# GEHEIME CODES

## OF HOE WISKUNDE EEN OORLOG KAN BEÏNVLOEDEN

dr. Luc Gheysens
2014

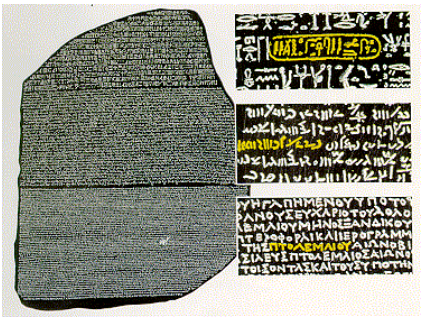
---

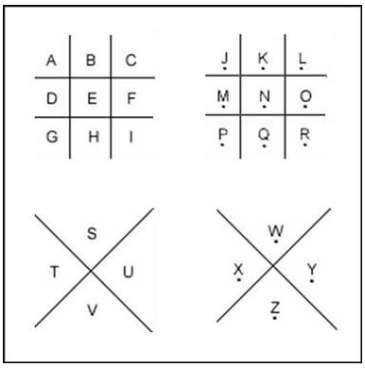
Codering in vredestijd

1. De steen van Rosette
2. Code van de vrijmetselaars
3. ASCII-code
4. ISBN-code
5. QR-code

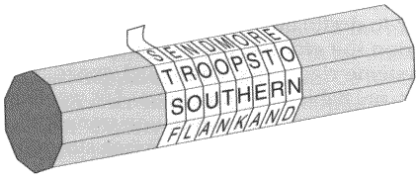
Codering in oorlogstijd

6. Scytale
7. Caesarcode
8. Vigenèrecijfer
9. ADFGX-code in WO I
10. ENIGMA in WO II







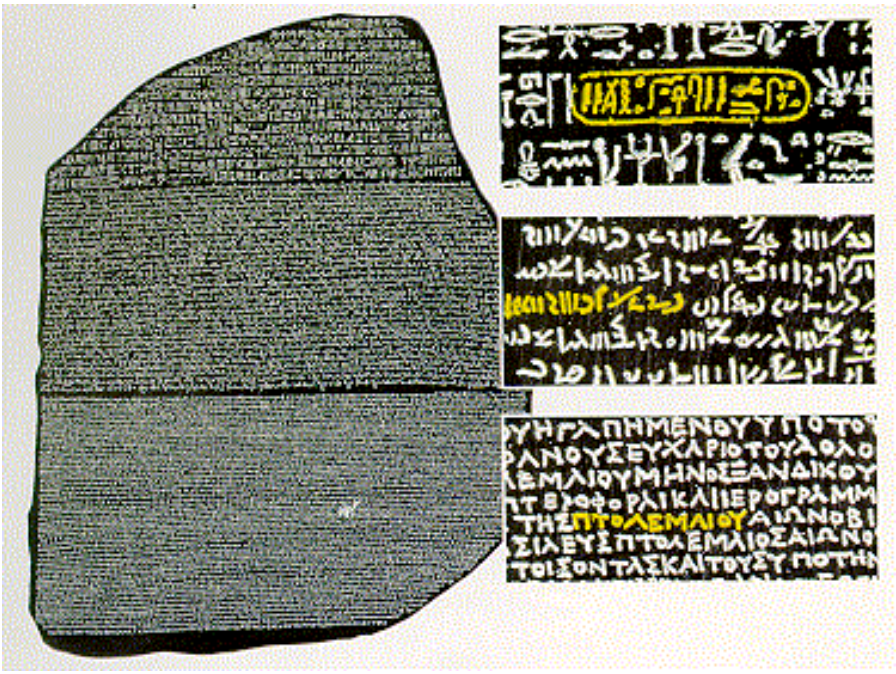



| | A | D | F | G | X |
|---|---|---|---|---|---|
| A | R | M | G | S | Z |
| D | W | N | A | L | Y |
| F | B | T | F | I/J | Q |
| G | X | U | D | V | K |
| X | H | E | O | P | C |

## De steen van Rosette

De steen van Rosette is zeer belangrijk geweest voor het ontcijferen (decoderen) van het hiëroglyfenschrift van de Egyptenaren. De steen stamt uit de tijd rond 200 v. Chr., is gemaakt van basalt en weegt 762 kg. De afmetingen zijn 118 x 77 x 30 cm. De tekst op de steen gaat over de kroning van farao Ptolemaeus.

De steen was voor het ontcijferen belangrijk omdat er drie keer dezelfde tekst op staat in telkens een andere taal:



Hiëroglyfenschrift (bovenaan): gebruikt door de oude Egyptenaren
Demotisch (in het midden): een oud Egyptisch schrift
Grieks (onderaan)

De steen werd in juli 1799 tijdens een expeditie van Napoleon naar Egypte, gevonden bij Rosette, vlakbij Rashid. Dit ligt ongeveer 200 km ten noorden van Cairo aan de kust van de Middellandse Zee. Tot dan toe was niemand er in geslaagd de oud Egyptische teksten die tijdens opgravingen waren gevonden te ontcijferen. Maar dit veranderde door de vondst van de steen van Rosette. Omdat het Demotisch en het Grieks bekend waren slaagde de Fransman Jean-François Champollion er, na zo'n twintig jaar in, het hiëroglyfenschrift te ontcijferen (1821).

Bron : http://histoforum.digischool.nl/rosette/rosette.htm

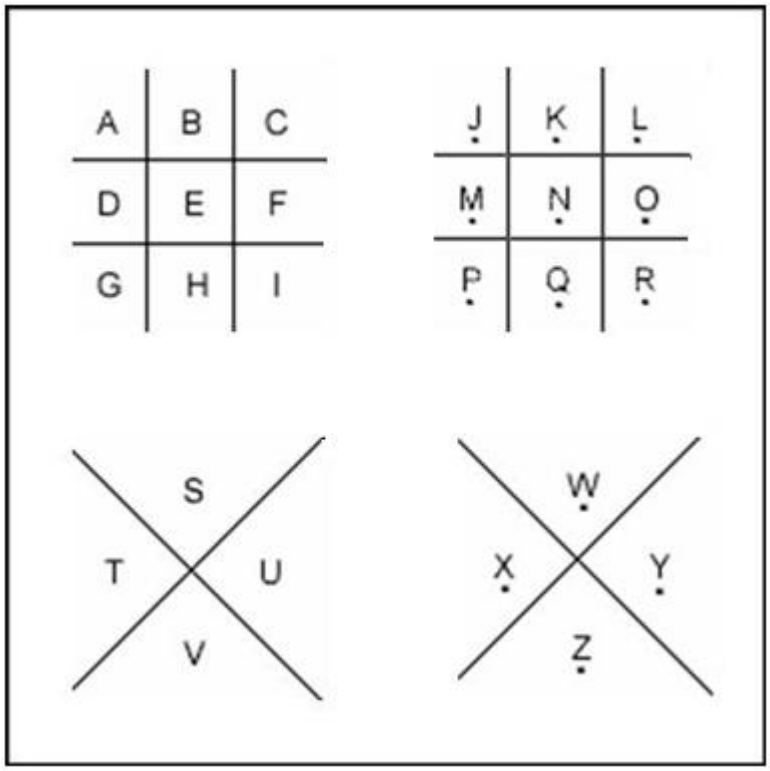
## VRIJMETSELAARS CODE

Het **rozenkruisersgeheimschrift** (ook wel vrijmetselaarsalfabet) is een methode van coderen waarbij de letters vervangen worden door eenvoudig te onthouden diagrammen.

De methode, die ook onder de minder lovende naam varkenshokversleuteling (of pigpen) bekend is, wordt in het algemeen toegeschreven aan de rozenkruisers. Dit geheim genootschap van wijsgerigen zou het gebruikt hebben om haar geheimen mee te bewaren.

De oudst bekende variant is van Heinrich Cornelius Agrippa von Nettesheim die de methode uitlegt in zijn De occulta philosophia uit 1533. Dit werk werd in 1586 door Blaise de Vigenère hergebruikt in zijn tractaat aangaande geheimschrift. Er zijn vele varianten mogelijk, een geoefend cryptoanalist zal doorgaans echter geen moeite hebben met de ontcijfering.

In de 18de eeuw maakten Vrijmetselaars hiervan gebruik voor hun archieven.




Voorbeeld.


Opdracht.
Wat staat hier?

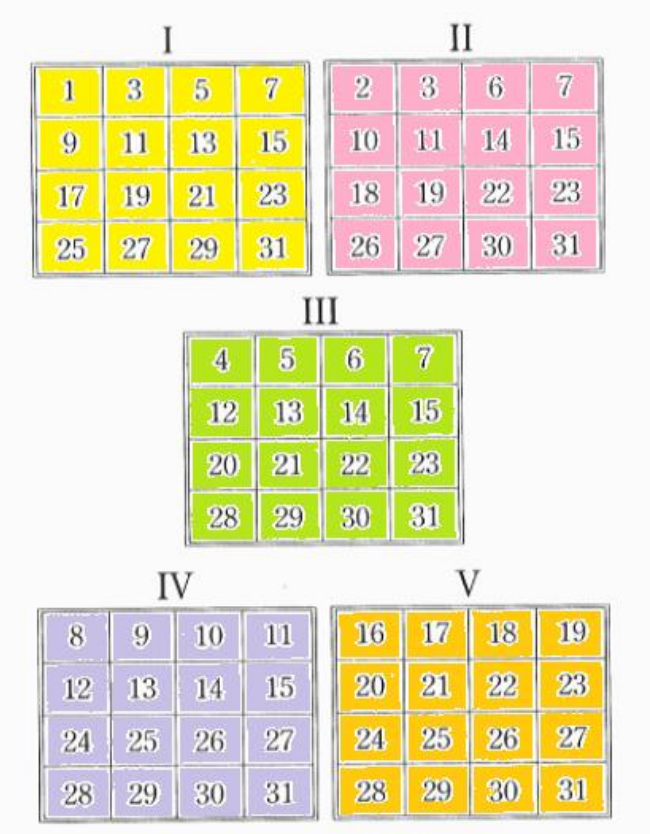
## ASCII-CODE

**ASCII** is een afkorting van *American Standard Code for Information Interchange* en is een standaard om een aantal letters, cijfers, leestekens en andere symbolen te representeren en aan ieder teken in die reeks een geheel getal te koppelen, waarmee dat teken kan worden aangeduid. De code werd ontworpen door Bob Bemer. Bron: Wikipedia.

| Dec | Oct | Hex | Binair | Code | Dec | Oct | Hex | Binair | Code | Dec | Oct | Hex | Binair | Code |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 32 | 040 | 20 | 0100000 | SP | 64 | 100 | 40 | 1000000 | @ | 96 | 140 | 60 | 1100000 | ` |
| 33 | 041 | 21 | 0100001 | ! | 65 | 101 | 41 | 1000001 | A | 97 | 141 | 61 | 1100001 | a |
| 34 | 042 | 22 | 0100010 | " | 66 | 102 | 42 | 1000010 | B | 98 | 142 | 62 | 1100010 | b |
| 35 | 043 | 23 | 0100011 | # | 67 | 103 | 43 | 1000011 | C | 99 | 143 | 63 | 1100011 | c |
| 36 | 044 | 24 | 0100100 | $ | 68 | 104 | 44 | 1000100 | D | 100 | 144 | 64 | 1100100 | d |
| 37 | 045 | 25 | 0100101 | % | 69 | 105 | 45 | 1000101 | E | 101 | 145 | 65 | 1100101 | e |
| 38 | 046 | 26 | 0100110 | & | 70 | 106 | 46 | 1000110 | F | 102 | 146 | 66 | 1100110 | f |
| 39 | 047 | 27 | 0100111 | ' | 71 | 107 | 47 | 1000111 | G | 103 | 147 | 67 | 1100111 | g |
| 40 | 050 | 28 | 0101000 | ( | 72 | 110 | 48 | 1001000 | H | 104 | 150 | 68 | 1101000 | h |

**BINAIRE CODE: 42 (decimaal) wordt 101010 (binair)**

**Binaire toverkaartjes**




"Er zijn maar 10 soorten mensen: zij die de binaire code begrijpen en zij die ze niet begrijpen"

## ISBN-code

**ISBN** staat voor **Internationaal Standaard Boeknummer.**

Het ISBN bestaat uit dertien cijfers, opgebouwd uit vijf opeenvolgende groepen.

Het **prefix** onderscheidt een ISBN van andere productcodes. Zulke productcodes worden gebruikt door EAN International (EAN = European Article Numbering). EAN International heeft aan ISBN's twee prefixen toegewezen, elk van drie cijfers: 978 en 979. In 2008 is alleen het prefix 978 in gebruik.

De **registratiegroep** geeft doorgaans het land van publicatie aan, maar kan ook het taalgebied vertegenwoordigen. Zo is voor Nederland, maar ook voor Nederlandstalig België, dit groepsnummer 90; ook het nieuwe 94 komt beschikbaar. Dit groepsnummer is dus tweecijferig.

De **uitgeversaanduiding** is een cijferreeks, opnieuw van uiteenlopende lengte, die de uitgever definieert. De vuistregel luidt: hoe groter het uitgeversfonds is, des te korter is de uitgeversaanduiding. Zo blijft er opnieuw optimale ruimte over voor de titelaanduiding. Bekende uitgevers in het Nederlandse taalgebied krijgen twee of drie cijfers: zo identificeert 02 de Standaard Uitgeverij en 20 Uitgeverij Lannoo.

De **titelaanduiding** identificeert de "titel": een bepaald werk in een bepaalde uitvoering, en uitgegeven door een bepaalde uitgever. In deze groep kunnen in het Nederlandstalige gebied maximaal vijf cijfers worden toegekend.

Het **controlecijfer** wordt toegevoegd ter voorkoming of correctie van fouten in het ISBN.

Voorbeeld.

**ISBN** **:**9789020998566
**Verkoopprijs** **:**19,99 EUR


**Afwerking** **:**Paperback
**Druk** **:**1
**Aantal pagina's:**144
**Uitgave** **:**Uitgeverij Lannoo

ISBN 978 – 90 – 20 – 99856 – 6

978: prefix voor boeken
90: verwijst naar het land (België)
20: verwijst naar Uitgeverij Lannoo
99856: SOS Piet 5
6: controlecijfer.

Het controlecijfer wordt als volgt berekend. Uitgegaan wordt van het ISBN dat aan een uitgave is toegekend, maar dat nog geen controlecijfer heeft. Het heeft dus nog slechts twaalf cijfers.

1. Tel de cijfers samen op de oneven posities.
2. Tel de cijfers samen op de even posities en vermenigvuldig die som met 3.
3. Tel de twee gevonden sommen samen.

Men kijkt dan hoeveel deze som verschilt van het daarop volgende hogere tiental. Dat verschil is het controlecijfer. Als het verschil 10 is, dan is het controlecijfer 0.

Voor SOS Piet 5 wordt dit:

$$(9 + 8 + 0 + 0 + 9 + 5) + 3 \bullet (7 + 9 + 2 + 9 + 8 + 6) = 31 + 3 \bullet 41 = 31 + 123 = 154.$$

Het daarop volgende hogere tiental is 160 en 160 – 154 = 6. Dit is het controlecijfer.

---

Opdracht.

De Derde Slag Bij Ieper 1917 (Koen Koch) : E-book


Voor de geallieerden was 1917 het zwartste jaar in de Eerste Wereldoorlog. De Russische Revolutie betekende het einde van de Russische deelname aan de oorlog, onder de Franse soldaten waren muiterijen uitgebroken en de Duitse onderzeebootoorlog dreigde de geallieerde bevoorrading lam te leggen. In deze benarde omstandigheden ondernam het Britse leger een even spectaculair als rampzalig offensief.
Deze Derde Slag bij Ieper geldt, met de slagen van de Somme en Verdun, als een van de beruchtste veldslagen van de Eerste Wereldoorlog. Koen Koch gaat in op de politieke en militaire gebeurtenissen en staat stil bij het lot van de soldaten die door de oorlogsmachine werden vermalen.

Dit boek heeft als ISBN-code 978 – 90 – 26 – 32224 – ?
Bereken het controlecijfer.

## QR-code

De letters *QR* zijn een afkorting van *Quick Response* ("snelle reactie").

Een QR-code is een tweedimensionale streepjescode die in 1994 is ontwikkeld door Denso-Wave, een dochteronderneming van het Japanse bedrijf Denso, een toeleverancier van Toyota. Ze waren dus oorspronkelijk enkel bedoeld om snel auto-onderdelen te identificeren.

QR-codes kunnen snel en eenvoudig ingescand kunnen worden met de fotocamera van bijna iedere moderne mobiele telefoon. De code wordt dan omgezet ("dequrificeren" genoemd) in (interactieve) tekst en/of een link. Je loopt bijvoorbeeld door de stad en ziet een poster voor een evenement dat interessant lijkt. Je pakt je mobiele telefoon, scant de QR-code en je krijgt direct meer informatie en een link naar een bijbehorende website waar je direct kaarten kunt bestellen. Je hoeft dus geen webadressen (URL's) meer in te typen of te onthouden en omdat QR-codes erg klein kunnen zijn, bespaart dit veel ruimte op het product. Tegenwoordig beschikken alle smartphones en tablets over een QR-codescanner.

Naargelang het aantal lettertekens van de boodschap varieert het aantal blokjes van 21 x 21 (1 tot 14 tekens) tot 61 x 61 (214 tot 251 tekens).

Op www.qurify.com kan je zelf jouw boodschappen omzetten in QR-codes (qurificeren). Hiermee kan je dan bijvoorbeeld boeken of cd's rangschikken, een identificatiecode op sleutels aanbrengen, evenementen promoten waaraan je meewerkt …

QR-code met 25 x 25 blokjes van mijn wiskundeblog
www.gnomon.bloggen.be

# SCYTALE

Een **scytale** (ook wel **skytale**, Grieks *σκυτάλη*) is een cryptografisch gereedschap dat wordt gebruikt om transpositionele versleuteling mee toe te passen. De algemene voorstelling is een cilindrisch voorwerp met daaromheen gewikkeld een strook papier. Vermoedelijk werd dit type versleuteling gebruikt door de oude Grieken. De zender en de ontvanger dienen beide een in vorm gelijk voorwerp te bezitten. In de oudheid droegen mensen frequent een wapenstok of een staf zodat ze als het ware de volledige scytale bij zich hadden. Om deze reden noemt men de scytale ook wel stafversleuteling.

Hoewel ook wel stafversleuteling genaamd kan men van veel voorwerpen een scytale maken. Bijvoorbeeld van een potlood, een glas, een vaas of zelfs een boek.

Om een tekst te versleutelen wikkelt men een strook perkament, leer, of (tegenwoordig) papier diagonaal om de cilindervorm waarna men de tekst er horizontaal opschrijft. Daarna haalt men de strook eraf en stuurt deze naar de ontvanger die op zijn beurt de strook om zijn scytale wikkelt en de tekst er weer af leest.

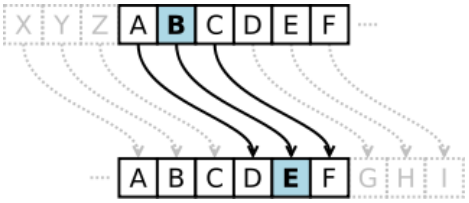
De Grieks historicus Plutarchus (1ste eeuw n. Chr.) vermeldt het gebruik van een scytale tijdens de Peloponnesische Oorlog tussen de stadstaten Sparta en Athene (5de eeuw v. Chr.) in zijn biografie van de Griekse admiraal Lysander.

Bron: Wikipedia.

## CAESARCODE

De Caesarcode of Caesarrotatie is een eenvoudig coderingssysteem waarbij men elke letter uit het alfabet vervangt door een letter die een vast aantal plaatsen verderop staat. Hierbij maakt men de afspraak dat men na de letter Z herbegint bij de letter A.

Wanneer men bijvoorbeeld elke letter vervangt door de letter die 3 posities verderop staat in het alfabet, spreekt men van Rot 3, waarbij Rot verwijst naar 'Rotatie'.




De X moet men dan vervangen door A, de Y door B en de Z door C.

Het gebruik van Caesarrotatie wordt beschreven door Suetonius, een bekend Romeins schrijver en biograaf uit de 1ste – 2de eeuw n. Chr.. Hij vermeldt het gebruik van deze methode door zowel Julius Caesar als door Augustus. Hoewel het geheimschrift naar hem vernoemd is, is van Julius Caesar bekend dat hij meer ingewikkelde methodes gebruikte.

Deze methode zou nu weinig efficiënt zijn omdat er in principe maar 25 verschillende rotaties mogelijk zijn. De computer zou de codering direct kraken. Bovendien beschikt men (in elke taal) over lijstjes met de letterfrequenties (het aantal keer dat een letter gemiddeld voorkomt in een tekst). Hieronder staat een dergelijke tabel met de frequentie van de letters in de Nederlandse taal.

| | | | | | | |
|---|---|---|---|---|---|---|
| E 19.06% | N 9.41% | T 6.74% | A 6.72% | R 6.45% | I 6.44% | D 5.91% |
| O 5.87% | S 4.00% | L 3.94% | G 3.14% | V 2.90% | M 2.41% | H 2.32% |
| K 2.28% | U 1.93% | B 1.80% | C 1.60% | P 1.59% | W 1.57% | J 1.49% |
| Z 1.18% | F 0.74% | Y 0.29% | Q 0.11% | X 0.11% | | |

Bron: Cryptografie, Monique Stienstra en Harm Bakker.

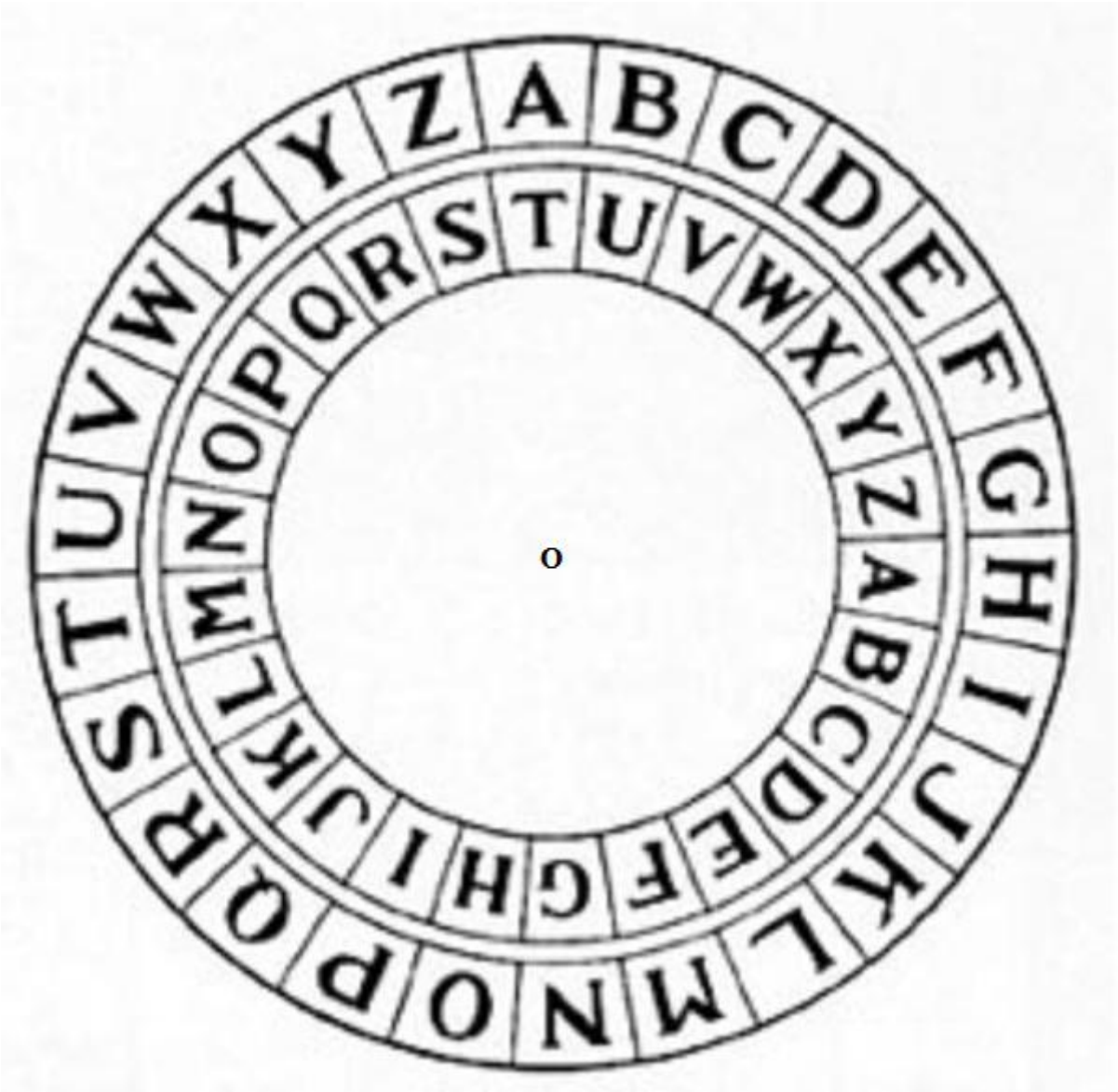
Het eenvoudigste en zelfs tot in de 20ste eeuw gebruikte cryptosysteem van dit soort is het Rot 13-systeem. Hierbij schrijft men de eerste 13 letters boven de volgende 13. Op die manier heeft men een tabel waarmee men tegelijk kan coderen en decoderen (U wordt H en een H in de gecodeerde tekst wordt terug U).

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 Z

Op http://web.forret.com/tools/rot13.asp kan je het Rot 13-algoritme zelf uitproberen.

Spelopdracht.

Maak twee kopietjes van de onderstaande figuur. Knip uit één van beide bladen het binnenste letterwieltje uit en bevestig dit centraal met behulp van een splitpen bovenop het andere blad. Je hebt meteen een rotatiewiel waarbij je – in de stijl van Julius Caesar – kunt coderen en decoderen.




Bron: www.encyclopedoe.nl/index.php?onderwerp_id=129 (met een aantal spelideetjes over geheimschrift en codering).

# Vigenèrecode

De **Vigenèrecode** is in de cryptografie één van de klassieke coderingsmethoden. Het werd uitgevonden door Giovanni Batista Bellaso in 1553, maar het was door Blaise de Vigenère 1523 - 1596) een Frans diplomaat en cryptograaf dat het algemeen bekend raakte, waardoor het zijn naam kreeg. Het werd echter zelden gebruikt vanwege zijn complexiteit.

Het systeem bestaat erin dat elke letter in de te coderen tekst vervangen wordt door een andere letter door gebruik te maken van een codewoord (dat telkens wordt herhaald) en de zogenaamde *tabula recta*, een tabel waarop op iedere regel een alfabet staat waarvan elk alfabet steeds één letter verschoven is:

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

Tabula recta

Men kiest eerst een geheim sleutelwoord, bijvoorbeeld `ZODIAK`. Dit schrijft men onder de te coderen tekst. Vervolgens zoekt men elke letter uit de te coderen tekst op in het verticale alfabet en de letter van het sleutelwoord in het horizontale alfabet. De kruising van beiden is de resulterende codeletter. Zo kunnen we zien dat de kruising van `D` en `Z` in de tabel de letter `C` is.

```
Te coderen tekst : D I T I S Z E E R G E H E I M
Sleutelwoord:      Z O D I A K Z O D I A K Z O D
                   --------------------------
Gecodeerde tekst : C W W Q S J D S U O E R D W P
```

Om te tekst CWWQS JDSUO ERDWP weer te ontcijferen schrijft men het sleutelwoord boven de gecodeerde tekst. Vervolgens zoekt men elke sleutelletter op in het horizontale alfabet dat boven de tabula recta staat en gaat naar beneden tot men de betrokken codeletter tegenkomt. De letter in het verticale alfabet (links van de tabula recta), die zich op dezelfde rij bevindt is de gezochte letter uit de oorspronkelijke tekst.

300 jaar lang dacht men dat de Vigenèrecode onbreekbaar was. Ze kreeg zelfs de bijnaam *le chiffre indéchiffrable*. In de 19e eeuw vonden Charles Babbage en Friedrich Kasiski onafhankelijk van elkaar toch een methode om ze te breken.

Merk op dat de letter E kan vercijferd worden als D, maar ook als Q en als E. Als het sleutelwoord 6 letters lang is kan eenzelfde te coderen letter tot 6 verschillende coderingen hebben. Hierdoor kan de code niet gebroken worden met een eenvoudige letterfrequentie-analyse, zoals bij een enkelvoudig substitutiecijfer.

Indien er voldoende cijfertekst is kan men echter de grootte van het sleutelwoord eruit afleiden door de grootste gemeenschappelijke deler te nemen van alle afstanden tussen veel voorkomende stukjes cijfertekst. Indien op die manier het sleutelwoord 6 letters lang blijkt, dan moet men letterfrequentie-analyse toepassen op de 6 afzonderlijke stukken van de tekst.

Opdracht.

Gebruik het woord FOSGEEN als codewoord om de volgende tekst te ontcijferen.
Fosgeen is een giftig gas en werd voor het eerst als wapen gebruikt in de Eerste Wereldoorlog door de Duitsers, op 19 december 1915.

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| d | d | w | x | m | i | g | n | g | e | u | w | x | r | w | r | y | g | w |
| | | | | | | | | | | | | | | | | | | |

Nota.
Op http://sharkysoft.com/misc/vigenere/ vind je een programma waarmee je een tekst kunt coderen en decoderen aan de hand van een vigenèrecode.

## De ADFGX-code in de Eerste Wereldoorlog

De **ADFGX-code** werd op het einde van de Eerste Wereldoorlog ingevoerd door de Duitse veld-officier Erich Ludendorff voor het Lenteoffensief in Frankrijk in 1918. De code werd bedacht door kolonel Fritz Nebel. Men koos voor de letters A, D, F, G, en X omdat deze zeer duidelijk te onderscheiden zijn in morsecode. Tijdens het offensief ontstond een variant die de letter V toevoegde en daarom sprak men over de **ADFGVX-code**. Zo kon men in een 6 x 6 rooster ook de 10 cijfers eraan toevoegen.

De ADFGX-code werd ingevoerd op 5 maart 1918, net voor het grote offensief dat begon op 21 maart. Men had een nieuwe codering nodig om het verrassingseffect te behouden, en men koos voor de ADFGX-code omdat het onbreekbaar geacht werd.

Op 6 april 1918 slaagde de cryptoanalist van het Franse Bureau du Chiffre Georges Painvin erin een bericht in de ADFGX-variant te breken. Op 1 juni 1918 kreeg Painvin het eerste bericht in de 6-letter-variant (ADFGVX) onder ogen. Met de tot dan toe opgedane kennis brak hij het bericht echter al op 2 juni. Hierdoor kregen de Fransen een aanzienlijk strategisch voordeel en wisten zij de Duitsers in een slag op 9 juni terug te dringen. Een keerpunt in het offensief.

Het breken van de versleuteling werd tot 1966 officieel geheimgehouden.

Hoe codeert men een boodschap?

1. Vertrek van een zogenaamd **Polybiusvierkant**. Dit is een, door de Griekse historicus Polybios in de 2$^{de}$ eeuw v. Chr. bedacht vierkant dat geschikt is voor codering. Hij zag hierin een middel om boodschappen via vuurtorens te versturen. Hierbij worden de 26 letters in een 5 x 5 – vierkant geplaatst (I en J plaatste men samen) met daarboven en daarnaast de codeletters. Oorspronkelijk gebruikte Polybios cijfers. Voor de ADFGX-code wordt dit bijvoorbeeld:

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

2. Zet elke letter in de tekst die je wenst te coderen om een letterpaar. De letter T wordt zo gecodeerd als FD en de letter P als XG.

   We coderen hiermee bijvoorbeeld de tekst EET MEER FRUIT.

| E | E | T | M | E | E | R | F | R | U | I | T |
|---|---|---|---|---|---|---|---|---|---|---|---|
| XD | XD | FD | AD | XD | XD | AA | FF | AA | GD | FG | FD |

3. Zet deze letterparen van links naar rechts en van boven naar onder in een nieuw rooster, met daarboven een nieuw codewoord (of een codezin). We kiezen bijvoorbeeld als codewoord BORD.

| B | O | R | D |
|---|---|---|---|
| X | D | X | D |
| F | D | A | D |
| X | D | X | D |
| A | A | F | F |
| A | A | G | D |
| F | G | F | D |

4. De letters van het sleutelwoord worden dan in alfabetische volgorde geplaatst met daaronder de overeenkomstige kolommen letters uit het bovenstaande rooster.

| B | D | O | R |
|---|---|---|---|
| X | D | D | X |
| F | D | D | A |
| X | D | D | X |
| A | F | A | F |
| A | D | A | G |
| F | D | G | F |

5. Hierin lees je nu de gecodeerde boodschap af:

   XFXAAF DDDFDD DDDAAG XAXFGF

Hoe decodeert men een boodschap?

1. De ontvanger kent het codewoord BORD en het Polybiusvierkant.
   Hij zet eerst de letters van het codewoord in alfabetische volgorde en bekomt BDOR.

2. Hij plaatst de 4 groepjes van 6 letters in kolommen onder BDOR en bekomt zo het rooster dat hierboven bij punt 4 staat.

3. Hij herschikt de letters van BDOR tot het codewoord BORD en verplaatst de vier kolommen bij deze letters tot hij het rooster bij punt 3 bekomt.

4. Hij leest in dit rooster van links naar rechts en van boven naar onder in groepjes van twee letters de gecodeerde boodschap af en bekomt zo de code

| XD | XD | FD | AD | XD | XD | AA | FF | AA | GD | FG | FD |
|---|---|---|---|---|---|---|---|---|---|---|---|

5. Met behulp van het Polybiusvierkant zet hij elk groepje van twee letters om naar een letter uit de boodschap: XD wordt E, FD wordt T enz.

Opgave. Decodeer de volgende boodschap:

GGGGDDFD GDDXDDXX DFFDGGGD XGXXFXDD

met behulp van het bovenstaand Polybiusvierkant. Het codewoord is OBUS.

1. Zet in het onderstaande rooster in de vakjes op de eerste lijn de letters van OBUS in alfabetische volgorde. Plaats dan de vier bovenstaande codes van 8 letters in de kolommen onder elke letter.

| | | | |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

2. Neem de vier kolommen over onder elke letter in het onderstaande rooster.

| O | B | U | S |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

3. Groepeer de letters per twee (van links naar rechts en van boven naar onder) en schrijf de groepjes over in de grijze hokjes in de onderstaande tabel (twee letters per vakje en van links naar rechts).

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

4. Zet onder elk groepje van twee letters in de witte vakjes de overeenkomstige letter uit het Polybiusvierkant en lees dan de boodschap af in de twee rijen met witte vakjes.
   Tip: het gaat om een evenement in 2013 in Bydgoszcz.

# ENIGMA CODEERMACHINE

Het Enigma-logo.
Enigma is Grieks voor raadsel

Het Enigma-toestel is een elektromechanische codeermachine die in de jaren twintig op de markt werd gebracht en in gebruik genomen door verscheidene Europese bedrijven en diplomatieke diensten. Het toestel was dus ontworpen voor vredelievende doeleinden.

Op 23 februari 1918 had de Duitser Arthur Scherbius als eerste een patent aangevraagd voor een zogenaamde rotormachine, een codeermachine die werkte met draaiende schijven waarop de letters van het alfabet stonden. Het was echter de Nederlander Hugo Alexander Koch die op 7 oktober 1919 in Nederland een patent aanvroeg voor een codeermachine die later bekend zou worden als Enigma, de codeermachine van de Wehrmacht vóór en tijdens de Tweede Wereldoorlog in nazi-Duitsland.

Nadat eerst de Poolse en nadien, tijdens de Tweede Wereldoorlog, de Britse inlichtingendienst erin slaagde de Enigmacodes te breken, bleek het toestel een goudmijn van informatie over de Duitse oorlogsmachine. De informatie, verkregen door ontcijfering van de geheime Duitse berichten, kreeg de codenaam "Ultra" en speelde een uiterst belangrijke rol in het verloop van de Tweede Wereldoorlog, vooral in de U-bootoorlog in de Atlantische Oceaan, de veldslagen in Afrika en de landing in Normandië.

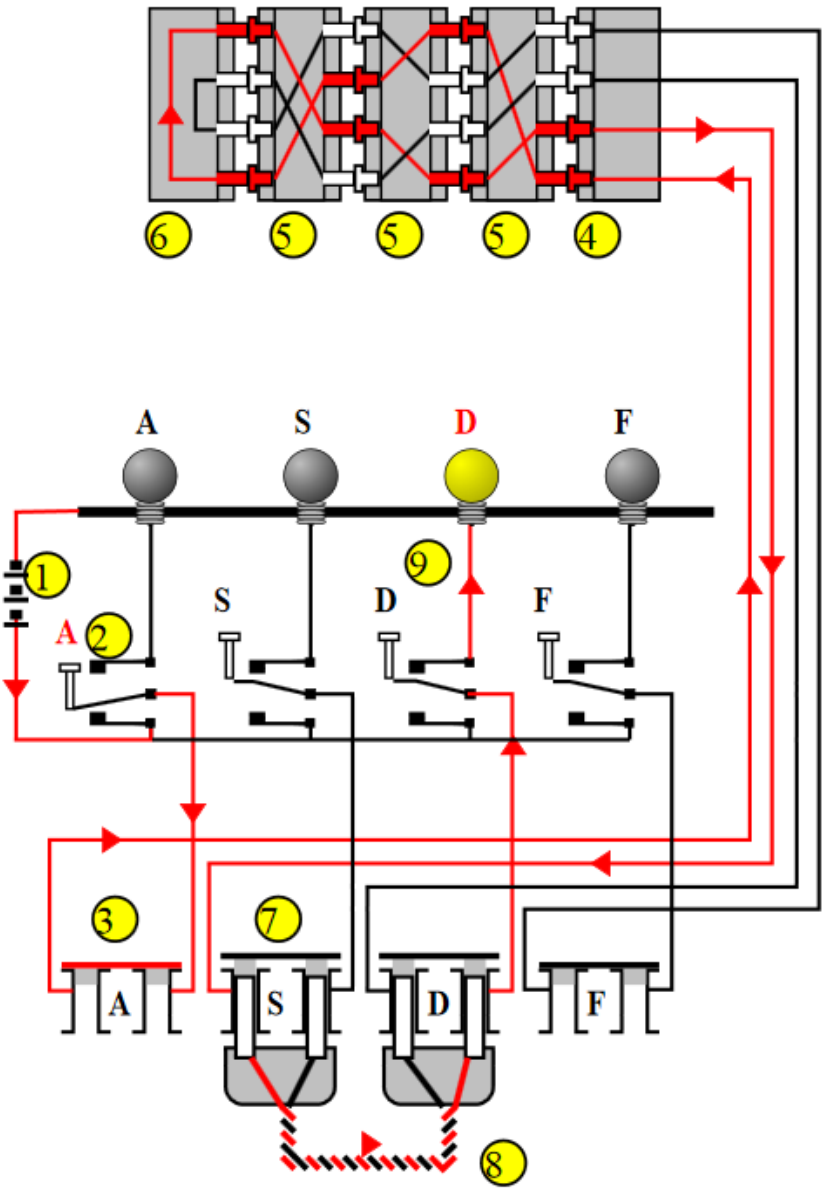
De Enigma-machine was een zeer degelijk ontwerp waarvan de code onbreekbaar leek vanwege een ongeëvenaard cryptografisch veiligheidsniveau. Het waren in beslag genomen codeboeken, fouten door operators en onveilige procedures bij de vercijfering van berichten die het breken van de Enigmacode mogelijk maakten.

*Een 3-rotor Wehrmacht Enigma in het Imperial War Museum, London.*

Hoe werkte de Enigma-machine?

De Enigma-machine is een elektromechanisch systeem. Het toestel bestaat uit een (QWERTZ-)toetsenbord, drie draaiende contactschijven, *rotors* genaamd, die worden voortbewogen door een *stappenmechanisme*, en een paneel met lampjes. De Enigma werkte dus op basis van een combinatie van een elektrische circuit en de mechanische beweging van de rotors. Het indrukken van een toets wordt via het elektromechanisch systeem vertaald in een oplichtend lampje, dat de vercijferde letter voorstelt.

Een eenvoudige simulatie vind je op http://russells.freeshell.org/enigma/ (online).
Op http://users.telenet.be/d.rijmenants/nl/enigmasim.htm kan je de mooie versie van Dirk Rijmenants downloaden.
Op http://mckoss.com/Crypto/Enigma.htm staat een papieren simulatie.



De bovenstaande afbeelding toont een machine met slechts vier letters. In werkelijkheid zijn er natuurlijk 26 letters. Via dit vereenvoudigd model kunnen we de werking van de codeermachine gemakkelijk uitleggen.

De batterij (1) levert de elektrische stroom.

De wisselschakelaar (2) wordt hier op de tekening bediend door de ingedrukte A-toets (rood).

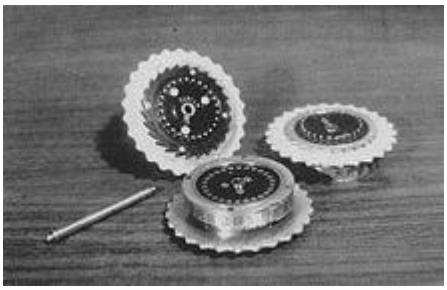
Het signaal komt toe bij de letter A (3) op het stekkerbord (7). Met behulp van kabeltjes (8) zet men een bepaalde letter om in een andere letter. Men kon dus dagelijks de plaatsing van de kabeltjes wijzigen. Op het schema is er geen kabeltje voorzien om de letter A om te zetten in een andere letter. Het blijft dus een A.

De stroom loopt daarna naar een ingangspaneel (4) en komt terecht in drie opeenvolgende rotors (5). Dit zijn draaiende cilinders die via hun interne bedrading elk lettersignaal omzetten in een andere letter.

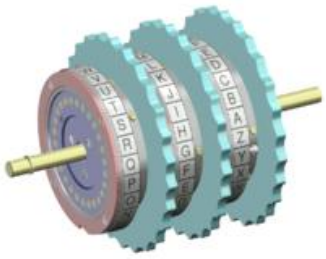
Het signaal komt terecht op de reflector (6) en gaat terug via de drie rotors. De reflector zorgde voor een reciproque codering, d.w.z. wanneer een ingetypte letter S werd gecodeerd als een letter D, werd een ingetypte D weer omgezet naar een S.

Op het schema arriveert het signaal dan op het stekkerbord (7) bij de letter S. Hier is een kabeltje (8) gelegd dat de letter S omzet in D.

Zo komt de stroom uiteindelijk op het toetsenbord terecht bij de letter D (9) waar een lampje gaat branden.

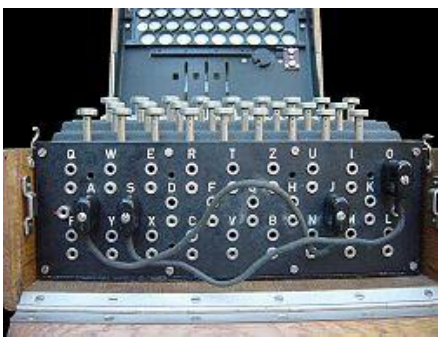


*De drie losgemaakte rotors.*



*Tekening van de groep van drie rotors.*

*Een reflector*



*Het stekkerbord.*

De Duitse militaire operatoren die de Enigma bedienden, maakten gebruik van codeboeken waarin de dagsleutel stond om de stekkers en de rotors in te stellen. De combinatie van het gebruik van de kabeltjes en de rotors zorgde voor bijna ‘oneindig veel’ mogelijke combinaties. Met 26 letters kunnen immers 26! (het uitroepteken staat voor faculteit) verschillende volgordes (permutaties) worden gemaakt.

26! = 403 291 461 126 605 635 584 000 000.

Geen wonder dat men daarom dacht dat de Enigma onkraakbaar was.

Het breken van de ENIGMA-codes

De Polen waren de eersten die erin slaagden om Duitse Enigma-codes te ontcijferen. Ze gebruikten hiervoor de zogenaamde Bomba-methode ("bomba kryptologiczna"). De Bombe was een grote machine met een groot aantal rotors, die allerlei vermoedelijke stukjes van de berichten kon uitproberen. Alle mogelijke combinaties werden hierdoor gecontroleerd. Het feit dat de Enigma-machines nooit een ingetypte letter omzetten naar dezelfde letter in de gecodeerde boodschap, verminderde al sterk het aantal mogelijke combinaties.

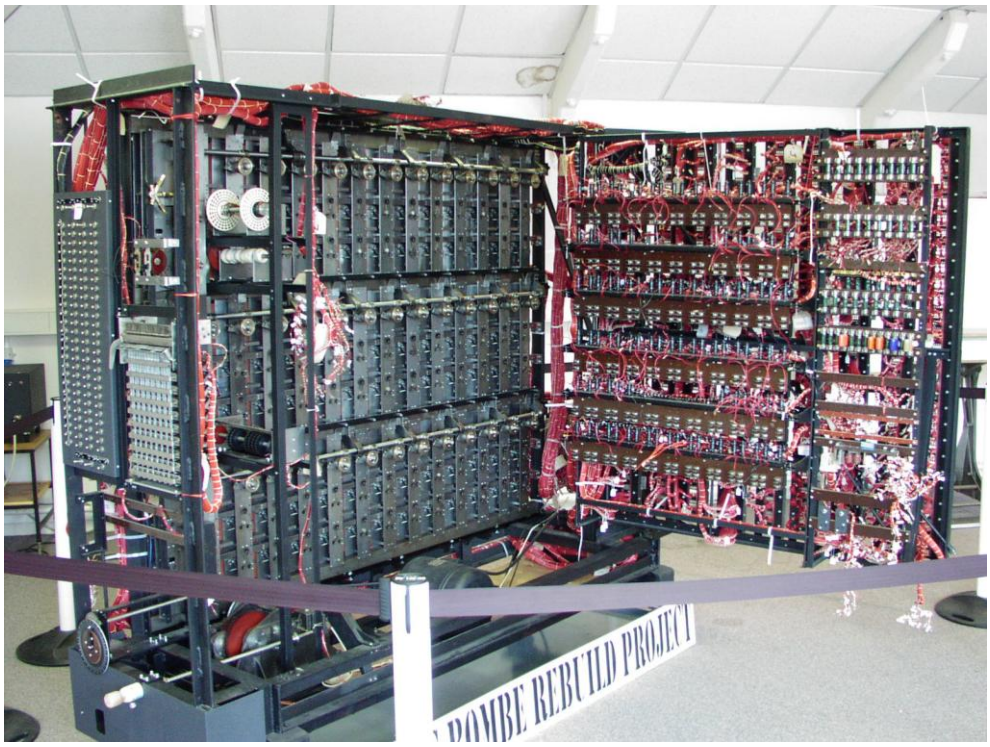
De Britse Government Code and Cipher School in Bletchley Park (de naam van een landhuis in Bletchley in Zuid-Engeland, tegenwoordig onderdeel van de stad Milton Keynes) startte al in augustus 1940 met het gebruik van hun eigen 'Bombe', ontwikkeld door Alan Turing, een geniale Britse wiskundige. Alle informatie die werd verkregen via het breken van Enigma had de codenaam "Ultra", en speelde een beslissende rol tijdens de gehele oorlog.


*Alan Turing (23 juni 1912 – 7 juni 1954).*

Turing maakte o.a. gebruik van enkele zwakke punten in het Enigma-coderingsysteem. Zo begonnen de Duitsers dagelijks hun doorgeseinde boodschappen met het weerbericht. De herhaling van deze patronen leverde nuttige informatie op. Ook vergat men soms de instelling van de rotors te veranderen. Door spionage zal men ongetwijfeld ook wel Enigma-machines en codeboeken in handen hebben gekregen.

Deze topgeheime informatie diende erg omzichtig gebruikt te worden, opdat het Duitse oppercommando niet zou beseffen dat er Enigmacodes gebroken werden. Daarom werden er speciale verbindingsofficieren geplaatst in belangrijke hoofdkwartieren op het terrein, die ervaren waren in het gebruik van de Ultra-informatie. Zij kregen hun informatie rechtstreeks van een speciale afdeling die gespecialiseerd was in tactische analyse en snelle verspreiding van belangrijke informatie. Winston Churchill zou het belang van geheimhouding zo groot hebben gevonden, dat hij een bombardement op Coventry door de Duitsers heeft laten plaatsvinden, hoewel de informatie hierover via "Ultra" vooraf bekend zou zijn geweest.

De "Ultra"-informatie bleek vooral uiterst doeltreffend in de strategisch zeer belangrijke Atlantische Oceaan in de strijd tegen de geduchte Duitse U-boten. De aanvallen van deze duikboten waren zo vernietigend voor de geallieerde bevoorrading, dat ze bijna de oorlog beslisten in het voordeel van Duitsland. Dankzij het onderscheppen van de communicatie tussen de U-boten kon het tij alsnog gekeerd worden.



*Een replica van een 'bombe' in het National Codes Centre in Bletchley Park.*

Na de oorlog werkte Turing aan de universiteit van Manchester verder aan de ontwikkeling van de zogenaamde Turingmachine, die men terecht de voorloper van de computer mag noemen.

In 1952 werd hij gearresteerd onder beschuldiging van homoseksualiteit. Op 7 juni 1954 werd hij dood aangetroffen met in z'n bezit een appel die met cyanide vergiftigd was. Er wordt over zijn dood veel gespeculeerd. De officiële doodsoorzaak was zelfmoord, maar er wordt ook beweerd dat hij door de Engelse geheime dienst is vermoord omdat hij te veel zou weten over de geheime codes, en daardoor een te groot veiligheidsrisico was.