Codebreakers

Een handleiding

Inhoud

[**Monoalfabetische substitutie** 4](#_Toc456640898)

[**Homofone substitutie** 4](#_Toc456640899)

[**Polygrafische substitutie** 5](#_Toc456640900)

[**Polyalfabetische substitutie** 5](#_Toc456640901)

[Caesarcijfer 6](#_Toc456640902)

[**Voorbeeld** 6](#_Toc456640903)

[**Geschiedenis** 7](#_Toc456640904)

[**Het breken** 7](#_Toc456640905)

[**Rot13** 7](#_Toc456640906)

[Transpositiecijfer 8](#_Toc456640907)

[Kolomtranspositie 8](#_Toc456640908)

[Onderbroken kolomtranspositie 9](#_Toc456640909)

[Handcijfer 11](#_Toc456640910)

[Vercijferingsmethodes 11](#_Toc456640911)

[Sleutelwoorden 11](#_Toc456640912)

[De klassieke handcijfers 12](#_Toc456640913)

[Veiligheid 13](#_Toc456640914)

[Vigenèrecijfer 14](#_Toc456640915)

[Werkwijze 14](#_Toc456640916)

[De code breken 15](#_Toc456640917)

[Autoclave 16](#_Toc456640918)

[Bifidcijfer 18](#_Toc456640919)

[Trifidcijfer 19](#_Toc456640920)

[Playfaircijfer 20](#_Toc456640921)

[ADFGX-cijfer 22](#_Toc456640922)

[Geschiedenis 22](#_Toc456640923)

[Werkwijze 22](#_Toc456640924)

[Dubbele transpositie cijfer 24](#_Toc456640925)

[Straddling checkerboard cijfer 26](#_Toc456640926)

[Atbash 28](#_Toc456640927)

[Werking 28](#_Toc456640928)

[Baconalfabet 29](#_Toc456640929)

[Omschrijving 29](#_Toc456640930)

[Coderen 29](#_Toc456640931)

[Decoderen 29](#_Toc456640932)

[Nadeel 29](#_Toc456640933)

[Tussenvorm 29](#_Toc456640934)

[Modern voorbeeld 30](#_Toc456640935)

[One-time-pad 31](#_Toc456640936)

[Ontstaan 31](#_Toc456640937)

[Eigenschappen 31](#_Toc456640938)

[Praktische voorbeelden 32](#_Toc456640939)

[Problemen bij gebruik 33](#_Toc456640940)

[Toepassingen 34](#_Toc456640941)

[Snake Oil 35](#_Toc456640942)

[Paardensprongcijfer 36](#_Toc456640943)

[Polybiusvierkant 37](#_Toc456640944)

[Algemene vorm 37](#_Toc456640945)

[Veiligheid 37](#_Toc456640946)

[Rozenkruisersgeheimschrift 38](#_Toc456640947)

[Scytale 38](#_Toc456640948)

**Substitutieversleuteling**

**Substitutieversleuteling** is een [encryptiemethode](http://nl.wikipedia.org/wiki/Encryptie). De [versleuteling](http://nl.wikipedia.org/wiki/Cryptografie) veronderstelt de aanwezigheid van een set ter vervanging dienende [symbolen](http://nl.wikipedia.org/wiki/Symbool). Deze symbolen zijn niet beperkt tot alfabetten.

Buiten het vervangen *per letter* kan men ook *combinaties* van letters vervangen. Men spreekt in het eerste geval van een *eenvoudige substitutie* en in het tweede van *polygrafische subsititutie*. Daarnaast bestaat het onderscheid tussen *monoalfabetische substitutie*, waarbij voor het hele te versleutelen bericht één enkel substitutie-alfabet gebruikt wordt, en *polyalfabetische substitutie*, waarbij het substitutie-alfabet tijdens de versleuteling verandert.

Technisch gezien zou men [Morsecode](http://nl.wikipedia.org/wiki/Morse) als substitutieversleuteling kunnen zien. Morsecode is echter nooit *geheim* geweest en kan dientengevolge niet worden ingedeeld in de *geheim*schriften.



Substitutie komt voor in [literatuur](http://nl.wikipedia.org/wiki/Literatuur), bijvoorbeeld in [Edgar Allan Poe](http://nl.wikipedia.org/wiki/Edgar_Allan_Poe)'s [de goud-kever](http://nl.wikipedia.org/wiki/De_goud-kever) maar ook in [Sherlock Holmes](http://nl.wikipedia.org/wiki/Sherlock_Holmes)' *Avontuur van de dansende mannen*.

Substitutieversleuteling verschilt van [transpositieversleuteling](http://nl.wikipedia.org/wiki/Transpositieversleuteling), waar de letters niet vervangen worden maar alleen anders gerangschikt. Combinaties zijn uiteraard mogelijk.

**Monoalfabetische substitutie**

Monoalfabetische substitutie vervangt gedurende de hele encryptie elke letter van het [klaarschrift](http://nl.wikipedia.org/wiki/Klare_tekst_en_cijfertekst) met een vooraf vastgesteld substituut. Historische voorbeelden hiervan zijn het [Caesarcijfer](http://nl.wikipedia.org/wiki/Caesarcijfer) en [atbash](http://nl.wikipedia.org/wiki/Atbash). Er zijn verscheidene variaties op deze twee methoden en totdat Arabische [wiskundigen](http://nl.wikipedia.org/wiki/Wiskunde) in de 9e eeuw de techniek van [frequentieanalyse](http://nl.wikipedia.org/wiki/Frequentieanalyse_%28cryptografie%29) ontdekten werden ze als onbreekbaar beschouwd. Naast de twee genoemde is ook het [rozenkruisersgeheimschrift](http://nl.wikipedia.org/wiki/Rozenkruisersgeheimschrift) een voorbeeld van monoalfabetische substitutie.

**Homofone substitutie**

Een belangrijke ontwikkeling om de frequentieanalyse tegen te gaan was de **homofone substitutie**. Hierbij worden in het versleutelingsalfabet meer symbolen gebruikt dan in het alfabet van het klaarschrift. De veel voorkomende letter **E** kan bijvoorbeeld vervangen worden door drie substituten, bijvoorbeeld de getallen **5**, **31** en **57**. Veel voorkomende letters krijgen bij homofone substitutie meer substituten dan minder vaak voorkomende. De frequentieverdeling van de versleutelde tekst wordt als gevolg daarvan *plat*, omdat elk substituut ongeveer even vaak voorkomt.

Homofone substitutie wordt vermoedelijk gebruikt in het [Voynichmanuscript](http://nl.wikipedia.org/wiki/Voynichmanuscript). Een uitgebreidere variant van homofone substitutie is de *nomenclatuur*[[1]](http://nl.wikipedia.org/wiki/Substitutieversleuteling#cite_note-0). Hier wordt het gebruikt in combinatie met een codeboek waarin veel voorkomende namen en begrippen een eigen substituut krijgen. Een voorbeeld hiervan is het [Grote Geheimschrift van Lodewijk XIV](http://nl.wikipedia.org/wiki/Grote_Geheimschrift_van_Lodewijk_XIV)

**Polygrafische substitutie**

Bij polygrafische substitutie worden de letters in combinatie in plaats van per letter vervangen. Dit was een belangrijke ontdekking tegen frequentieanalyse. De oudst bekende verhandeling van polygrafische substitutie komt uit 1586 beschreven in *de furtivis literarum notis* van [Giambattista della Porta](http://nl.wikipedia.org/wiki/Giambattista_della_Porta). [Felix Delastelle](http://nl.wikipedia.org/wiki/Felix_Delastelle) publiceerde over verscheidene polygrafische versleutelingen zoals het [bifid-](http://nl.wikipedia.org/wiki/Bifid), het [trifid-](http://nl.wikipedia.org/wiki/Trifidcijfer) en het [vier-vierkantencijfer](http://nl.wikipedia.org/w/index.php?title=Vier-vierkanten&action=edit&redlink=1). Een ander bekend voorbeeld van polygrafische subtitutie is het [playfaircijfer](http://nl.wikipedia.org/wiki/Playfaircijfer).

**Polyalfabetische substitutie**

Bij polyalfabetische substitutie wordt gebruikgemaakt van meerdere versleutelingsalfabetten, veelal in de vorm van tabellen. De oudst bekende omschrijving van polyalfabetische substitutie stamt uit [1463](http://nl.wikipedia.org/wiki/1463) en komt van [Leone Battista Alberti](http://nl.wikipedia.org/wiki/Leone_Battista_Alberti) in omstreeks [1500](http://nl.wikipedia.org/wiki/1500) gevolgd door een beschrijving in het werk *Steganographia* van [Johannes Trithemius](http://nl.wikipedia.org/wiki/Johannes_Trithemius). In [1563](http://nl.wikipedia.org/wiki/1563) wordt in *De Furtivis Literarum Notis* van [Giambattista della Porta](http://nl.wikipedia.org/wiki/Giambattista_della_Porta) een meer complexe manier met een gemengd alfabet omschreven. Het meest bekende werk aangaande polyalfabetische substitutie komt echter van [Blaise de Vigenère](http://nl.wikipedia.org/wiki/Blaise_de_Vigen%C3%A8re). Zijn [Vigenèrecijfer](http://nl.wikipedia.org/wiki/Vigen%C3%A8recijfer) heeft lang bekend gestaan als *le chiffre indéchiffrable* (Frans: het onontcijferbare geheimschrift).

# Caesarcijfer

Ga naar: [navigatie](http://nl.wikipedia.org/wiki/Caesarcijfer#column-one), [zoeken](http://nl.wikipedia.org/wiki/Caesarcijfer#searchInput)





Schematisch voorbeeld van een Rotatie3

Het **Caesarcijfer** is een klassiek mono-alfabetisch [substitutiecijfer](http://nl.wikipedia.org/wiki/Substitutiecijfer). Het is bekend onder verscheidene namen waaronder Caesarrotatie, of kortweg *Rot*. Het is vernoemd naar [Julius Caesar](http://nl.wikipedia.org/wiki/Julius_Caesar) die het gebruikte om te communiceren met zijn veldheren. De versleuteling werkt door elke letter van de *platte tekst* te vervangen door een vooraf vastgestelde rotatie of verschuiving. Bij Rot3 (een rotatie van drie) wordt de letter *A* vervangen door de letter *D* (zie plaatje).

Meer complexe schematieken, zoals het [Vigenèrecijfer](http://nl.wikipedia.org/wiki/Vigen%C3%A8recijfer), zijn deels gebaseerd op het principe. Vandaag de dag komt de rotatie voornamelijk voor in het [Rot13](http://nl.wikipedia.org/wiki/Rot13) systeem. Als alle mono-alfabetische substituties biedt deze vorm van versleuteling geen enkele bescherming tegen [cryptoanalyse](http://nl.wikipedia.org/wiki/Cryptoanalyse).

**Voorbeeld**

Het Caesarcijfer is een [handcijfer](http://nl.wikipedia.org/wiki/Handcijfer). Het is gebruikelijk om bij de versleuteling gebruik te maken van twee alfabetten. Een regulier en een met rotatie daarin.

**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**

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

Hierna vervangt men de letters van de onversleutelde tekst door de letter die eronder staat in de tabel. Zodoende wordt de geheime boodschap:

Klare tekst: **D** I T I S Z E E R G E H E I M

Cijfertekst: **A** F Q F P W B B O D B E B F J

De methode kan ook door middel van een [modulair wiskundige](http://nl.wikipedia.org/wiki/Modulair_rekenen) formule weergegeven worden. Hiervoor dient men de letter te vervangen door de oplopende cijfers van 0 tot en met 25. Hierna kan de volgende formule gebruikt worden waarbij *X* de letter in de platte tekst is en *N* de gekozen rotatie.

Voor versleuteling:



en voor ontsleuteling:



**Geschiedenis**

Het gebruik van Caesarrotatie wordt beschreven door [Suetonius](http://nl.wikipedia.org/wiki/Gaius_Suetonius_Tranquillus). Hij vermeldt het gebruik van deze methode door zowel Julius Caesar als door [Augustus](http://nl.wikipedia.org/wiki/Gaius_Julius_Caesar_Octavianus).

*Wanneer hij schreef in cijferschrift gebruikte hij de B voor de A en de C voor de B*

Een duidelijke omschrijving van een Rot1 uit *Het leven van Augustus*.

Hoewel het geheimschrift naar hem vernoemd is, is van Julius Caesar bekend dat hij meer ingewikkelde methodes gebruikte.

Over de effectiviteit van de versleuteling wordt getwijfeld, men vermoedt dat het, gezien de ongeletterdheid van de vijanden van Caesar, toentertijd sufficiënt was. De methode is tot het begin van de twintigste eeuw in gebruik geweest bij bepaalde onderdelen van het leger.

**Het breken**

Vandaag de dag is het breken van een met een Caesarcijfer versleuteld bericht geen kunst aangezien er maar vijfentwintig mogelijkheden zijn. In het predigitale tijdperk was het cijfer echter ook zeer kwetsbaar voor [frequentieanalyse](http://nl.wikipedia.org/wiki/Frequentieanalyse_%28cryptografie%29).

**Rot13**

Een speciaal geval is Rot13. Deze methode is minder bekend onder de naam *Caesaralfabet*. Hierbij schrijft men de eerste 13 letters van het alfabet op de bovenste rij met daaronder de 13 resterende letters. Deze methode is wederkerig, het versleutelings- en ontsleutelingsmechanisme zijn gelijk. Door de eenvoud van implementatie is deze methode erg populair geworden om bijvoorbeeld leeswaarschuwingen kracht bij te zetten in moderne communicatiekanalen zoals [usenet](http://nl.wikipedia.org/wiki/Usenet).

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

# Transpositiecijfer

Het **transpositiecijfer** is een van de klassieke [handcijfers](http://nl.wikipedia.org/wiki/Handcijfers), een [versleutelingsmethode](http://nl.wikipedia.org/wiki/Cryptografie) die toegepast wordt in de [cryptografie](http://nl.wikipedia.org/wiki/Cryptografie). Bij transpositie worden letters of tekens van plaats verwisseld met andere [letters](http://nl.wikipedia.org/wiki/Letter) of tekens.

In de klassieke cryptografie gebruikt men vooral de techniek van kolomtranspositie. Enkele voorbeelden van kolomtranspositie zijn het [transpositie cijfer](http://nl.wikipedia.org/wiki/Transpositie_cijfer) en de [dubbele transpositie](http://nl.wikipedia.org/wiki/Dubbele_transpositie_cijfer). Ook bij de moderen cryptografische algoritmes voor computergebruik kent men transpositie. Daar worden dan binaire gegevens van plaats verwisseld.

Meestal wordt transpositie gebruikt in combinatie met [fractionering](http://nl.wikipedia.org/wiki/Fractionering_%28cryptografie%29) en [Substitutie](http://nl.wikipedia.org/wiki/Substitutie_%28cryptografie%29). Vooral de combinatie met [fractionering](http://nl.wikipedia.org/wiki/Fractionering_%28cryptografie%29) is zeer effectief. Een voorbeeld van zo'n combinatie is het [ADFGVX-cijfer](http://nl.wikipedia.org/wiki/ADFGVX-cijfer).

Er zijn vele verschillende methodes om een transpositietabel te vullen met klare tekst.

We beschrijven eerst de gewone kolomtranspositie om vervolgens twee voorbeelden te geven van onderbroken transpositie. Deze methode is beter bestand tegen anagramming dan gewone kolomtranspositie vanwege zijn grillige plaatsing van de klare tekst. Bovendien zijn er vele variaties van invullen mogelijk, volgens een vooraf bepaald patroon, met open gedeeltes, rijen of diagonalen die éérst worden ingevuld enzovoort.

## Kolomtranspositie

In ons voorbeeld is het sleutelwoord LEONARDO. De letters van dit woord worden volgens alfabet genummerd, van links naar rechts. Onder dit woord schrijven we de klare tekst van links naar recht en boven naar onder.

De klare tekst is DIT DRINGEND BERICHT IS ZEER GEHEIM.

L E O N A R D O

4 3 6 5 1 8 2 7

---------------

D I T D R I N G

E N D B E R I C

H T I S Z E E R

G E H E I M

Vervolgens lezen we de tekst af per kolom, beginnende met het kleinste nummer. Kolom 1 is dus REZI, kolom 2 is NIE. De bekomen tekst verdelen we in groepen.

Cijfertekst: REZIN IEINT EDEHG DBSET DIHGC RIREM

Om de cijfertekst te ontcijferen moeten we eerst een tabel maken met het sleutelwoord en het juiste aantal kolommen. Uit het aantal letters in de cijfertekst kunnen we dan het aantal lange en korte kolommen afleiden. We vullen de tabel met de cijfertekst, kolom per kolom, in volgorde van het sleutelwoord. Dan lezen we de tekst af van links naar rechts en boven naar onder.

## Onderbroken kolomtranspositie

Bij onderbroken kolomtranspositie wordt de tekst op onregelmatige wijze ingevuld in de tabel. Er zijn vele mannieren waarop we de tekst kunnen invullen.

Ook hier gebruiken we het sleutelwoord LEONARDO. Onder het sleutelwoord schrijven we de klare tekst van links naar rechts en boven naar onder, maar worden de rijen slechts gedeeltelijk opgevuld. Voor de eerste rij wordt deze ingevuld tot en met de kolom waar de eerste letter staat. In ons voorbeeld is dit de letter A. De tweede rij wordt ingevuld tot en met de tweede letter, zijnde D. Zo vult men rij na rij verder in. Indien er vele rijen nodig zijn begint men na de laatste rij opnieuw met een rij met de lengte van de eerste letter.

L E O N A R D O

4 3 6 5 1 8 2 7

---------------

D I T D R

I N G E N D B

E R

I

C H T I

S Z E

E R G E H E I M

Vervolgens lezen we de tekst af per kolom, beginnende met het kleinste nummer. Kolom 1 is dus RNH, kolom 2 is BI en kolom 3 is INRHZR.

Cijfertekst: RNHBI INRHZ RDIEI CSEDE IETGT EGMDE

Om de cijfertekst te ontcijferen moeten we eerst een tabel maken met het sleutelwoord en lengte van elke rij bepalen aan de hand van de nummering van het kolommen. Uit het aantal letters in de cijfertekst kunnen we dan afleiden tot hoe ver naar beneden de kolommen ingevuld dienen te worden. Vervolgens vullen we de tabel met de cijfertekst, kolom per kolom, in volgorde van het sleutelwoord. Tenslotte lezen we de tekst af van links naar rechts en boven naar onder.

In het tweede voorbeeld van onderbroken kolom transpositie maken we een tabel waarin de tekst past. In ons voorbeeld is de tekst 30 letters lang en gebruiken we een tabel van 8 X 4, met dus een overschot van 2 letters. We passen voor de grootte van de rij hetzelfde principe toe als in het vorige voorbeeld. We beginnen te tekst in te vullen van links naar rechts en van boven naar onder en als het linkerveld is ingevuld gaan we verder met invullen in het rechterveld.

L E O N A R D O

4 3 6 5 1 8 2 7

---------------

D I T D R **C H T**

I N G E N D B **I**

E R **S Z E E R G**

I **E H E I M**

Vervolgens lezen we de tekst af per kolom, beginnende met het kleinste nummer. Kolom 1 is dus RNEI, kolom 2 is HBR.

Cijfertekst: RNEIH BRINR EDIEI DEZET GSHTI GCDEM

Om de cijfertekst te ontcijferen moeten we ook hier de tabel opnieuw reconstrueren en de indeling bepalen alvorens de tekst in te vullen.

Zoals u kunt merken geven deze drie voorbeelden van transpositie op deze korte tekst drie totaal verschillende resultaten. Combinatie van verschillende transposities behoren tot de sterkste klassieke vercijferingen. Enkele voorbeelden zijn [dubbele transpositie](http://nl.wikipedia.org/wiki/Dubbele_transpositie_cijfer), [SECOM](http://users.telenet.be/d.rijmenants/nl/secom.htm) en het [VIC-cijfer](http://www.quadibloc.com/crypto/pp1324.htm).

# Handcijfer

De **handcijfers**, ook wel pen-en-papiercodes genoemd, zijn [vercijferingsmethodes](http://nl.wikipedia.org/wiki/Cryptografie) om met behulp van een geheime sleutelwoord of zin een tekst om te zetten in een onleesbare code. De tekst kan enkel (eenvoudig) [ontcijferd](http://nl.wikipedia.org/wiki/Decryptie) worden door de persoon die dezelfde methode gebruikt en in het bezit is van dezelfde geheime sleutel. Er zijn verscheidene technieken ontwikkeld waarvan enkele zeer betrouwbaar bleken.

Hoewel de ontwikkeling van cryptografische machines en [computers](http://nl.wikipedia.org/wiki/Computer) veel van het handwerk overbodig maakte, bleef er altijd een rol weggelegd voor de handcijfers. Veldcijfers - zo noemen militairen de handcijfers - zoals de dubbele transpositie werden nog zeer veel gebruikt tijdens de [Tweede Wereldoorlog](http://nl.wikipedia.org/wiki/Tweede_Wereldoorlog). Het grote voordeel van veldcijfers is de eenvoudige toepassing zonder speciale toestellen. Daarom blijven deze veldcijfers tot op vandaag nog steeds een interessant alternatief om een boodschap op eenvoudige wijze toch veilig over te brengen. In dit artikel beschrijven we de bekendste klassieke handcijfers.

## Vercijferingsmethodes

Een methode van vercijfering noemen we een cijfer. De leesbare tekst noemen we klare tekst, en de vercijferde of gecodeerde tekst noemen we cijfertekst. De cijfertekst wordt meestal ingedeeld in groepen van vijf letters. Er zijn drie grote indelingen in de techniek van het vercijferen:

* [Substitutie](http://nl.wikipedia.org/wiki/Substitutie_%28cryptografie%29): vervangen van letters door andere letters
* [Transpositie](http://nl.wikipedia.org/wiki/Transpositie_%28cryptografie%29): verwisselen van de positie van letters binnen een tekst
* [Fractionering](http://nl.wikipedia.org/wiki/Fractionering_%28cryptografie%29): breken van letters in verschillende delen waarna deze verplaatst worden

Vooral de combinatie van transpositie en fractionering blijkt zeer effectief. Hierdoor worden de verschillende delen van één letter verspreid over de ganse tekst, waardoor de vercijfering voldoet aan [Claude Elwood Shannons](http://nl.wikipedia.org/wiki/Claude_Shannon) diffusie. Het ideale cijfer is dus een combinatie van de drie vercijferingsprincipes, en dat bovendien eenvoudig is in gebruik. Enkele voorbeelden die transpositie en fractionering combineren zijn [Bifid](http://nl.wikipedia.org/wiki/Bifid_cijfer), [Trifid](http://nl.wikipedia.org/wiki/Trifid_cijfer), en [ADFGVX](http://nl.wikipedia.org/wiki/ADFGVX-cijfer). De principes van substitutie, transpositie en fractionering worden in de moderne crypto-algoritmes voor computer nog steeds toegepast.

## Sleutelwoorden

Een vereiste voor een goed cijfer is dat het eenvoudig is in gebruik. Daarom gebruikt men veelal sleutelwoorden om een substitutie-alfabet of een [matrix](http://nl.wikipedia.org/wiki/Matrix_%28wiskunde%29) te vullen. Doorgaans noteert men het sleutelwoord, of de zin, schrapt de letters die er dubbel in voorkomen, en vult achter dit sleutelwoord de resterende letters van het alfabet aan. Hoe langer het sleutelwoord of de zin, des te minder men alfabetisch dient aan te vullen.

Sleutelwoord : SLEUTELWOORD

Cijferalfabet: SLEUTWORDABCFGHIJKMNPQVXYZ

Voor een matrix kan men vele verschillende manieren van vullen gebruiken die zender en ontvanger overeen kunnen komen. In de voorbeelden hieronder zien we in de eerste matrix het sleutelwoord van links naar rechts en boven naar onder. De tweede matrix is spiraalgewijs tegen de klok in van buiten naar binnen gevuld. De derde matrix is van boven naar onder en van rechts naar links. De vierde matrix is van linksboven zigzaggend naar rechtsonder. Vele andere combinaties, richtingen en figuren zijn mogelijk. Hieraan is te zien dat men van één sleutelwoord veel totaal verschillende matrices kan maken.

**S L E U T** **S** IJ H G F Q IJ B **W S** **S L E U T**

**W O R D** A **L** K Y X C V K C **O L** A **D R O W**

B C F G H **E** M Z V B X M F **R E** B C F G H

IJ K M N P **U** N P Q A Y N G **D U** P N M K IJ

Q V X Y Z **T W O R D** Z P H A **T** Q V X Y Z

## De klassieke handcijfers

In de loop der eeuwen zijn vele verschillende methodes ontwikkeld voor de vercijfering van text. Hieronder worden enkele van de bekendste vercijferingsmethodes voorgesteld.

* De [rotatievercijfering van Caesar](http://nl.wikipedia.org/wiki/Caesarcijfer) is een van de oudst gekende cijfers en werd gebruikt voor de communicatie tussen [Romeinse](http://nl.wikipedia.org/wiki/Romeinse_Rijk) veldheren. Deze vercijfering wordt ook wel rotatiecijfer of ROT genoemd.
* Het [substitutiecijfer](http://nl.wikipedia.org/wiki/Substitutiecijfer) is een monoalfabetische substitutie. Hierbij wordt elke letter vervangen door een andere letter.
* [Vigenère](http://nl.wikipedia.org/wiki/Vigen%C3%A8recijfer) is een polyalfabetische substitutie, het vervangen van letters aan de hand van verschillende alfabetische reeksen in een tabel, het Vigenère-tableau.
* [Autoclave](http://nl.wikipedia.org/wiki/Autoclave) is een verbetering van het Vigenèrecijfer. Hierbij vercijfert men, mits een kleine verschuiving door een sleutelwoord, de klare tekst met zichzelf.
* [Homofone substitutie](http://nl.wikipedia.org/wiki/Homofone_substitutiecijfer) gebruikt een evenredige verdeling van letters naar getallen om bestand te zijn tegen letterfrequentie-analyse.
* [Bifid](http://nl.wikipedia.org/wiki/Bifidcijfer) is een matrix die een combinatie van substitutie met fractionering gebruikt. Elke letter wordt opgesplitst in twee getallen.
* [Trifid](http://nl.wikipedia.org/wiki/Trifidcijfer) is een drievoudige matrix welke een combinatie van substitutie met fractionering gebruikt. Elke letter wordt opgesplitst in drie getallen.
* [Playfair](http://nl.wikipedia.org/wiki/Playfaircijfer) is een substitutiecijfer waarbij een matrix is gebruikt om bigrammen te vercijferen.
* [ADFGVX](http://nl.wikipedia.org/wiki/ADFGVX-cijfer) combineert fractionering van een Polybiusvierkant, dat een monoalfabetisch substitutie bevat, met een enkelvoudige kolomstranspositie. Het was tijdens de [Eerste Wereldoorlog](http://nl.wikipedia.org/wiki/Eerste_Wereldoorlog) het veldcijfer van het [Duitse](http://nl.wikipedia.org/wiki/Duitsland) leger.
* [Dubbele transpositie](http://nl.wikipedia.org/wiki/Dubbele_transpositie_cijfer) is een tweevoudige kolomtranspositie. Dit was één van de veiligste handcijfers, gebruikt tijdens de [Tweede Wereldoorlog](http://nl.wikipedia.org/wiki/Tweede_Wereldoorlog).
* [Straddling checkerboard](http://nl.wikipedia.org/wiki/Straddling_checkerboard_cijfer) of spreidend dambord is een fractionerend monoalfabetisch substitutiecijfer. Het is een matrixcijfer dat meestal gevolgd wordt door een bijkomende dubbele transpositie.

## Veiligheid

Alle hierboven beschreven handcijfers werden vroeg of laat met succes gebroken door [cryptoanalyse](http://nl.wikipedia.org/wiki/Cryptoanalyse). Sommige van de veldcijfers zijn desondanks nuttig indien de tijd, nodig voor cryptoanalyse, zo lang is dat de verkregen informatie achterhaald en nutteloos blijkt. De sterkste veldcijfers, beschreven in dit artikel, zijn [dubbele transpositie](http://nl.wikipedia.org/wiki/Dubbele_transpositie_cijfer) en [ADFGVX](http://nl.wikipedia.org/wiki/ADFGVX-cijfer). In de [Verenigde Staten](http://nl.wikipedia.org/wiki/Verenigde_Staten) is de informatie over cryptoanalyse van de dubbele transpositie geheim gebleven tot enkele jaren geleden.

Succesvolle cryptoanalyse is enkel mogelijk indien genoeg cijfermateriaal ter beschikking is dat met dezelfde sleutel werd vercijferd. Over het algemeen geldt dat grotere sleutelwoorden een betere veiligheid geven en hoe minder tekst vercijferd is, des te moeilijker de cijfertekst te kraken is. Letterfrequentie-analyse is bijvoorbeeld onbetrouwbaar als er slechts één zin werd gecodeerd, of er verhoudingsgewijs veel zeldzame letters in de tekst zitten. Zo is het eenvoudige [Vigenère](http://nl.wikipedia.org/wiki/Vigen%C3%A8recijfer) onbreekbaar indien één korte zin met een lang sleutelwoord vercijferd werd, maar is het breken van het veel veiliger [dubbel transpositiecijfer](http://nl.wikipedia.org/wiki/Dubbele_transpositie_cijfer) minder moeilijk indien er genoeg cijfertekst voorhanden is.

Indien het wenselijk is de sterkte van een bestaand cijfer te verhogen, kan men het combineren met andere cijfers. Bijvoorbeeld kan men bij [trifid](http://nl.wikipedia.org/wiki/Trifidcijfer) na omzetting in een getallenreeks, deze eerst bewerken met een [dubbele transpositie](http://nl.wikipedia.org/wiki/Dubbele_transpositie_cijfer) vóór de gefractioneerde letters terug worden samengevoegd. Door een enkele [kolomstranspositie](http://nl.wikipedia.org/wiki/Transpositie_cijfer) te gebruiken vóór vercijfering met [Playfair](http://nl.wikipedia.org/wiki/Playfaircijfer) trekt men de veelgebruikte digrammen in de klare tekst uit elkaar.

# Vigenèrecijfer

Het **Vigenèrecijfer** is in de [cryptografie](http://nl.wikipedia.org/wiki/Cryptografie) één van de klassieke [handcijfers](http://nl.wikipedia.org/wiki/Handcijfers). Het werd uitgevonden door [Giovanni Batista Belaso](http://nl.wikipedia.org/w/index.php?title=Giovanni_Batista_Belaso&action=edit&redlink=1) in 1553, maar het was door [Blaise de Vigenère](http://nl.wikipedia.org/wiki/Blaise_de_Vigen%C3%A8re) dat het algemeen bekend raakte, waardoor het zijn naam kreeg. Het werd echter lange tijd zelden gebruikt vanwege zijn complexiteit.

## Werkwijze

Het is een [polyalfabetische substitutie](http://nl.wikipedia.org/wiki/Substitutie_%28cryptografie%29), het vervangen van letters aan de hand van verschillende alfabetische reeksen. Daarbij gebruiken we het zogenaamde [tabula recta](http://nl.wikipedia.org/wiki/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

Men kiest eerst een geheim sleutelwoord, bijvoorbeeld ZODIAK. Dit schrijft men onder de klare tekst. Vervolgens zoekt men de klare letter 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.

Klare 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

 -----------------------------

Cijfertekst : **C** W W Q S J D S U O E R D W P

De cijfertekst: CWWQS JDSUO ERDWP

Om te ontcijferen schrijft men het sleutelwoord boven de cijfertekst. Vervolgens zoekt men elke sleutelletter op in het horizontale alfabet en gaat naar beneden tot men de betrokken codeletter tegenkomt. De letter, in het verticale alfabet, die zich op dezelfde rij bevindt is de klare letter.

## De code breken

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](http://nl.wikipedia.org/wiki/Charles_Babbage) en [Friedrich Kasiski](http://nl.wikipedia.org/wiki/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 een klare 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 grootst gemene 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. Eén analysetekst zou dan de eerste, zevende, dertiende... letter bevatten. De tweede tekst de tweede, achtste, veertiende letter enz...

# Autoclave

Het **Autoclave-**, **Autokey-** of **Autosleutelcijfer** is een van de klassieke [handcijfers](http://nl.wikipedia.org/wiki/Handcijfers).

Autoclave werd uitgevonden door [Blaise de Vigenère](http://nl.wikipedia.org/wiki/Blaise_de_Vigen%C3%A8re) en is een verbetering van het [Vigenèrecijfer](http://nl.wikipedia.org/wiki/Vigen%C3%A8recijfer), uitgevonden door [Giovanni Batista Belaso](http://nl.wikipedia.org/w/index.php?title=Giovanni_Batista_Belaso&action=edit&redlink=1) in [1553](http://nl.wikipedia.org/wiki/1553), maar genoemd naar Blaise de Vigenère.

Het is een polyalfabetische [substitutie](http://nl.wikipedia.org/wiki/Substitutie_%28cryptografie%29), het vervangen van letters aan de hand van verschillende alfabetische reeksen. Daarbij gebruiken we een tabel waarvan elk alfabet één letter verschoven is. Dit is dezelfde tabel als gebruikt bij het [Vigenèrecijfer](http://nl.wikipedia.org/wiki/Vigen%C3%A8recijfer).

 **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

Het sleutelwoord, of in dit geval beter de sleutelzin, is gevormd door een kort sleutelwoord, gevolgd door de klare tekst. Hierdoor vercijfert men, mits een kleine verschuiving, de klare tekst met zichzelf. In ons voorbeeld is het sleutelwoord ZODIAK.

Vervolgens zoekt men de elke klare letter 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.

Hierbij wordt de tekst zelf gebruikt om de tekst te vercijferen. De substitutietabel is dezelfde als bij het gewone Vigenèrecijfer.

Klare tekst : **D** I T I S Z E E R G E H E I M . . . .

Sleutelwoord: **Z** O D I A K D I T I S Z E E R G E H E I M....

 ---------------------------------------------

Cijfertekst : **C** W W Q S J H M K O W G I M D .....

De cijfertekst: CWWQS JHMKO WGIMD ..... .....

Om de tekst te kunnen ontcijferen dient men te beginnen met het korte sleutelwoord, om dan de ontcijferde tekst beetje bij beetje verder aan te vullen achter het sleutelwoord. Indien er één fout is bij het ontcijferen zal de rest van de vercijfering ook fout zijn.

De sterkte van dit cijfer ligt erin dat niet steeds opnieuw hetzelfde sleutelwoord gebruikt is, maar de steeds variërende klare tekst. Voor de cryptoanalyse van dit cijfer kunnen bepalen van sleutellengte en letterfrequenties hier niet toegepast worden zoals bij de gewone [Vigenèrevercijfering](http://nl.wikipedia.org/wiki/Vigen%C3%A8recijfer).

# Bifidcijfer

Het **bifidcijfer** is één van de klassieke [handcijfers](http://nl.wikipedia.org/wiki/Handcijfers).

Bifid is een combinatie van [substitutie](http://nl.wikipedia.org/wiki/Substitutie_%28cryptografie%29) met [fractionering](http://nl.wikipedia.org/wiki/Fractionering_%28cryptografie%29). Eerst creëren we een 5 X 5 matrix van letters, de rijen en kolommen genummerd van 1 tot 5. De matrix vullen we met het alfabet aan de hand van een sleutelwoord. In ons voorbeeld gebruiken we het sleutelwoord NACHTBOMMENWERPER.

 | **1 2 3 4 5**

-+-----------

**1**| N A C H T

**2**| B O M E W

**3**| R P D F G

**4**| I J K L Q

**5**| S U V X YZ

Vervolgens lezen we voor elke letter de rij en kolom af en schrijven de getallen verticaal onder de klare tekst. Zo heeft de I de waarde 41 omdat zij in rij 4 en kolom 1 staat.

Klare tekst: D **I** T I S G E H E I M

 ---------------------

Rij : 3 **4** 1 4 5 3 2 1 2 4 2

Kolom : 3 **1** 5 1 1 5 4 4 4 1 3

Nu schrijven we de cijfers opnieuw, van links naar rechts en boven naar onder, in groepen van twee. Dan zetten we de nieuwe getallen terug om in letters.

34 14 53 21 24 23 15 11 54 44 13

F H V B E M T N X L C

De cijfertekst: FHVBE MTNXL C

Ontcijfering gebeurt door elke letter van de cijfertekst terug om te zetten in een getal aan de hand van de tabel. De getallenreeks wordt in twee verdeeld en de twee delen onder elkaar geschreven. Tenslotte zetten we elke verticale groep van twee getallen terug om in een letter met behulp van de tabel.

# Trifidcijfer

[handcijfers](http://nl.wikipedia.org/wiki/Handcijfers). Trifid is een combinatie van [substitutie](http://nl.wikipedia.org/wiki/Substitutie_%28cryptografie%29) en [fractionering](http://nl.wikipedia.org/wiki/Fractionering_%28cryptografie%29) gebaseerd op hetzelfde pricipe als [bifid](http://nl.wikipedia.org/wiki/Bifidcijfer), maar hier worden de letters gefractioneerd in drie stukken. Als voorbeeld van opvulling van het alfabet gebruiken we het sleutelwoord LEONARDO DA VINCI waarbij we de dubbele letters weglaten en aanvullen met de rest van het alfabet.

 **1 2 3**

 ----- ----- -----

**1** L E O N A R D V I

**2** C B F G H J K M P

**3** Q S T U W X Y Z /

 **1 2 3 1 2 3 1 2 3**

Vervolgens lezen we voor elke letter het vierkant, de rij en kolom af en schrijven de getallen verticaal onder de klare tekst. Zo heeft de D de waarde 311, omdat zij in vierkant 3, rij 1 en kolom 1 staat.

Klare tekst: **D** I T I S G E H E I M

 ---------------------

Vierkant : **3** 3 1 **3 1 2** 1 2 1 3 3

Rij : **1** 1 3 1 3 2 1 2 1 1 2

Kolom : **1** 3 3 3 2 1 2 2 2 3 2

Nu schrijven we de getallen opnieuw, van links naar rechts en boven naar onder, in groepen van drie. Dan zetten we de nieuwe getallen terug om in letters.

331 **312** 121 331 131 321 211 213 332 122 232

 Y V C Y Q K N R Z B W

De cijfertekst: YVCYQ KNRZB W

De ontcijfering gebeurt door elke letter van de cijfertekst om te zetten in een getal aan de hand van de tabel. De bekomen getallen worden van links naar rechts en boven naar onder in drie gelijke rijen geschreven. Tenslotte zetten we elke verticale groep van drie getallen terug om in een letter met behulp van de tabel.

# Playfaircijfer

Het **Playfaircijfer** is een van de klassieke [handcijfers](http://nl.wikipedia.org/wiki/Handcijfers). Dit cijfer werd in 1854 door Sir [Charles Wheatstone](http://nl.wikipedia.org/wiki/Charles_Wheatstone) uitgevonden maar draagt de naam van [Lyon Playfair](http://nl.wikipedia.org/w/index.php?title=Lyon_Playfair&action=edit&redlink=1) die het gebruik ervan promootte[[1]](http://nl.wikipedia.org/wiki/Playfaircijfer#cite_note-codebreakers-0). De eenvoud in gebruik en de veiligheid van deze polygrafische [substitutieversleuteling](http://nl.wikipedia.org/wiki/Substitutieversleuteling), vergeleken met andere substitutiecijfers zoals [Vigenère](http://nl.wikipedia.org/wiki/Vigen%C3%A8recijfer), maakten van Playfair een populaire cijfermethode die al snel werd overgenomen als veldcijfer. In een 19 pagina's lang pamflet uit 1914 van de hand van [Joseph O. Mauborgne](http://nl.wikipedia.org/w/index.php?title=Joseph_O._Mauborgne&action=edit&redlink=1) wordt voor het eerst de oplossing van een Playfaircijfer gegeven.[[1]](http://nl.wikipedia.org/wiki/Playfaircijfer#cite_note-codebreakers-0)

We beginnen met het opstellen van een vierkant van 5 X 5. We kiezen een sleutelwoord en vullen dit in het vierkant in. Dit kan spiraalgewijs, van onder naar boven, van recht of van links zijn, zolang beide partijen maar een invulmethode afspreken. Hier gebruiken we het woord STALINGRAD. De letters I en J worden als één letter gezien.

S T A L I/J

N G R D B

C E F H K

M O P Q U

V W X Y Z

Eerst breken we de klare tekst op in bigrammen, groepen van twee letters. Indien een bigram uit twee identieke letters bestaat, voegen we een X tussen de tekst in. Indien er één letter overblijft, vullen we aan met een X.

DI TI SE EN ZE ER GE HE IM BE RI CH TX

Nu vercijferen we per bigram. Hiervoor maken we een denkbeeldig vierkant van de te vercijferen letters en zoeken de letters in de 'tegenoverliggende hoeken'. We beginnen met de tegenoverliggende letter in dezelfde rij als de eerste letter van het bigram.

. . . **L** I/J

. . . D **B**

. . . . .

. . . . .

. . . . .

Voor het vierkant DI is dit BL.

DI TI SE EN ZE ER GE HE IM BE RI CH TX

BL

Bij het volgend bigram TI liggen beide letters op dezelfde rij. We nemen dan de letters onmiddellijk rechts ervan op diezelfde rij. Als de letter op de meest rechtse plaats staat moet door worden geteld naar de meest linkse plaats.

**S** T **A** . I/J

. . . . .

. . . . .

. . . . .

. . . . .

Voor het trigram TI is dit dus AS.

DI TI SE EN ZE ER GE HE IM BE RI CH TX

BL AS TC CG WK FG

Bij het bigram GE liggen beide letters in dezelfde kolom. We nemen dan de letters onmiddellijk eronder op diezelfde rij. Als het onderste element gebruikt is dan moet bovenste element genomen worden.

. . . . .

. G . . .

. **E** . . .

. **O** . . .

. . . . .

Voor het bigram GE is dit dus EO.

Alle mogelijke situaties zijn nu beschreven en we kunnen alle bigrammen verder vercijferen.

DI TI SE EN ZE ER GE HE IM BE RI CH TX

BL AS TC CG WK FG EO KF SU GK BA EK AW

De cijfertekst: BLAST CCGWK FGEOK FSUGK BAEKA W

Om de cijfertekst te ontcijferen moeten we enkel het proces omkeren. Voor de vierkanten kiezen we gewoon de tegenover liggende hoeken, voor letters in dezelfde rij kiezen we de letters onmiddellijk links ervan, en voor letters in dezelfde kolom kiezen we de letters onmiddellijk erboven.

# ADFGX-cijfer

Het **ADFGX-cijfer** was tijdens de [Eerste Wereldoorlog](http://nl.wikipedia.org/wiki/Eerste_Wereldoorlog) het handcijfer van de Duitse veld-officier [Erich Ludendorff](http://nl.wikipedia.org/wiki/Erich_Ludendorff) voor het lente-offensief in Frankrijk in [1918](http://nl.wikipedia.org/wiki/1918). Het [cijfer](http://nl.wikipedia.org/wiki/Cryptografie) werd uitgevonden door kolonel [Fritz Nebel](http://nl.wikipedia.org/w/index.php?title=Fritz_Nebel&action=edit&redlink=1). Dit cijfer combineerde [fractionering](http://nl.wikipedia.org/wiki/Fractionering_%28cryptografie%29) van een [Polybiusvierkant](http://nl.wikipedia.org/wiki/Polybiusvierkant), met een enkelvoudige [transpositie](http://nl.wikipedia.org/wiki/Transpositie_%28cryptografie%29). Men koos voor de letters ADFGX omdat deze zeer duidelijk te onderscheiden zijn in [morsecode](http://nl.wikipedia.org/wiki/Morsecode). Tijdens het offensief ontstond een variant die de letter V toevoegde; **ADFGVX**.

## Geschiedenis

De ADFGX-variant werd ingevoerd op [5 maart](http://nl.wikipedia.org/wiki/5_maart) [1918](http://nl.wikipedia.org/wiki/1918), net voor het grote offensief dat begon op [21 maart](http://nl.wikipedia.org/wiki/21_maart). Men had een nieuw cijfer nodig om het verrassingseffect te behouden, en men koos voor het ADFGX-cijfer omdat het onbreekbaar geacht werd.

Op [6 april](http://nl.wikipedia.org/wiki/6_april) 1918 slaagde de [cryptoanalist](http://nl.wikipedia.org/wiki/Cryptoanalist) van het Franse [Bureau du Chiffre](http://nl.wikipedia.org/w/index.php?title=Bureau_du_Chiffre&action=edit&redlink=1) [Georges Painvin](http://nl.wikipedia.org/w/index.php?title=Georges_Painvin&action=edit&redlink=1) erin een bericht in de ADFGX-variant breken. Op [1 juni](http://nl.wikipedia.org/wiki/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](http://nl.wikipedia.org/wiki/2_juni). Hierdoor kregen de Fransen een aanzienlijk strategisch voordeel en wisten de Duitsers in een slag op [9 juni](http://nl.wikipedia.org/wiki/9_juni) terug te dringen. Een keerpunt in het offensief.

Het breken van de versleuteling werd tot 1966 officieel geheimgehouden.

## Werkwijze

We beginnen met het opstellen van een vierkant van 6 × 6. We kiezen een sleutelwoord en vullen dit in het vierkant in. In ons voorbeeld is het eerste sleutelwoord NACHTBOMMENWERPER waarbij we de dubbele letters weglaten en aanvullen met de rest van het alfabet. Om de getallen aan te vullen kunnen we deze vlak na hun letter plaatsen (1 na A, 2 na B enz...). De kolommen en rijen worden benoemd met de letters ADFGVX.

 | **A D F G V X**

-+------------

**A**| N A **1** C **3** H

**D**| **8** T B **2** O M

**F**| E **5** W R P D

**G**| **4** F **6** G **7** I

**V**| **9** J **0** K L Q

**X**| S U V X Y Z

dan zetten we de tekst om in bigrammen, bestaande uit de kop-letters van de rij en de kolom.

d i t i s z e e r g e h e i m

FX GX DD GX XA XX FA FA FG GG FA AX FA GX DX

Vervolgens wordt op de gefractioneerde tekst kolomstranspositie toegepast. In ons voorbeeld is het tweede sleutelwoord PILOTEN (in realiteit worden veel langer sleutelwoorden of zinnen gebruikt). Het sleutelwoord is genummerd volgens het alfabet. De bigrammen worden van links naar rechts en van boven naar onder ingevuld.

**P I L O T E N**

6 2 3 5 7 1 4

-------------

F X G X D D G

X X A X X F A

F A F G G G F

A A X F A G X

D X

Nu lezen we de tekst af volgens de nummering per kolom, en verdelen in groepen van vijf.

De cijfertekst: DFGGX XAAXG AFXGA FXXXG FFXFA DDXGA

Om de cijfertekst te ontcijferen moeten we eerst een tabel maken met het sleutelwoord en het juiste aantal kolommen. Uit het aantal letters in de cijfertekst kunnen we dan het aantal lange en korte kolommen afleiden. We vullen de tabel met de cijfertekst, kolom per kolom, in volgorde van het sleutelwoord. Vervolgens lezen we de tekst van links naar recht en boven naar onder af. De bekomen tekst splitsen we op in bigrammen. Aan de hand van het vierkant zetten we de bigrammen terug om in klare tekst.

# Dubbele transpositie cijfer

Het **dubbele transpositie cijfer** is één van de klassieke [handcijfers](http://nl.wikipedia.org/wiki/Handcijfers), ook wel veldcijfer genoemd vanwege zijn militair gebruik.

Het dubbele transpositie cijfer was één van de veiligste handcijfers dat door alle partijen gebruikt werd tijdens de Tweede Wereldoorlog. De zwakke schakel in dit cijfers is wanneer vele berichten met dezelfde sleutelwoorden vercijferd worden, deze door een ingewikkelde techniek van multiple-anagramming kunnen gebroken worden. Indien men echter regelmatig van sleutelwoorden wisselt is deze methode zeer veilig.

Het dubbele transpositie cijfer bestaat uit twee verschillende kolom-transposities. Men kan hierbij hetzelfde sleutelwoord voor beide stappen gebruiken, of twee verschillende sleutelwoorden kiezen. Men kiest best twee sleutelwoorden van verschillende lengte, het ene met even en het andere met oneven lengte. In ons voorbeeld is het eerste sleutelwoord LEONARDO. De letters van dit woord worden volgens alfabet genummerd, van links naar rechts. Onder dit woord schrijven we de klare tekst van links naar recht en boven naar onder.

**L E O N A R D O**

4 3 6 5 **1** 8 2 7

---------------

D I T I **S** E E N

Z E E R **G** E H E

I M B E **R** I C H

T

Vervolgens lezen we de tekst af per kolom, beginnende met het kleinste nummer. Kolom 1 is dus SGR, kolom 4 is DZIT. De nieuwe tekst schrijven we onder het tweede sleutelwoord DAVINCI eveneens van links naar rechts en van boven naar onder.

**D A V I N C I**

3 **1** 7 4 6 2 5

-------------

S **G** R E H C I

E **M** D Z I T I

R **E** T E B N E

H **E** E I

Tenslotte lezen we de tekst nogmaals af per kolom en volgens nummer. Daarna verdelen we in groepen van vijf.

De cijfertekst: GMEEC TNSER HEZEI IIEHI BRDTE

Om de cijfertekst te ontcijferen moeten we eerst een tabel maken met het tweede sleutelwoord en het juiste aantal kolommen. Uit het aantal letters in de cijfertekst kunnen we dan het aantal lange en korte kolommen afleiden. We vullen de tabel met de cijfertekst, kolom per kolom, in volgorde van het sleutelwoord. Dan lezen we de tekst af van links naar rechts en boven naar onder, en plaatsen die dan in een tweede tabel, met het eerste sleutelwoord. Ook hier vullen we de tabel kolom per kolom, in volgorde van het sleutelwoord. Tenslotte lezen we een laatste keer de tekst af van links naar rechts en boven naar onder om zo de klare tekst te bekomen.

Aangezien berichten normaal veel langer zijn dan deze voorbeelden worden voor de sleutelwoorden van kolom-transpositie dikwijls woorden of zinnen gebruikt met een lengte van 20 of meer letters.

# Straddling checkerboard cijfer

Het **Straddling checkerboard** of spreidend schaakbord is één van de klassieke [handcijfers](http://nl.wikipedia.org/wiki/Handcijfers). Dit cijfer is een [fractionerend](http://nl.wikipedia.org/wiki/Fractionering_%28cryptografie%29) monoalfabetisch [substitutie](http://nl.wikipedia.org/wiki/Substitutie_%28cryptografie%29) cijfer. De tabel heeft 10 kolommen en 3 rijen. De eerste rij mag slechts 8 letters bevatten. Aangezien er 28 vakjes gevuld dienen te worden, kan men aanvullen met een slash ( / om begin en einde van getallen aan te geven waarbij A = 1, B = 2 enz...) en een punt.

Als bovendien in de bovenste rij van de tabel de meest voorkomende letters geplaatst worden is het cijfer beter bestand tegen letterfrequentie-analyse door het onderdrukken van pieken in de frequentietabel en kunnen we spreken van een homofoon cijfer. Tip: De meest vookomende letters kan je onthouden met het woord ANTIROES(T).

Men kan een vast alfabet gebruiken en de nummering van de tabel bepalen aan de hand van een sleutelwoord, of een tabel gebruiken met vaste nummering en het alfabet invullen aan de hand van een sleutelwoord. In ons voorbeeld passen we de eerste methode toe. We gebruiken in de eerste rij het woord ANTIROES(T) en vullen de tweede en derde rij alfabetisch aan. Vervolgens nemen we de eerste 10 letters van het sleutelwoord UBOOTJAGER en nummeren deze alfabetisch, met 0 als laatste getal.

U B O O T J A G E R

0 2 6 7 9 5 1 4 3 8

Met de bekomen getallen nummeren we de kolommen van de tabel. De getallen die in de eerste rij geen letter hebben worden ook gebruikt om de tweede en derde rij te nummeren.

 |0 2 6 7 9 5 1 4 3 8

-+-------------------

 |A N T I R O E S

3|B C D F G H J K L M

8|P Q U V W X Y Z . /

Als bijkomende veiligheid kunnen we eventueel de tweede en derde rij laten verschuiven volgens het getal van die rij. De tweede rij, met het getal 3, zou dan "K L M B C D F G H J" worden en de derde rij zouden we dan 8 plaatsen verschuiven naar "U V W X Y Z . / P Q". Voordeel van deze methode bij een vast alfabet is dat het niet steeds dezelfde lettercombinaties per kolom bevat. In ons voorbeeld gebruiken we echter geen verschuivingen om de alfabetische aanvulling duidelijk te maken.

De vercijfering gebeurt door omzetting van de letters naar de getallen van de rij en kolom. Voor de letters in de bovenste rij wordt echter het getal erboven genomen. Zo krijgt in ons voorbeeld de letter D de getallen 36 en krijgt de letter T enkel het getal 6.

Klare tekst: D I T I S Z E E R G E H E I M

Cijfertekst: 36 37 6 37 4 84 1 1 9 39 1 35 1 7 38

Aangezien onbestaande combinaties niet kunnen gevormd worden bij ontcijfering, kunnen alle getallen samengevoegd worden. Zo kan in ons voorbeeld 36376... de eerste 3 niet alleen gebruikt worden en moet dus wel aan de 6 gekoppeld worden. De volgende twee getallen, 3 en 7, zijn dus ook een paar. Het volgende getal 6 is een alleenstaand getal want er is geen rij met het nummer 6. Het is deze voor Straddling Checkerboard typische onregelmatige nummering die cryptoanalyse bemoeilijkt.

De cijfertekst: 36376 37484 11939 13517 38

Het resultaat van deze vercijfering wordt meestal gevolgd door een bijkomende vercijfering zoals een [dubbele transpositie](http://nl.wikipedia.org/wiki/Dubbele_transpositie_cijfer), uitgevoerd op de getallenrij. Dit verhoogt de sterkte van het cijfer aanzienlijk.

Een beroemde variant is het [VIC cijfer](http://www.quadibloc.com/crypto/pp1324.htm). Bij dit cijfer initialiseert het sleutelwoord een LFG (Lagged Fibonacci Generator). De gegenereerde getallenreeks wordt gebruikt om eerst een gewone en daarna een onderbroken [transpositie](http://nl.wikipedia.org/wiki/Transpositiecijfer) te nummeren. Het VIC cijfer werd gebruikt door VICTOR, de Russische spion Reino Hayhanen. De met VIC vercijferde berichten bleven ongebroken tot Hayhanen in 1957 overliep naar het westen. Het VIC cijfer wordt beschouwd als het meest complex handcijfer dat ooit gebruikt werd. Andere cijfers die een uitgebreid checkerboard met dubbele onderbroken transpositie gebruiken zijn [PPC-XX](http://users.telenet.be/d.rijmenants/nl/ppc-xx.htm) en[SECOM](http://users.telenet.be/d.rijmenants/nl/secom.htm).

# Atbash

**Atbash** is een eenvoudige [substitutieversleuteling](http://nl.wikipedia.org/wiki/Substitutieversleuteling) vergelijkbaar met [Caesarrotatie](http://nl.wikipedia.org/wiki/Caesarcijfer). Atbash komt voor in het Bijbelboek [Jeremia](http://nl.wikipedia.org/wiki/Jeremia) (25:26 & 51:41) en wordt geassocieerd met de esoterische methodologien van Joodse mystici. De naam komt uit het [Hebreeuws](http://nl.wikipedia.org/wiki/Hebreeuws) en illustreert de werking, de eerste (letter) wordt de laatste. A (aleph) wordt Z (taw), B (beth) wordt Y (sin of shin); atbash.

Een minder bekende en meer betwiste variant van atbash, **atbam**, komt schijnbaar voor in [Jesaja](http://nl.wikipedia.org/wiki/Jesaja_%28Hebreeuwse_Bijbel%29) (7:6). Deze methode is volledig gelijk aan het [Caesaralfabet](http://nl.wikipedia.org/wiki/Caesarcijfer#Rot13).

Hiernaast bestaat er ook nog de **atbah** variant waarbij de letters worden omgezet in cijfers en vervangen door het equivalent waarmee het 10 wordt, zodoende wordt Aleph (de eerste letter) vervangen door teth (de negende). Het is onduidelijk wat er exact gebeurd met letters die boven de 10 uitkomen en deze variant komt niet voor in de bijbel. Een voorbeeld is wel te vinden in de [Talmoed](http://nl.wikipedia.org/wiki/Talmoed) (*Seder Mo'ed*, Sukkah 52b).

## Werking

Voor versleuteling noteert men het alfabet als volgt:
A B C D E F G H I J K L M
Z Y X W V U T S R Q P O N
Om te versleutelen men zoekt de te versleutelen letter en vervangt deze door de corresponderende letter daarboven of daaronder. Zodoende wordt een sleuteltekst als *de kunst van het oorlogvoeren* versleuteld tot *wv pfmhg ezm svg llioltelvivm*.

Aangezien atbash een eenvoudige vorm van substitutie is zijn berichten versleuteld middels dit cijfer zeer kwetsbaar voor [frequentieanalyse](http://nl.wikipedia.org/wiki/Frequentieanalyse_%28cryptografie%29).

# Baconalfabet

Een **Baconalfabet** of Baconversleuteling, is een door de Britse filosoof, wetenschapper en politicus [Francis Bacon](http://nl.wikipedia.org/wiki/Francis_Bacon_%28wetenschapper%29) ontwikkelde [versleutelingsmethode](http://nl.wikipedia.org/wiki/Cryptografie) in twee stappen.

## Omschrijving

### Coderen

#### Stap 1

Eerst wordt elke letter in de originele tekst (de "klare tekst") omgezet in een groep van vijf a's of b's (een tweeletter-alfabet) volgens

a → aaaaa g → aabba n → abbaa t → baaba

b → aaaab h → aabbb o → abbab u-v → baabb

c → aaaba i-j → abaaa p → abbba w → babaa

d → aaabb k → abaab q → abbbb x → babab

e → aabaa l → ababa r → baaaa y → babba

f → aabab m → ababb s → baaab z → babbb

- zie figuur 1. Het is hierbij gebruikelijk om de i en de j aan elkaar gelijk te stellen, en ook de u en de v. Dit is een [binaire](http://nl.wikipedia.org/wiki/Binair) codering. Twee tekens (a en b) worden gebruikt op vijf posities, dus er zijn 25 (= 32) mogelijkheden waarvan er 24 worden gebruikt voor 26 letters.

#### Stap 2

Daarna wordt een willekeurige tekst genomen of verzonnen. Deze wordt met twee lettertypes zo geschreven, dat het ene lettertype een "a" betekent en het andere een "b" - zie figuur 2. Het maakt niet uit welke letter wordt gebruikt, het gaat alleen om het lettertype. Om te verhullen dat het om een gecodeerd bericht gaat, worden twee sterk gelijkende lettertypen gebruikt. In figuur 2 scheelt het vaak maar een haaltje.

### Decoderen

De versleutelde tekst wordt op omgekeerde wijze gedecodeerd. Daarom moet de ontvanger het recept voor de lettertypes (figuur 2) ook hebben.

## Nadeel

Een Baconalfabet is een klassiek [handcijfer](http://nl.wikipedia.org/wiki/Handcijfer) (handmatige versleuteling). Het grootste nadeel is dat het handmatige proces arbeidsintensief is.

## Tussenvorm

Gezien het grote *verstop*gehalte van de versleuteling wordt het Baconalfabet gezien als een vorm tussen [cryptografie](http://nl.wikipedia.org/wiki/Cryptografie) en [steganografie](http://nl.wikipedia.org/wiki/Steganografie).

## Modern voorbeeld

De versleuteling van het codewoord *alice* wordt:
alice → aaaaa ababa abaaa aaaba aabaa.

Voor de twee lettertypes in de willekeurige tekst kiezen we elke willekeurige kleine letter = a, elke willekeurige **hoofdletter** = **b**, zodat bijvoorbeeld aaaaa → allem of een ander woord met vijf kleine letters enzovoorts.

 a l i c e

aaaaa a**b**a**b**a a**b**aaa aaa**b**a aa**b**aa

allem e**N**s**E**n w**O**rde nvr**I**j en**G**el

Met als resultaat de over te zenden tekst:
"alle meNsEn wOrden vrIj en Gelijk in waardigheid en rechten geboren."

Om het principe te tonen zijn de hoofdletters en corresponderende b's **vet** weergegeven. In een handschrift valt een codering met twee bijna gelijke lettertypes haast niet op.

# One-time-pad

**One-time-pad**, soms ook wel OTP, Vernam-cijfer, eenmalig blokcijfer, of het perfecte cijfer genoemd, is de enige bewezen methode voor [cryptografie](http://nl.wikipedia.org/wiki/Cryptografie) die een onbreekbare vercijfering mogelijk maakt, mits correct toegepast. Het One-time-pad werd ontwikkeld als een methode voor papier en potlood gebaseerd op het oorspronkelijke door [Gilbert Vernam](http://nl.wikipedia.org/w/index.php?title=Gilbert_Vernam&action=edit&redlink=1) in [1917](http://nl.wikipedia.org/wiki/1917) ontwikkelde systeem voor gebruik bij [telexverkeer](http://nl.wikipedia.org/wiki/Telex_%28communicatie%29).

## Ontstaan

Bij het Vernam systeem werd elke verstuurde 5-bits ITA (International Telegraph Alphabet) Telexcode (een afleiding van de [Baudotcode](http://nl.wikipedia.org/wiki/Baudotcode) voor telegrafie) [modulus 2](http://nl.wikipedia.org/wiki/Modulair_rekenen) opgeteld bij een 5-bits sleutelcode geponst in een geluste papieren strook (Telexband), de one-time-sleutelband. Elk teken van de tekst werd vercijferd met het volgende teken in de sleutelband. Enige tijd later stelde een kapitein van het [US Signal Corps](http://nl.wikipedia.org/w/index.php?title=US_Signal_Corps&action=edit&redlink=1) voor de sleutel uit volledig willekeurige tekens te laten bestaan, even lang als het te verzenden bericht. Zowel zender als ontvanger had een lange band met exact dezelfde sleuteltekens. Deze papieren strook liep bij de zender parallel met de telexband met de **klare tekst**, bij de ontvanger met de band met de **cijfertekst**. Daar de Telexcode in wezen een [binair](http://nl.wikipedia.org/wiki/Binair) getal van 5 posities is, kon de modulo 2 optelling eenvoudig worden uitgevoerd door de [logische functie](http://nl.wikipedia.org/wiki/Booleaanse_algebra) [XOR](http://nl.wikipedia.org/wiki/XOR) (exclusieve OR, exclusieve OF). Vernam bereikte dit (zonder te weten dat het de modulus 2, resp. de genoemde logische functie betrof) met een twaalftal [relais](http://nl.wikipedia.org/wiki/Relais) (elektromagnetische schakelaars). Door hetzelfde te doen met de cijfertekst en de sleutel, werd de originele klare tekst weer verkregen. De uitvinding van Vernam was de basis voor alle latere pen-en-papierversies, gebaseerd op hetzelfde principe. Hoewel de onbreekbaarheid van one-time-pad niet alleen theoretisch bewezen is, maar het systeem ook praktisch toegepast kan worden, is de lange sleutel en het sleutelbeheer een groot probleem.

## Eigenschappen

Om de theoretische onbreekbaarheid van one-time-pad te verwezenlijken dient aan verschillende voorwaarden voldaan te zijn.

* De lengte van de sleutel dient minstens even lang te zijn als de te vercijferen gegevens.
* De sleutel mag enkel bestaan uit werkelijk willekeurige tekens.
* Een sleutel mag slechts één keer gebruikt worden om één bericht te vercijferen en dient na gebruik vernietigd te worden.
* Van een sleutel mogen slechts twee kopieën bestaan, zijnde een voor de verzender en een voor de ontvanger van de gegevens.

Enkel indien een vercijfering aan deze voorwaarden voldoet is deze onbreekbaar. Elke letter van een bericht kan immers vercijferd worden door elke willekeurige letter, met elke willekeurige letter als resultaat. Men kan hier ook niet alle mogelijkheden van de sleutel uitproberen, de zogenaamde [brute-force-attack](http://nl.wikipedia.org/wiki/Brute_force), omdat iedere mogelijk sleutel in een andere oplossing kan resulteren. Zo kan men een bericht op zodanige wijze ontcijferen dat het resultaat een totaal ander bericht is. Wanneer we bijvoorbeeld het woord HALLO vercijferen met de sleutel XTOVB bekomen we ETZGR. Indien we ETZGR echter ontcijferen met de foutieve sleutel EEKCR, bekomen we als klaartekst het woord APPEL. Zo kan men elk vercijferd bericht in eender welke gewenste klaartekst ontcijferen, zolang we maar de "juiste" verkeerde sleutel gebruiken. Er is dus geen mogelijkheid om te weten of het bericht correct ontcijferd werd.

In de praktijk is one-time-pad enkel bruikbaar voor het veilig overbrengen van gegevens indien verzender en ontvanger vooraf op een absoluut veilige manier, meestal door de betrokkenen zelf of een koerier, een sleutel ter beschikking gesteld werd. Bij correct gebruik en toepassing van de voorwaarden is one-time-pad de enige bestaande bewezen perfect veilige vercijfering, bestand tegen elke mogelijke [cryptoanalytische](http://nl.wikipedia.org/wiki/Cryptoanalyse) aanval. Dit werd bewezen in [Claude Shannons](http://nl.wikipedia.org/wiki/Claude_Shannon) verhandeling 'Communication theory of secrecy systems'. Het systeem is o.a. in gebruik geweest tijdens de [koude oorlog](http://nl.wikipedia.org/wiki/Koude_oorlog), voor een veilige communicatie tussen Washington en Moskou.

## Praktische voorbeelden

De logische XOR kan alleen toegepast worden bij binaire tekens. Er wordt daarom gebruik gemaakt van een modulus (of modulo) berekening. Hiertoe wordt de uitkomst van een berekening gedeeld door het modulusgetal, de overgebleven rest is de gewenste uitkomst.

Voorbeeld: 24×26(mod9)=624/9=69, rest 3. De rest 3 is dus de uitkomst van de berekening. Dit soort **eenweg** berekeningen produceert, vooral met berekeningen met machtsverheffen, een uitkomst die niet is te herleiden tot de oorspronkelijke getallen; ze worden o.a. (tezamen met XOR bewerkingen) veel gebruikt in moderne vercijferingssystemen. Een alledaags voorbeeld van een modulus berekening is het bepalen van de tijd na een bepaald aantal uren. Het is nu 3 uur in de middag, hoe laat is het na 59 uur? Berekening:

15+59(mod24)=74/24=3, rest 2. Het is dan dus 2 uur in de morgen (op de derde dag na vandaag).

In het eerste voorbeeld gebruiken we een one-time-pad op basis van getallen. We kiezen als sleutel een reeks totaal willekeurige getallen van 00 tot 99. We geven elke letter een waarde waarbij A=00, B=01 enzovoort tot Z=25. Bij het vercijferen rekenen we met de **afzonderlijke** cijfers: de **overeenkomstige** cijfers van de "waarde" van de letters van de **klare tekst** en die van de sleutel worden modulo 10 (mod10) opgeteld; dit is eenvoudig te verwezenlijken door de positieve overdracht achterwege te laten, dat heeft hier hetzelfde effect als delen. Bijvoorbeeld: 09+05=04 en niet 14! en 24+98=12. Merk op dat de twee cijfers van elke "waarde" **afzonderlijk** worden opgeteld; dat kan hier dus ook van links naar rechts.

Om het bericht te ontcijferen trekken we de sleutel af van de **cijfertekst**, ook hier weer modulo 10, dus zonder eventuele negatieve overdracht (vb. 25-59=76) en zetten vervolgens de getallen weer om in letters.

Tekst: D I T I S G E H E I M

 03 08 19 08 18 06 04 07 04 08 12 (opzoeken in tabel)

Sleutel: +15 84 78 39 66 95 20 16 33 57 48

 ---------------------------------

Resultaat: 18 82 87 37 74 91 24 13 37 55 50

Cijfertekst: 18828 73774 91241 33755 50

Als voorbeeld van de ontcijfering nemen we de tweede positie: het **cijferteken** is 82, daar trekken we de bijbehorende sleutelwaarde 84 mod10 (weer voor elke positie apart) van af:

82-84(mod10)=08, en dat is precies de waarde van de tweede letter in de **klare tekst**.

In volgend voorbeeld maken we gebruik van sleutelletters i.p.v. getallen. De sleutel bestaat hier dus uit een reeks willekeurige letters. Ook hier geven we elke letter een waarde waarbij A=00, B=01 enzovoort tot Z=25. Tekst- en sleutelwaarden worden weer opgeteld, deze keer modulus 26 (hier de gehele waarde, de cijfers dus niet afzonderlijk) en wél met overdracht (als het resultaat groter is dan 25 trekken we 26 af, dat heeft hier hetzelfde effect als delen). Tenslotte zetten we de getallen om in letters. Om het bericht te ontcijferen zetten we cijfertekst en sleutel om in getallen en trekken we de sleutel af van de cijfertekst, ook hier weer met modulo 26 (als het resultaat kleiner is dan 0 tellen we er 26 bij).

Tekst: D I T I S G E H E I M

 03 08 19 08 18 06 04 07 04 08 12

Sleutel: X V H E U W N O P G D

 +23 21 07 04 20 22 13 14 15 06 03

 ---------------------------------

Resultaat: 26 29 26 12 38 28 17 21 19 14 15 (in tabel opzoeken)

Mod 26 = 00 03 00 12 12 02 17 21 19 14 15 (facultatief)

 ---------------------------------

Cijfertekst: A D A M M C R V T O P

Cijfertekst: ADAMM CRVTO P

Om het werk te vereenvoudigen kunnen we een Vigenère-tabel (tabula recta) gebruiken om de letters op te zoeken, dat is behoorlijk omslachtig. Het kan veel eenvoudiger: we maken onderstaande hulptabel, dan hoeven we ook de modulus 26 niet te berekenen door 26 af te trekken resp. op te tellen, we kunnen de letter namelijk direct in de tabel aflezen. De tabel is zowel bij het vercijferen als het ontcijferen te gebruiken.

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 Z

------------------------------------------------------------------------------------

Waarde 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

Mod - 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51

Mod + -26-25-24-23-22-21-20-19-18-17-16-15-14-13-12-11-10-09-08-07-06-05-04-03-02-01

Er zijn nog vele andere manieren om one-time-pad toe te passen, maar deze zijn altijd gebaseerd op een willekeurige sleutel die bij de te vercijferen gegevens wordt opgeteld.

## Problemen bij gebruik

Om one-time-pad toe te passen zijn er twee belangrijke problemen die het gebruik ervan bemoeilijken en zeer duur maken:

* Een eerste probleem is van technische aard en betreft het produceren van grote aantallen willekeurige getallen of tekens voor de sleutel. Om absolute willekeurigheid te maken kan men deze reeksen niet creëren met behulp van eenvoudige mechanische of elektronische middelen. Het produceren van grote aantallen van deze willekeurige gegevens is dan ook een dure onderneming.
* Het tweede probleem is van praktische aard. Aangezien elke sleutel even groot als de te vercijferen gegevens dient te zijn en slechts eenmalig gebruikt mag worden zijn er een grote aantal verschillende sleutels nodig en dienen deze op veilige wijze ter beschikking gesteld te worden van verzender en ontvanger van een bericht. Dit heeft enorme logistieke en veiligheidsproblemen tot gevolg, indien er veel communicatie beveiligd dient te worden.

In de praktijk werd dit grotendeels opgelost door meerdere genummerde, lange banden, resp. grote aantallen pagina's met sleutelcodes te gebruiken. Bij de telexband ging men voor het volgende bericht gewoon verder met de sleuteltekst op het punt waar het vorige bericht opgehouden was. Dit werd geforceerd door bijvoorbeeld de lezer die de band met de sleutels las, te voorzien van een mesje dat de transportponsing doorsneed nadat een positie gelezen was. Dit teken en alle voorgaande tekens konden dus automatisch niet meer gebruikt worden. Bij de "pads" werden alle reeds gebruikte pagina's (ze waren soms tevens als werkpagina's ingericht) vernietigd; men begon dus bij een volgende pagina. In beide gevallen had men dus de beschikking over een flinke voorraad sleutels.

## Toepassingen

Vanwege de praktische bezwaren om een one-time-pad correct toe te passen is het gebruik ervan zeer beperkt. Zij worden o.a. gebruikt voor communicatie tussen [inlichtingendiensten](http://nl.wikipedia.org/wiki/Inlichtingendienst) en hun veldagenten. De one-time-pad-sleutels, dikwijls zeer kleine boekjes of blaadjes met getallenreeksen, soms op microfilms, kunnen gemakkelijk verborgen worden.

Tot begin jaren '80 werden zij ook gebruikt om militair en diplomatiek telex-verkeer te beveiligen. De telexen gebruikten daarbij het originele principe van Vernam met de one-time-banden. Later volgden elektronische systemen zoals computer-en telefoonverbindingen die gebruikt maakten van een elektronisch opgeslagen one-time-pad-sleutel.

De enorme kosten voor veilige productie, verspreiding, beheer en vernietiging van enorme aantallen one-time-tapes en pads konden enkel gedragen worden door overheidsinstanties zoals leger, inlichtingendiensten en diplomatie. Door het exponentieel toenemen van communicatie werd grootschalig gebruik van one-time-pads onhoudbaar en schakelde men over op de meer praktische, maar weliswaar minder veilige, cryptografische apparaten en computeralgoritmes.

Een vervangend alternatief voor one-time-pad zijn de "stream ciphers" of [stroomvercijfering](http://nl.wikipedia.org/wiki/Stroomvercijfering), waarbij via een algoritme een pseudo-willekeurige getallenreeks geproduceerd wordt. Beginnen beide partijen met eenzelfde parameter in dit algoritme (en dat moet dus weer gecommuniceerd worden), dan zal het resultaat exact hetzelfde zijn. Deze stromen benaderen slechts de werkelijke willekeurigheid en voldoen dus nooit aan de voorwaarden om onbreekbaar te zijn. De gebruikte algoritmen hiervoor voorzien dan ook vaak in een methode om dit bijna 100% te bereiken. Dikwijls wordt ten onrechte aangenomen dat men een one-time-pad kan creëren met de random-functie op computers, terwijl deze vaak gebruikmaken van een algoritme dat niet bedoeld is om grote series willekeurige getallen te produceren. Moderne computersystemen bezitten overigens over verbeterde algoritmen. De enige tot nu toe bekende manier is de sleutels te maken via een elektronische ruisgenerator met nog wat elektronica. Hiervan neemt men aan dat de output volkomen willekeurig is, mits de schakeling en de bouw ervan aan een serie voorwaarden voldoet.

Vanwege zijn absolute veiligheid blijft one-time-pad echter nog steeds in gebruik bij communicatie waar veiligheid en geheimhouding absolute voorrang hebben. De toepassingen zijn echter zeer beperkt. Dit is onder meer het geval bij de zogenaamde [hotlines](http://nl.wikipedia.org/wiki/Hotline) van belangrijke wereldleiders en topgeheime communicatie bij inlichtingendiensten en legers. Tijdens de koude oorlog werd het systeem nog gebruikt voor communicatie tussen Washington en Moskou.

## Snake Oil

Helaas zijn er in de praktijk vele voorbeelden van vercijfering die beweren onbreekbaar te zijn, maar die niet voldoen aan de nodige vereisten. Zo is er veel software op de markt waarvan de makers beweren het onbreekbare one-time-pad of Vernam-systeem toe te passen - klinkt indrukwekkend - maar in werkelijkheid geen echt willekeurige gegevens genereren, een te kleine sleutel gebruiken of meermaals vercijferen met dezelfde sleutel. Bovendien heeft het geen zin om bestanden eenmalig te vercijferen met een eenmalige sleutel die even groot is, en veilig dient bewaard te worden, respectievelijk overgebracht te worden naar de ontvanger. Men kan evengoed het bestand zelf op veilige wijze bewaren of overbrengen.

Zo is er het fantastisch klinkende verhaal van de oplossing van het sleutelbeheer door middel van twee sleutels. Meneer A zendt zijn bericht, vercijferd met sleutel A. Meneer B kan dit niet ontcijferen, maar vercijfert dit nogmaals met zijn eigen sleutel B, en stuurt dit terug naar Meneer A. Die ontcijfert het bericht met zijn sleutel A en zendt dit nogmaals naar Meneer B. Aangezien het bericht nu enkel nog vercijferd is met sleutel B kan Meneer B het toch ontcijferen, en dit zonder uitwisseling van de geheime sleutels! Hoewel hier op het eerste zicht one-time-pad is toegepast zonder het probleem van sleuteldistributie, gaat de vlieger echter niet op. Meneer A stuurt het bericht één keer met zijn sleutel en één keer met B's sleutel, én het wordt door Meneer B, met beide sleutels vercijferd, teruggestuurd. Elke sleutel werd tweemaal gebruikt, voldoet dus niet meer aan de verplichte voorwaarden, en het bericht kan gebroken worden:

Sleutel B = bericht(A+B) - bericht(A) & Sleutel A = bericht(A+B) - bericht(B)

Maar er is nog iets anders: het zogenaamde "ontcijferde" bericht bevat vaak louter onzin, want er is een klassiek symmetrisch vercijfersysteem gebruikt. Dat zit zo: bij symmetrische systemen wordt wat het laatste is gedaan bij het vercijferen, als eerste teruggedraaid bij het ontcijferen. Het is als met aan- en uitkleden: bij het aankleden worden eerst de sokken aangetrokken, vervolgens de schoenen; bij het uitkleden worden eerst de schoenen uitgetrokken, daarna de sokken. Zoals duidelijk te zien is, is dat hierboven niet het geval. NB. Wordt een van bovengenoemde one-time-pad systemen met modulo berekeningen gebruikt, waarbij A en B ongelijke sleutels hebben, het maakt namelijk niet uit in welke volgorde je de verschillende optellingen en aftrekkingen doet. Het ontcijferde bericht is dan wel correct; het tweemaal gebruiken van een sleutel blijft natuurlijk fout.

Er zijn nog vele variaties op dit thema en voorbeelden van ronduit slechte cryptografische systemen en software die al dan niet goedbedoelde "onbreekbare" veiligheid aanbieden, maar daarbij minstens een van de verplichte voorwaarden negeren. Deze programma's zijn bekend onder de term [snake-oil](http://nl.wikipedia.org/w/index.php?title=Snake-oil&action=edit&redlink=1), of slangenolie, genoemd naar de producten van kwakzalvers.

# Paardensprongcijfer

Een **paardensprongcijfer** is een manier voor het [versleutelen](http://nl.wikipedia.org/wiki/Cryptografie) van *platte tekst*, gebaseerd op het [schaakstuk paard](http://nl.wikipedia.org/wiki/Paard_%28schaken%29). Voor de versleuteling maakt men gebruik van een schaakbord, een eenheid met 64 cellen. Het paard maakt in het schaakspel specifieke *sprongen* binnen een rechthoek van 2x3. Men *springt* met het paard net zolang totdat alle vlakken van het bord eenmaal bestreken zijn en geeft de cellen een oplopende nummering, als volgt:

* Paardensprongschaakbord

 1 4 53 18 55 6 43 20

52 17 2 5 38 19 56 7

 3 64 15 54 31 42 21 44

16 51 28 39 34 37 8 57

63 14 35 32 41 30 45 22

50 27 40 29 36 33 58 9

13 62 25 48 11 60 23 46

26 49 12 61 24 47 10 59

Vervolgens voegt men de te versleutelen tekst in op de oplopende nummers waarna men ofwel de kolommen ofwel de rijen afleest en geschikt maakt voor verzending. Er bestaat ook de variatie dat men eerst de tekst in het vierkant van 8x8 plaatst, waarna men de letters er in de oplopende volgorde van de paardensprong uitleest.

Aangezien er enorm veel mogelijkheden zijn voor een zogenaamde [*Knight's Tour*](http://en.wikipedia.org/wiki/Knight%27s_Tour) is het zaak dat zender en ontvanger een [identieke route](http://nl.wikipedia.org/wiki/Symmetrische_cryptografie) volgen. Paardensprongversleuteling is een [transpositiecijfer](http://nl.wikipedia.org/wiki/Transpositiecijfer).

# Polybiusvierkant

Een **Polybiusvierkant** is een, door de Grieks historicus [Polybios](http://nl.wikipedia.org/wiki/Polybios) ontwikkeld, [versleutelings](http://nl.wikipedia.org/wiki/Cryptografie)-gereedschap waarmee de letters van het alfabet vervangen worden door cijfers.

## Algemene vorm

In zijn algemene vorm ziet een polybiusvierkant er als volgt uit:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|   | **1** | **2** | **3** | **4** | **5** |
| **1** | A | B | C | D | E |
| **2** | F | G | H | I | K |
| **3** | L | M | N | O | P |
| **4** | Q | R | S | T | U |
| **5** | V | W | X | Y | Z |

Elke letter wordt vervolgens vervangen door zijn betreffende coördinaten in het vierkant. POLYBIUS wordt dus 35 34 31 54 12 24 45 43. Het weglaten/samenvoegen van de I en de J is een gebruikelijke manier om de 26 letters in een vierkant van 5 bij 5 te passen. Polybius had dit probleem niet aangezien hij het 24 letters tellende [Griekse alfabet](http://nl.wikipedia.org/wiki/Grieks_alfabet) gebruikte. Polybiusvierkanten bestaan ook in 6 bij 6 varianten om bijvoorbeeld het [Cyrillische alfabet](http://nl.wikipedia.org/wiki/Cyrillische_alfabet) (33 letters) mee te versleutelen.

## Veiligheid

Tekst versleuteld met een polybiusvierkant alleen verschaft geen werkelijke beveiliging aangezien de methode uitmondt in [monoalfabetische substitutie](http://nl.wikipedia.org/wiki/Substitutieversleuteling#Monoalfabetische_substitutie). De vierkanten bieden echter de mogelijkheid om een tekst te [fractioneren](http://nl.wikipedia.org/wiki/Fractionering_%28cryptografie%29) en kan als zodanig gebruikt worden in complexere versleutelingen zoals de [nihillistversleuteling](http://nl.wikipedia.org/w/index.php?title=Nihillist_versleuteling&action=edit&redlink=1).

# Rozenkruisersgeheimschrift





Pigpen

Het **rozenkruisersgeheimschrift** (ook wel *vrijmetselaarsalfabet*) is een monoalfabetische [versleutelings-methode](http://nl.wikipedia.org/wiki/Cryptografie) waarbij de letters van de *platte tekst* door middel van eenvoudig te onthouden diagrammen verborgen worden. De methode, die ook onder de minder lovende naam *varkenshokversleuteling* (of *pigpen*) bekend is, wordt in het algemeen toegeschreven aan de [rozenkruisers](http://nl.wikipedia.org/wiki/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](http://nl.wikipedia.org/wiki/Heinrich_Cornelius_Agrippa_von_Nettesheim) die de methode uitlegt in zijn *De occulta philosophia* uit [1533](http://nl.wikipedia.org/wiki/1533). Dit werk werd in [1586](http://nl.wikipedia.org/wiki/1586) door [Blaise de Vigenère](http://nl.wikipedia.org/wiki/Blaise_de_Vigen%C3%A8re) hergebruikt in zijn tractaat aangaande geheimschrift. Er zijn vele varianten mogelijk, een geoefend [cryptoanalist](http://nl.wikipedia.org/wiki/Cryptoanalyse) zal doorgaans echter geen moeite hebben met de ontcijfering.

# Scytale

Een **scytale** (ookwel **skytale**, Grieks *σκυτάλη*) is een cryptografisch gereedschap dat wordt gebruikt om [transpositionele](http://nl.wikipedia.org/wiki/Transpositie_%28cryptografie%29) 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](http://nl.wikipedia.org/wiki/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 ookwel stafversleuteling genaamd kan men van veel voorwerpen een scytale maken. Bijvoorbeeld van een potlood, een glas, een vaas of zelfs een boek.

Om *platte 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.