T en de *s* aan de S en de *c* aan de C gekoppeld enzovoorts. Het is daarbij handig als de spieker enige lengte heeft!
Vervolgens ontdekte Turing een ander soort lussen tussen de klare tekst en de cijfertekst zoals in het volgende voorbeeld:

Gegokte klare tekst: w e t t e r n u l l s e c h s

Bekende cijfertekst: E T J W P X J J S X C P L E J



In dit voorbeeld is de***w*** aan de **E**gekoppeld, de ***e*** aan de **T** en de ***t*** weer aan de **W**. Turing bedacht om drie Enigma's aan elkaar te koppelen door de E van machine 1 te koppelen aan de *e* van machine 2, de T van machine 2 aan de *t* van machine 3 en de W van machine 3 aan de *w*van machine 1. De schakelborden zouden de letters verwisselen, maar dat zou voor iedere machine hetzelfde zijn. Daarmee werden de schakelborden eigenlijk geneutraliseerd. Schematisch kunnen we het ons zo voorstellen dat door het schakelbord de ***w*** wordt omgezet in de letter $\mathbf{L_1}$, de ***e*** in de letter $\mathbf{L_2}$ en de ***t*** in letter $\mathbf{L_3}$. In de figuur hiernaast wordt de ***e***correct verbonden met de **T** als de scramblers van Enigma 2 in de juiste positie staan.

De scramblerinstelling van machine 2 werd 1 stap vóór gezet op die van machine 1 en die van machine 3 werd 3 stapen vóór gezet op die van machine 1, immers bij iedere aanslag gaat de scramblerinstelling 1 positie verder. Als de scrambler alle 17576 standen doorloopt is er een stand waarin de verbindingen door de scramblers bij alle drie de machines goed zijn. In deze stand is het circuit gesloten en gaat er een stroompje lopen. Dit geeft een signaal waardoor we weten dat de juiste scramblerstand gevonden is.

Daarbij zijn we er even van uitgegaan dat de drie scramblers de juiste zijn en in de goede volgorde staan. Zoals we weten zijn er echter 60 mogelijkheden om 3 scramblers van 5 op volgorde te zetten, zodat alle 60 scramblerschikkingen moeten worden uitgeprobeerd.

Op 10 mei 1940 veranderden de Duitsers hun protocol en vanaf dat moment zou de scramblerorientatie niet meer tweemaal vooraf aan een bericht gestuurd worden. Turing bouwde echter nieuwe *Bombes* gebaseerd op zijn eigen idee. Op 8 augustus arriveerde de eerste *Bombe* op Bletchley Park. Eind 1942 was dit aantal opgelopen tot 49. Zij zouden een hoofdrol vervullen in het ontcijferen van de geheime boodschappen van de Duitsers en hun invloed uitoefenen op het verloop van de geschiedenis.

Een uitgebeidere uiteenzetting over de *Bombes* van Turing is te vinden op het internet.

Reflectie

Turing slaagde er op zijn manier in om het Enigma-probleem te ontrafelen in het probleem van de scramblerstand en het probleem van de schakelingen via het schakelbord. Hoe wordt het probleem van de schakelingen opgelost in het systeem van Turing?

klik hier

Voor de volledigheid moet er een klein stukje toegevoegd worden aan bovenstaand verhaal. Ieder onderdeel van het Duitse leger gebruikte zijn eigen variant van de Enigma. Het Duitse leger in Noord-Afrika had een eigen netwerk evenals het leger in Europa en evenals de Luftwaffe. Op Bletchley Park waren er daarom diverse afdelingen die zich bezig hielden met de diverse Enigma's. De Enigma van de Duitse marine was het best beveiligd. Er was een keuze uit 8 scramblers en de operateurs vermeden zorgvuldig stereotiepe berichten.
Het gevolg was dat het systeem niet te kraken was en de Duitse U-boten heersten op de Atlantische Oceaan. Tussen juni 1940 en juni 1941 verloren de geallieerden gemiddeld 50 schepen per maand en in de totale Tweede Wereldoorlog verloren 50.000 geallieerde zeelieden het leven. De enige weg om toch over de codes te kunnen beschikken was in dit geval door ze te stelen. Bij aanvallen op onderzeëers werden codeboeken buitgemaakt waarmee de cijferteksten opieuw te kraken waren. De admiraliteit waakte er echter voor niet al te duidelijk van de verkregen informatie gebruik te maken om de schijn in tact te houden dat de communicatie voor de Duitse bevelhebbers veilig was.

 Reflectie

De Duitse operateurs van de marine vermeden zorgvuldig het verzenden van stereotiepe berichten. Wat voor gevolg had dit voor de codeanalisten?

klik hier

De operatie waarin Bletchley-Park informatie verzamelde uit Duitse, Italiaanse en Japanse berichten staat bekend als *the Ultra Secret*. Voor degenen die hadden bijgedragen aan het grote succes, waardoor de oorlog zeker enkele jaren korter heeft geduurd, was het zuur, dat na de oorlog alles geheim moest blijven. De Britten wilden nog tot lang na de oorlog gebruik blijven maken van het decodeersysteem. Duizenden buitgemaakte Enigma's werden verspreid over de landen van het Gemenebest en door deze landen gebruikt zonder dat deze wisten dat de Enigma al door Engeland was gekraakt. In 1974 werd het boek van kapitein F.W.Winterbotham over 'the Ultra Secret' gepubliceerd en kreeg iedereen eindelijk de erkenning die hij of zij verdiende. De Enigma's werden toen al niet meer gebruikt. Onder het kopje 'De Navajo code' vind je een beschrijving van de curieuze rol van de Navajo-indianen in WO-II.

De Navajo code

Zoals de Duitsers hun Enigma hadden, hadden de Japanners in de oorlog een systeem dat bekend stond als Purple. De Amerikanen slaagden erin in 1942 Purple te breken, waardoor het Japanse leger belangrijke tegenslagen werden bezorgd. Het Britse leger gebruikte de Typex-cijfermachine en de Amerikanen de Sigaba. Beide machines waren complexer dan de Enigma, maar belangrijker nog, ze werden juist gebruikt zonder cilly's, beperkingen op schakelborden of scramblers en zonder stereotiepe berichten. Hierdoor bleven ze ongebroken.
De cijfermachines hadden duidelijk ook een nadeel, omdat ze zich niet leenden voor communicatie in moeilijke gebieden. Als haast geboden was werd er gewoon in het Engels gecommuniceerd waardoor waardevolle informatie verloren ging.

Philip Johnston bedacht in 1942 een systeem dat zeer eenvoudig was en niet te kraken. Johnston was grootgebracht in een van de Navajo reservaten in Arizona. Hij was een van de weinigen die doorgedrongen was tot deze gesloten cultuur, die gevrijwaard was van taalinvloeden van buitenaf. Het Navajo is familie van het Na-Dene, dat aan geen enkele Aziatische of Europese taal verwant is. Om die reden kon deze taal uitstekend dienst doen als codetaal. Het enige probleem was, dat niemand de taal kon spreken behalve de Navajo indianen. Alle andere indianenstammen waren vóór de oorlog al bezocht door Duitse studenten waardoor deze talen niet veilig leken als codetaal.
De Amerikaanse marine besloot tot een experiment. Vier maanden na de bombardementen op Pearl Harbor op 7 december 1941, startte het marineverbindingscorps met een cursus communicatie voor 29 Navajo codesprekers. Ter vervanging van militaire Engelse termen werd een ondubbelzinnige woordenlijst opgebouwd met Navajo termen. In plaats van vliegtuigen kozen de recruten vogelnamen en visnamen voor schepen.
Als test werd een opname van geseinde berichten doorgegeven aan de inlichtingendienst van de marine. Na 3 weken ingespannen cryptoanalyse moesten de experts erkennen dat ze geen stap verder gekomen waren.

Na enkele aanloopmoeilijkheden werden de Navajo sprekers ingezet in de strijd tegen de Japanners, die de Amerikanen grote nederlagen hadden toegebracht. Omdat woorden die niet vertaald konden worden in het Navajo, gespeld moesten worden met het speciale Navajo codealfabet maakte dit de berichten gevoelig voor frequentieanalyse. Hiervoor bedacht men *homofonen*, vervangers voor letters die vaak voorkwamen.
Uiteindelijk werden er 420 Navajo codesprekers ingezet en naarmate de strijd verhevigde speelden de Navajo-indianen een steeds belangrijker rol. Dankzij de snelle communicatie wisten de Amerikanen de overhand te krijgen op de Japanners. De regering verbood het de indianen na de oorlog te praten over hun aandeel. Net als de cryptoanalisten van Bletchley Park raakte hun werk in de vergetelheid totdat in 1968 de Navajo-code van de geheime lijst werd afgevoerd. In 1982 werden de Navajo indianen geëerd en 14 augustus werd uitgeroepen tot de Nationale Navajo codesprekersdag.

Voor wie haar niet kent is een moedertaal zonder betekenis. Archeologen hebben met het vertalen van oude geschriften in talen die verloren zijn gegaan hetzelfde probleem als de Japanse cryptoanalisten hadden met het Navajo. De ontcijfering van oude geschriften rekenen we echter niet onder de strijd tussen cryptografen en cryptoanalisten, simpelweg omdat er geen cryptografen meer zijn. De manier waarop onderzoekers oude geschriften hebben weten te ontcijferen doet echter sterk denken aan de manier waarop cryptoanalisten werken.

Over dit lesmateriaal

Colofon

Auteurs	Bètapartners
Team	Wikiwijs Maken Auteurs
Laatst gewijzigd	18 december 2014 om 14:09
Licentie	De Nederlandse Creative Commons 3.0 licentie waarbij de gebruiker het werk mag kopiëren, verspreiden en doorgeven en afgeleide werken mag maken onder de voorwaarden: Naamsvermelding en Gelijk Delen, zie http://creativecommons.org/licenses/by-sa/3.0/nl/. Meer informatie over de CC Naamsvermelding-GelijkDelen 3.0 Nederland licentie licentie.

Aanvullende informatie over dit lesmateriaal

Van dit lesmateriaal is de volgende aanvullende informatie beschikbaar:

Leerniveaus	HAVO 5
Leerinhoud en doelen	Wiskunde D, Inzicht en handelen
Eindgebruiker	leerling/student
Trefwoorden	e-klassen rearrangeerbaar