Opdrachten Enigma

# Versleutelen

De Enigma kan op een groot aantal manieren worden ingesteld. Voordat we de Enigmacode kunnen breken, moeten we eerst weten hoe deze werkt.

We gebruiken hiervoor een Enigma-simulatie, die je kan vinden op de volgende link.

<http://enigma.louisedade.co.uk/enigma.html>

**Opdracht:** Zet de Enigma op de standaardinstellingen door op *Clear Settings* te klikken. Wat gebeurt er als je een aantal A’s achter elkaar versleuteld? Wat zie je gebeuren in de vakjes bij *Grundstellung*? Blijf net zo lang doorgaan tot de *Grundstellung* met een B begint.

**Opdracht:** Zet de Enigma weer op zijn standaardinstellingen. Zet nu de *Grundstellung* op AAB. Versleutel weer een aantal A’s achter elkaar. Wat is de overeenkomst met het vorige resultaat?

We hebben nu gezien dat de *Grundstellung* het resultaat als het ware verschuift; het maakt blijkbaar niet uit of de Enigma van te voren op AAB gezet is of dat deze via het rotormechanisme daarop komt te staan. We hebben echter nog niet naar de andere elementen gekeken.

**Opdracht:** Zet de Enigma weer op zijn standaardinstellingen en sluit in het *Steckerbrett* A en B op elkaar aan door in het veld onder A een B te zetten. Versleutel nu een aantal B’s achter elkaar. Vergelijk het resultaat met dat van de vorige opdrachten. Wat valt je hieraan op?

**Opdracht:** Zet de Enigma weer op zijn standaardinstellingen en zet de *Ringstellung* op AAB. Versleutel nu een aantal **A**’s achter elkaar. Ga in ieder geval door tot de *Grundstellung* met een B begint. Vergelijk het resultaat weer met de eerdere resultaten. Welke overeenkomsten zie je en welke verschillen zie je?

**Opdracht:** Zet de Enigma terug naar zijn standaardinstellingen en draai de wielen om door de *Walzenlage* op III, II, I te zetten. Versleutel weer een aantal A’s achter elkaar. Zie je nog overeenkomsten met de vorige resultaten?

Je gaat nu een stuk tekst versleutelen alsof je een Duitse radio-operator bent. Je ziet hieronder een deel van het codeboek voor de maand november.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Datum | Walzenlage | Ringstellung | Steckerverbindungen | Grundstellung |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| 23 | I II III | W N M | HK CN IO FY JM LW | rao |
| 22 | III I II | C K U | CK IZ QT NP JY GW | vqn |
| 21 | II III I | B H N | FR LY OX IT BM GJ | xio |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

Je hebt de opdracht gekregen het onderstaande bericht te versleutelen en te versturen. Je ziet dat er cijfers, leestekens en spaties in staan die het toestenbord van de Enigma niet heeft. Het was gebruikelijk om leestekens weg te laten. Cijfers werden per cijfer uitgeschreven (*eins*, *zwei*, *drei*, *vier*, *fünf*, *sechs*, *sieben*, *acht*, *neun*, *nul*). Spaties werden normaal vervangen door een X. Je ziet ook een letter met een umlaut (zoals de ö in Dönitz) staan. In het Duits is het gebruikelijk om deze te vervangen door de letter gevolgd door een E.

An: Dönitz

Steuere Tanafjord an. Standort Qu. AC 4992, Fahrt 20 sm.

Scharnhorst

De vertaling hiervan is

Aan: (admiraal) Dönitz

Vaar richting de Tanafjord. Positie vierkant AC 4992, snelheid 20 zeemeil.

(Slagkruiser) Scharnhorst

**Opdracht:** Zet dit bericht om in een bericht dat door de Enigma versleuteld kan worden. Hier mogen dus alleen letters in voorkomen.

**Opdracht:** Versleutel dit bericht met de gegeven instellingen en wissel het bericht uit met je buurman. Laat hem of haar jouw versleutelde bericht weer ontsleutelen en ontsleutel zijn of haar bericht.

Om te voorkomen dat er te veel berichten met dezelfde instellingen werden versleuteld, werd voor elk bericht een nieuwe *Grundstellung* gekozen. Deze werd twee keer versleuteld met de *Grundinstellung* van die dag, en de rest van het bericht werd daarna versleuteld met die nieuwe instelling.

**Opdracht:** Kies een *Grundstellung* van drie letters en versleutel die twee keer met de gegeven *Grundstellung*. Versleutel daarna het bericht hierboven met die nieuwe instelling. Wissel het bericht uit met je buurman en ontsleutel elkaars bericht.

# Enigma breken

Deze opdracht is best lastig en tijdrovend. Het kan zijn dat je hier tijdens het keuzecollege niet aan toekomt. Als je het leuk vindt om meer te weten van hoe de Enigma in de jaren ’30 van de vorige eeuw gebroken werd door de Polen kan je deze opdracht doen.

We gaan een Enigmabericht breken door middel van de karakteristiekenmethode van Marian Rejewski. Deze methode maakt ervan gebruik dat de Duitsers per bericht een andere *Grundstellung* kozen, en die twee keer verstuurden. De Polen verzamelden veel versleutelde berichten, en gebruikten de eerste zes karakters om de instellingen van de Enigma te kraken. Ze noemden deze letters *indicatoren*.

Hieronder zie je de indicatoren van 30 berichten die onderschept zijn.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| YABANP | NGLMBO | DASTNY | ECGIAW | AMIVMH |
| TFAUJE | CJKSHA | BTRLWM | HRDHCC | KBDJVC |
| ZZYERB | XYFXXR | LKTBYQ | ZNQETG | SEZZST |
| PIPPOS | MPNNLL | VVMFDX | RCBOAP | ISORFI |
| ULUYGJ | GWWWEZ | QXHQIN | OUVCUK | BOCLQU |
| FOSDQY | WHJGZD | TEXUSF | EQAIPE | JDEKKV |

Om de karakteristieken van de Enigma-instellingen te vinden, maken we gebruik van het feit dat we weten dat de eerste en vierde letter, de tweede en vijfde letter en de derde en zesde letter hetzelfde zijn. Hier maken we cykels, een soort van lussen, van: we schrijven bijvoorbeeld op dat een Y op de eerste plek altijd betekent dat er een A op de vierde plek is, een A op de eerste plek betekent dat er een V op de vierde plek is enzovoorts. Op een gegeven moment kom je weer bij de Y uit en is de cykel compleet.

**Opdracht:** Zoek voor de drie letterparen uit welke cykels er zijn, en schrijf op wat de lengtes ervan zijn. Omdat we niet weten welke stekkers in het *Steckerbrett* zitten, kunnen we niet precies gebruiken welke letters we zien, maar wel hoe lang de cykels zijn.

Je hebt nu een aantal cykels gevonden. De karakteristiek van deze instelling is per letterpaar het aantal cykels en de lengte van de langste cykel. De Polen hadden een catalogus waar ze alle karakteristieken in opsloegen, zodat ze de instellingen van de Enigma konden vinden. Ze sloegen op wat de *Walzenlage* was, en wat de oorspronkelijke *Grundstellung* was. Bovendien konden ze hier de cykels zelf vinden voor de situatie dat het *Steckerbrett* niet gebruikt was.

**Opdracht:** Op onderstaande URL kan je een versie van deze catalogus vinden. Zoek de karakteristieken die je gevonden hebt op. Welke instellingen horen hierbij?

[https://gist.github.com/ralfvandenbroek/6f47175d944178a3ecd22da367935a9dh](https://gist.github.com/ralfvandenbroek/6f47175d944178a3ecd22da367935a9d)

Nadat de *Walzenlage* en de *Grundstellung* bekend waren, konden de Polen de stekkers in het *Steckerbrett* opzoeken. Ze deden dit door de cykels die in de catalogus staan, te vergelijken met die ze gevonden hadden. In dit geval weten we dat de Duitsers die dag 6 stekkers gebruikten. Dat betekent dat er 6 paren letters zijn die omgedraaid zijn als je de standaard cykels in de catalogus vergelijkt met de cykels die je zelf gevonden hebt.

Onthoud dat de cykels lussen zijn: (ABC), (BCA) en (CAB) zijn exact dezelfde cykels. Als je dus (ABC) in de catalogus ziet en (CKB) in wat je gevonden hebt, duidt dat erop dat er een stekker tussen de A en de K zit.

**Opdracht:** Zoek uit wat de instellingen van het *Steckerbrett* waren.

We hebben nu alles gevonden, op de *Ringstellung* na. Deze kan alleen gevonden worden door alle instellingen te proberen tot we een goed bericht vinden. De Polen maakten er gebruik van dat veel Duitse berichten begonnen met de tekst ‘An:’ gevolgd door een spatie. In de Enigma werd dat ANX. De instellingen die eerder gevonden zijn gingen ervanuit dat de *Ringstellung* AAA was. Als echter de *Ringstellung* AAB is, moet de *Grundstellung* ook aangepast worden; de laatste letter daarvan moet dan ook één positie opgeschoven worden. Een *Grundstellung* van OQI wordt dus OQJ als de *Ringstellung* AAB is, OQK als deze AAC is enzovoorts.

**Opdracht:** Probeer de onderstaande tekst te ontsleutelen. Onthoud dat de eerste zes letters de *Grundstellung* voor de rest van het bericht aangeven. Om het zoeken wat sneller te maken, is gegeven dat de eerste twee letters van de Ringstellung een A zijn.

JDEK KVKR FYXH UGAV HTNB OVLD XUNA FJIS FHOC MOKK YHKI RBWO EWYO DQRZ