Geheim

# De Opdracht

## Opdrachtgever:

De opdrachtgevers zijn Ralf van den Broek en Bas Heijne, docenten aan de Hanzehogeschool Groningen.

TODO: Standaard tekst hanzehogeschool plus logo en link.

## Situatie:

In het internettijdperk wordt er gigantische hoeveelheden informatie over het internet verspreid. In de vorm van telefoongesprekken, whatsapp berichten, E-mail, banktransacties, skype gesprekken, bezochte websites, enz. Sommige dingen daarvan zijn nauwelijks vertrouwelijk, voor andere berichten zijn er duistere partijen die bereid zijn veel moeite te doen om ze te onderscheppen. Veel berichten zitten hier natuurlijk tussen in.

Om dit in de praktijk goed uit te voeren wordt gebruik gemaakt van cryptografie. Dit is de kunst van het versleutelen en ontsleutelen van berichten. Hierbij komen tegenwoordig verschillende wiskundige principes samen om ervoor te zorgen dat

## De opdracht:

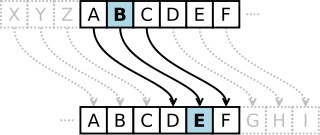
Voor jullie licht nu de opdracht om een methode te maken waarmee jullie onderling berichten naar elkaar kunnen sturen en versturen zonder dat iemand die meeluistert weet wat jullie bespreken.

# Uitwerking van de opdracht

## Oriëntatie:

Verdiep je voordat je begint in een aantal varianten van klassieke cryptografie. Bekijk in elk geval caesar encryptie, scytale en boekversleuteling. Verdiep je ook in de mogelijkheden om deze te breken, zoals histogramanalyse.

### Klassieke cryptografie[[bewerken](https://nl.wikipedia.org/w/index.php?title=Cryptografie&action=edit&section=3)]



Een voorbeeldversleuteling: de rotatie van Caesar, waarbij alle letters drie letters doorschuiven

Cryptografie gaat terug tot het oude [Egypte](https://nl.wikipedia.org/wiki/Oude_Egypte); bepaalde ontdekte tombes hebben afwijkende [hiërogliefen](https://nl.wikipedia.org/wiki/Hi%C3%ABroglief). Het is waarschijnlijk dat dit bedoeld is om boodschappen mee te versluieren. Ook in de [Kama Sutra](https://nl.wikipedia.org/wiki/Kama_Sutra) komt cryptografie voor. Van de Griekse schrijver Lysander weten we dat ten tijde van [Alexander de Grote](https://nl.wikipedia.org/wiki/Alexander_de_Grote) de [scytale](https://nl.wikipedia.org/wiki/Scytale_(cryptografie)) in gebruik was. Uit de tijd van Caesar stamt het [Caesarcijfer](https://nl.wikipedia.org/wiki/Caesarcijfer), een voorbeeld van een [substitutiecijfer](https://nl.wikipedia.org/wiki/Substitutiecijfer). Dit soort versleuteling kan gebroken worden met [frequentieanalyse](https://nl.wikipedia.org/wiki/Frequentieanalyse_(cryptografie)), die vermeld wordt in geschriften van Arabische geleerden zoals [Al-Kindi](https://nl.wikipedia.org/wiki/Al-Kindi).

Het meest beruchte voorbeeld van (slechte) cryptografie komt uit het [Babingtonverraad](https://nl.wikipedia.org/w/index.php?title=Babingtonverraad&action=edit&redlink=1). Het geheimschrift van [Anthony Babington](https://nl.wikipedia.org/wiki/Anthony_Babington) en zijn kornuiten werd gebroken door [Thomas Phelippes](https://nl.wikipedia.org/wiki/Thomas_Phelippes). Mede hierdoor werd [Maria I van Schotland](https://nl.wikipedia.org/wiki/Maria_I_van_Schotland) veroordeeld wegens hoogverraad. Het [Grote Geheimschrift van Lodewijk XIV](https://nl.wikipedia.org/wiki/Grote_Geheimschrift_van_Lodewijk_XIV) en de geheimschriften van [Johannes Trithemius](https://nl.wikipedia.org/wiki/Johannes_Trithemius) bleven daarentegen lange tijd ongebroken. Het [Voynichmanuscript](https://nl.wikipedia.org/wiki/Voynichmanuscript) is nog steeds onontcijferd.

Rond [1585](https://nl.wikipedia.org/wiki/1585) schreef de Franse diplomaat [Blaise de Vigenère](https://nl.wikipedia.org/wiki/Blaise_de_Vigen%C3%A8re) het *Traicte de Chiffres* waarin hij uitleg geeft over het later naar hem vernoemde [Vigenèrecijfer](https://nl.wikipedia.org/wiki/Vigen%C3%A8recijfer). Deze *polyalfabetische versleuteling* was een aanzienlijke verbetering op de tot dan gebruikte [substitutiecijfers](https://nl.wikipedia.org/wiki/Substitutiecijfer) maar is weinig gebruikt, het is buitengewoon omslachtig; codeboeken in combinatie met homofone substitutie zijn lange tijd de meest gebruikte vorm van geheimschrift geweest.

In de jaren 1700 had elke Europese [grootmacht](https://nl.wikipedia.org/wiki/Grootmacht) zijn eigen zogenaamde "Zwarte Kamer", een soort [geheime dienst](https://nl.wikipedia.org/wiki/Geheime_dienst) waar een team van codebrekers geheime berichten ontcijferden. Cryptografie speelde een belangrijke rol in een aantal slagen in de [Spaanse Onafhankelijkheidsoorlog](https://nl.wikipedia.org/wiki/Spaanse_Onafhankelijkheidsoorlog). [George Scovell](https://nl.wikipedia.org/wiki/George_Scovell) wist het berichtenverkeer van Napoleons troepen te ontcijferen waardoor de troepen van de Hertog van Wellington voorkennis hadden van op handen zijnde activiteiten.

Cryptografie werd gepopulariseerd door [Edgar Allan Poe](https://nl.wikipedia.org/wiki/Edgar_Allan_Poe) die zijn kennis in *Alexander's Weekly Messenger* uiteen zette. Later schreef hij [*De goud-kever*](https://nl.wikipedia.org/wiki/De_goud-kever)*, het eerste voorbeeld van cryptografie in fictie. Arthur Conan Doyle liet zijn* [Sherlock Holmes](https://nl.wikipedia.org/wiki/Sherlock_Holmes) ook een cryptografisch raadsel oplossen in *het verhaal van de dansende mannen*. Daarnaast gebruikte [Jules Verne](https://nl.wikipedia.org/wiki/Jules_Verne) in zijn *Mathias Sandorf* een methode die bekendstaat als *draaiend roosterversleuteling*. Meer recent gebruikte [Dan Brown](https://nl.wikipedia.org/wiki/Dan_Brown) cryptografie in zowel [*De Da Vinci Code*](https://nl.wikipedia.org/wiki/De_Da_Vinci_Code_(boek)) *als in* [*Het Juvenalis Dilemma*](https://nl.wikipedia.org/wiki/Het_Juvenalis_Dilemma)*.*

*https://nl.wikipedia.org/wiki/Cryptografie#Klassieke\_cryptografie*

## Een eerste versie:

Bedenkt dan voor het eerste keuzecollege een eigen versleuteling en ontsleutelingsmethode waarmee je binnen je groep willekeurige berichten naar elkaar kunt sturen.

Keuzecollege 1:  
 - Basis cryptografie  
 - Breken van de gemaakte codes  
 - Programmeerlessen in python  
 - Les priemgetallen en modulo rekening  
 -Introductie hanzehogeschool

## Orientatie moderne cryptografie:

Orienteer je op technieken voor moderne cryptografie. Denk aan het verschil tussen symmetrische en assymetrische cryptografie, manieren zoals ASCII om tekst om te zetten in getallen, en waarom priemgetallen en modulorekening gebruikt worden in cryptografie.

## Leer python:

Probeer tussen de keuzecolleges 2 je inzicht in python te vergroten. Zorg ervoor dat je je encryptiemethoden. Pythonboek: http://www.spronck.net/pythonbook/pythonboek.pdf

**Python** is een [programmeertaal](https://nl.wikipedia.org/wiki/Programmeertaal) die begin [jaren 90](https://nl.wikipedia.org/wiki/1990-1999) ontworpen en ontwikkeld werd door [Guido van Rossum](https://nl.wikipedia.org/wiki/Guido_van_Rossum), destijds verbonden aan het [Centrum voor Wiskunde en Informatica](https://nl.wikipedia.org/wiki/Centrum_voor_Wiskunde_en_Informatica) (daarvoor [Mathematisch Centrum](https://nl.wikipedia.org/wiki/Mathematisch_Centrum)) in Amsterdam. De taal is mede gebaseerd op inzichten van professor [Lambert Meertens](https://nl.wikipedia.org/wiki/Lambert_Meertens) die een op [BASIC](https://nl.wikipedia.org/wiki/BASIC)gebaseerde taal genaamd [ABC](https://nl.wikipedia.org/wiki/ABC_(programmeertaal)) had ontworpen, maar dan met allerlei zeer geavanceerde datastructuren. Inmiddels wordt de taal doorontwikkeld door een enthousiaste groep, geleid door Van Rossum. Deze groep wordt ondersteund door vrijwilligers op het [internet](https://nl.wikipedia.org/wiki/Internet). De ontwikkeling van Python wordt geleid door de [Python Software Foundation](https://nl.wikipedia.org/wiki/Python_Software_Foundation). Python is [vrije software](https://nl.wikipedia.org/wiki/Vrije_software).

Python heeft zijn naam te danken aan het favoriete televisieprogramma van Guido van Rossum, [Monty Python's Flying Circus](https://nl.wikipedia.org/wiki/Monty_Python%27s_Flying_Circus).[[1][2]](https://nl.wikipedia.org/wiki/Python_(programmeertaal))

*https://nl.wikipedia.org/wiki/Python\_(programmeertaal)*

Keuzecollege 2:  
 - Introductie moderne cryptografie  
 - RSA  
 - Programmeren in python  
 - Wiskunde  
 - Andere problemen met cryptografie

## De opdracht:

Schrijf een programma dat een door jullie gekozen ecryptiemethode kan uitvoeren. Je moet zowel kunnen versleutelen als ontsleutelen.

Je programma moet gebruik maken van een sleutelbestand om de versleuteling en ontsleuteling uit te voeren. Dit sleutelbestand mag hetzelfde zijn voor beide acties (dan is er sprake van symmetrische cryptografie) of anders (dan is er sprake van assymetrische cryptografie)