06. les 6 het grote publiek

Auteur	Its Academy
Laatst gewijzigd	18 december 2014
Licentie	CC Naamsvermelding-GelijkDelen 3.0 Nederland licentie
Webadres	https://maken.wikiwijs.nl/45957

Inhoudsopgave

Les 6 Het grote publiek

Inhoud van les 6: Het grote publiek

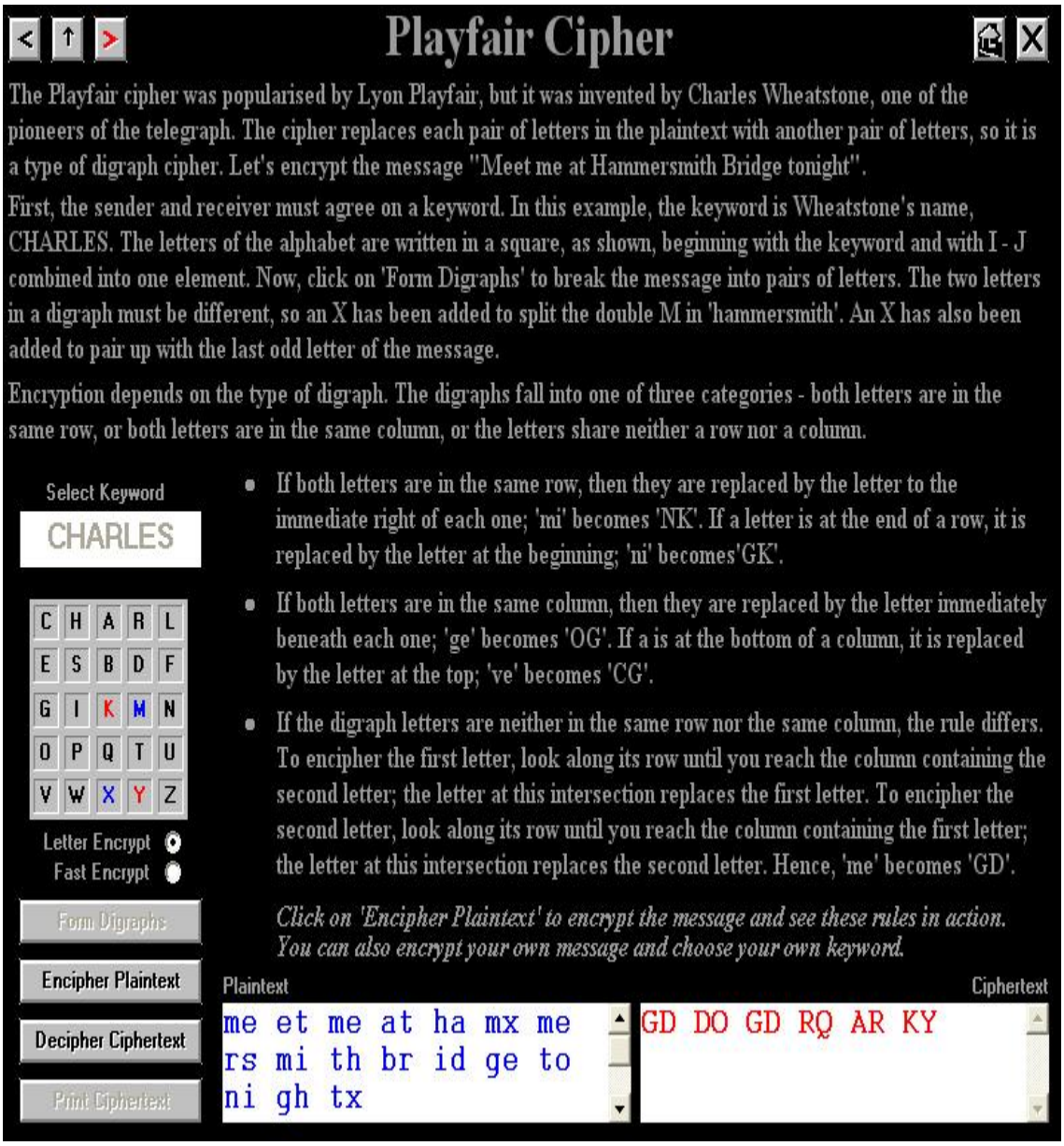
6.1 Playfair cijfer

Het Vigenère-cijfer had zijn betrouwbaarheid verloren na de publicatie van Kasiski. Er was dus dringend behoefte aan een nieuwe geheimtaal maar deze zou lang op zich laten wachten. De opkomst van de telegraaf maakte mensen bewust dat hun privacy beschermd moest worden. Hierdoor werd ook bij het grote publiek het geheimschrift populair. Allerlei verschillende geheimschriften werden ontwikkeld, waarvan we er hier een paar zullen bekijken.

In de Victoriaanse tijd was het geliefden in Engeland verboden elkaar hun genegenheid te laten blijken. Via 'persoonlijke oproepen' in de krant stuurden ze elkaar vercijferde berichten. Van Charles Babbage is bekend dat hij het een geliefde bezigheid vond om met zijn vrienden, Sir Charles Wheatstone en baron Lyon Playfair, de kranten af te speuren en berichten te ontcijferen. Cryptografen begonnen cijfertekstjes te plaatsen om daarmee hun collega's uit te dagen.
Naar een idee van Wheatstone ontwikkelde Babbage en zijn vrienden het zogenaamde Playfair-cijfer. Volgens dit systeem worden letterparen vervangen door andere letterparen. Op de CD-rom onder Junior Code Breakers/Playfair Cipher vind je onderstaand voorbeeld en wordt de werking gedemonstreerd. Voor je dit gaat bekijken kun je in opgave 1 proberen dit cijfer zelf te gebruiken en het voorbeeld af te maken.
De vercijfering loopt via een 5x5 vierkant waarin eerst een sleutelwoord wordt gekozen en de rest van de letters van het alfabet worden toegevoegd. Dit is vergelijkbaar met het sleutelwoord bij substitutie zoals dit aan het eind van les 1 werd uitgevoerd. De I en de J zijn gecombineerd tot één letter. De klare tekst wordt opgesplitst in tweetallen van 2 verschillende letters. Als er 2 gelijke letters gevormd dreigen te worden dan wordt er een vreemde letter (bijvoorbeeld een X) in de tekst ingelast. In onderstaand voorbeeld zouden de 2 m's in het woord Hammersmith een paar vormen. Door toevoeging van de x ontstaan de letterparen ha mx me rs mi th. Vervolgens worden de letters vervangen op de manier zoals in de Engelse tekst hieronder wordt uitgelegd.

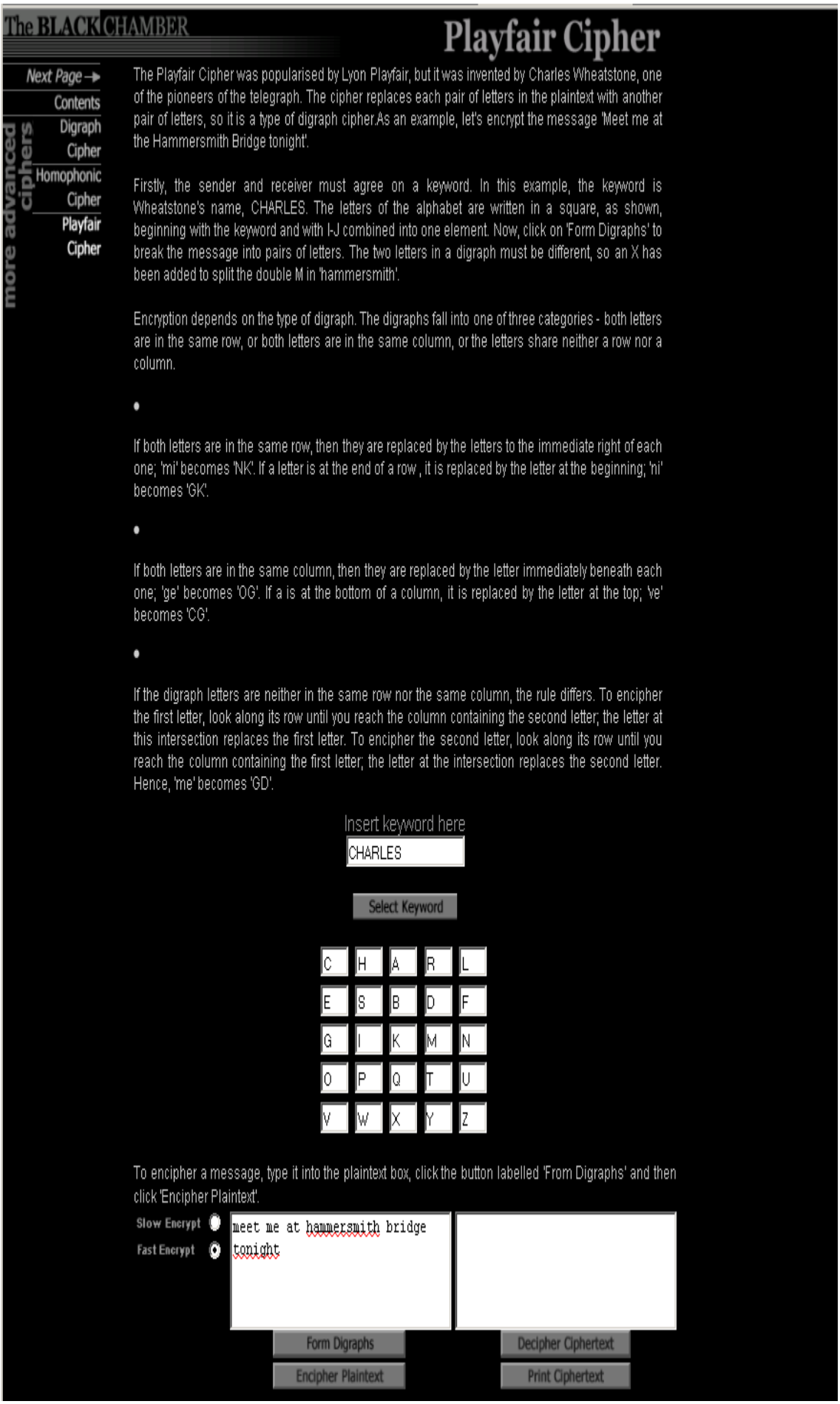
Opgave 1

Bestudeer de werking van het Playfair Cipher hieronder bij de drie aandachtspunten en maak de vercijfering af zonder gebruik te maken van de tool.



Opgave 2

Ontcijfer het volgende bericht met gebruik van de tool hieronder:
CS UQ CR ZD HK CM SC SG ID HA HM DU VS DM CV TC CS OD DC DP UP GO SO HB PM MF SD VG CD GU TC CU KV


The BLACK CHAMBER
Playfair Cipher
Next Page
Contents
more advanced ciphers
Digraph Cipher
Homophonic Cipher
Playfair Cipher
The Playfair Cipher was popularised by Lyon Playfair, but it was invented by Charles Wheatstone, one of the pioneers of the telegraph. The cipher replaces each pair of letters in the plaintext with another pair of letters, so it is a type of digraph cipher.As an example, let's encrypt the message 'Meet me at the Hammersmith Bridge tonight'.
Firstly, the sender and receiver must agree on a keyword. In this example, the keyword is Wheatstone's name, CHARLES. The letters of the alphabet are written in a square, as shown, beginning with the keyword and with I-J combined into one element. Now, click on 'Form Digraphs' to break the message into pairs of letters. The two letters in a digraph must be different, so an X has been added to split the double M in 'hammersmith'.
Encryption depends on the type of digraph. The digraphs fall into one of three categories - both letters are in the same row, or both letters are in the same column, or the letters share neither a row nor a column.
If both letters are in the same row, then they are replaced by the letters to the immediate right of each one; 'mi' becomes 'NK'. If a letter is at the end of a row , it is replaced by the letter at the beginning; 'ni' becomes 'GK'.
If both letters are in the same column, then they are replaced by the letter immediately beneath each one; 'ge' becomes 'OG'. If a is at the bottom of a column, it is replaced by the letter at the top; 've' becomes 'CG'.
If the digraph letters are neither in the same row nor the same column, the rule differs. To encipher the first letter, look along its row until you reach the column containing the second letter; the letter at this intersection replaces the first letter. To encipher the second letter, look along its row until you reach the column containing the first letter; the letter at the intersection replaces the second letter. Hence, 'me' becomes 'GD'.
Insert keyword here
CHARLES
Select Keyword
C H A R L
E S B D F
G I K M N
O P Q T U
V W X Y Z
To encipher a message, type it into the plaintext box, click the button labelled 'From Digraphs' and then click 'Encipher Plaintext'.
Slow Encrypt
Fast Encrypt
meet me at hammersmith bridge tonight
Form Digraphs
Encipher Plaintext
Decipher Ciphertext
Print Ciphertext

Klik hier om naar de site te gaan.

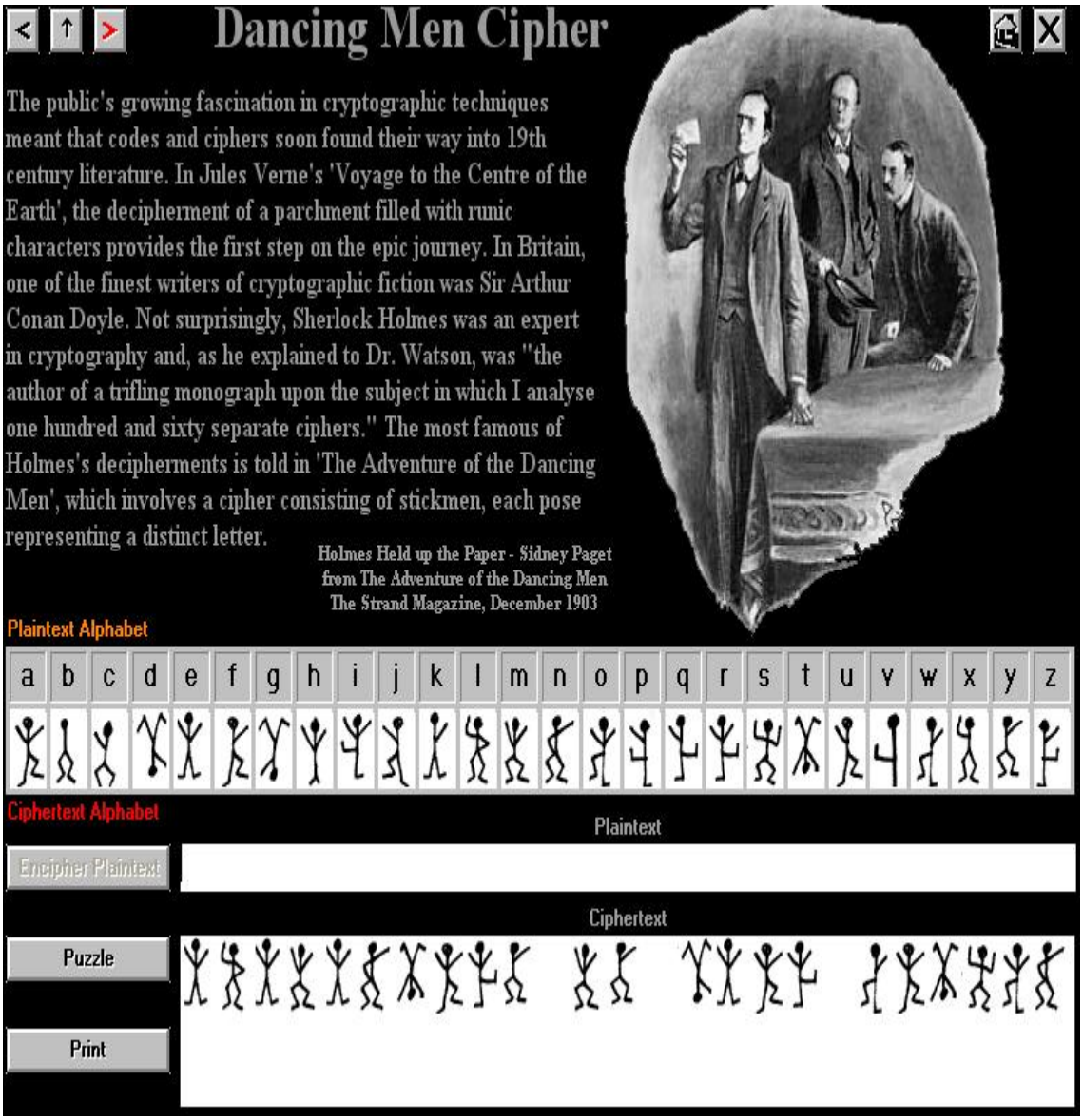
Het Playfair-cijfer was aan te tasten door te zoeken naar de meest voorkomende digrammen in de cijfertekst, en aan te nemen dat ze de meest algemene digrammen in de Engelse taal vertegenwoordigen, zoals de th, he, an, in, er, re en es.
Toch zou het cijfer in het geheim overgenomen worden door het Britse ministerie van oorlog.

6.2 Cijfers voor het grote publiek

Een wijdverbreide vorm van encryptie was de speldenprik-encryptie. Een brief versturen was kostbaar, maar kranten werden gratis verstuurd. De *zunige mensen* bedachten om elkaar boodschappen te sturen door op de voorpagina van de krant onopgemerkt letters te markeren met een speldenprikje. In wezen is dit een vorm van steganografie, het verbergen van een bericht.

Ook in de literatuur van de negentiende eeuw deed de cryptografie zijn intrede, zoals in het boek *Reis naar het middelpunt van de aarde* van Jules verne. Ook was Sherlock Holmes een expert in cryptografie:
Hieronder is het Dancing Men Cipher van Sherlock Holmes opgenomen in een leesactiviteit. Het is een beetje vergelijkbaar met het varkenshokcijfer en je kunt het terugvinden op de CD-rom onder Junior Code Breakers/Dancing Man.

 leesactiviteit



Opdracht: Ontcijfer de puzzle van het Dancing Men Cipher uit de bovenstaande afbeelding.

Voor het antwoord: (maar ontcijfer het eerst zelf!)

klik hier

6.3 Het boekcijfer en de Beale Papers

Een ware geschiedenis is het verhaal van The Beale Papers. Thomas Beale gaf in 1822 een kistje in bewaring bij Robert Morriss, een hoteleigenaar in het Amerikaanse Lynchburg in Virginia. In het kistje zou een geheim bewaard zijn over een bewaarplaats van een grote goud- en zilverschat die begraven lag. Drie vercijferde documenten bevatten slechts getallen. Het eerste beschreef de vindplaats van de schat, de tweede de inhoud en het derde gaf een lijst van verwanten aan wie Beale de schat naliet. Morriss gaf het geheim, dat hij zelf niet had kunnen ontraadselen, uiteindelijk in vertrouwen door aan een vriend. Deze wist de tweede pagina te ontcijferen en publiceerde anoniem het verhaal in een brochure. Het eerste en derde document is tot op heden nog niet ontcijferd.
Het gebruikte cijfersysteem in The Beale Papers berust op het zogenaamde *boekcijfer*: in een lange tekst worden eerst de woorden genummerd. In de klare tekst wordt letter voor letter vervangen door het nummer van een woord dat met deze letter begint. Staat er in een tekst op de 135ste plek het woord *infiltration* dan kan een *i* in de klare tekst dus vervangen worden door het getal 135. Zonder de

tekst is het daarom niet mogelijk de tekst te ontcijferen.
De anonieme schrijver had ontdekt dat het tweede document was vercijferd met de*Onafhankelijkheidsverklaring* van Amerika. Na jaren van vergeefse pogingen om de andere documenten te ontcijferen was de anonieme schrijver vervallen tot grote armoede. Hij besloot het geheim in 1885 openbaar te maken om er vanaf te zijn. Velen hebben nadien geprobeerd het geheim te ontrafelen maar de schat, als hij bestaat, ligt nog altijd begraven. Het boekcijfer is alleen te breken als de cryptoanalist beschikt over het juiste boek en het is denkbaar dat de eerste en derde tekst vercijferd zijn door een onbekende tekst van Beale zelf.

 Reflectie

Waarom is het boekcijfer zonder te beschikken over het boek onmogelijk te breken?

klik hier

In 1894 vond Guglielmo Marconi de radio uit. Na verloop van tijd werd dit aantrekkelijk voor militaire doeleinden omdat men ontdekte dat op deze manier rechtstreekse communicatie tussen commandanten en hun ondergeschikten mogelijk werd. Direct was ook duidelijk dat elke vijand het signaal kon ontvangen en mee kon luisteren, waardoor de behoefte aan een betrouwbare encryptie alleen maar verder groeide. Er werden echter geen spectaculaire vorderingen gemaakt onder de cryptografen en eigenlijk kon elk geheimschrift wel ontcijferd worden aan het eind van de negentiende eeuw.

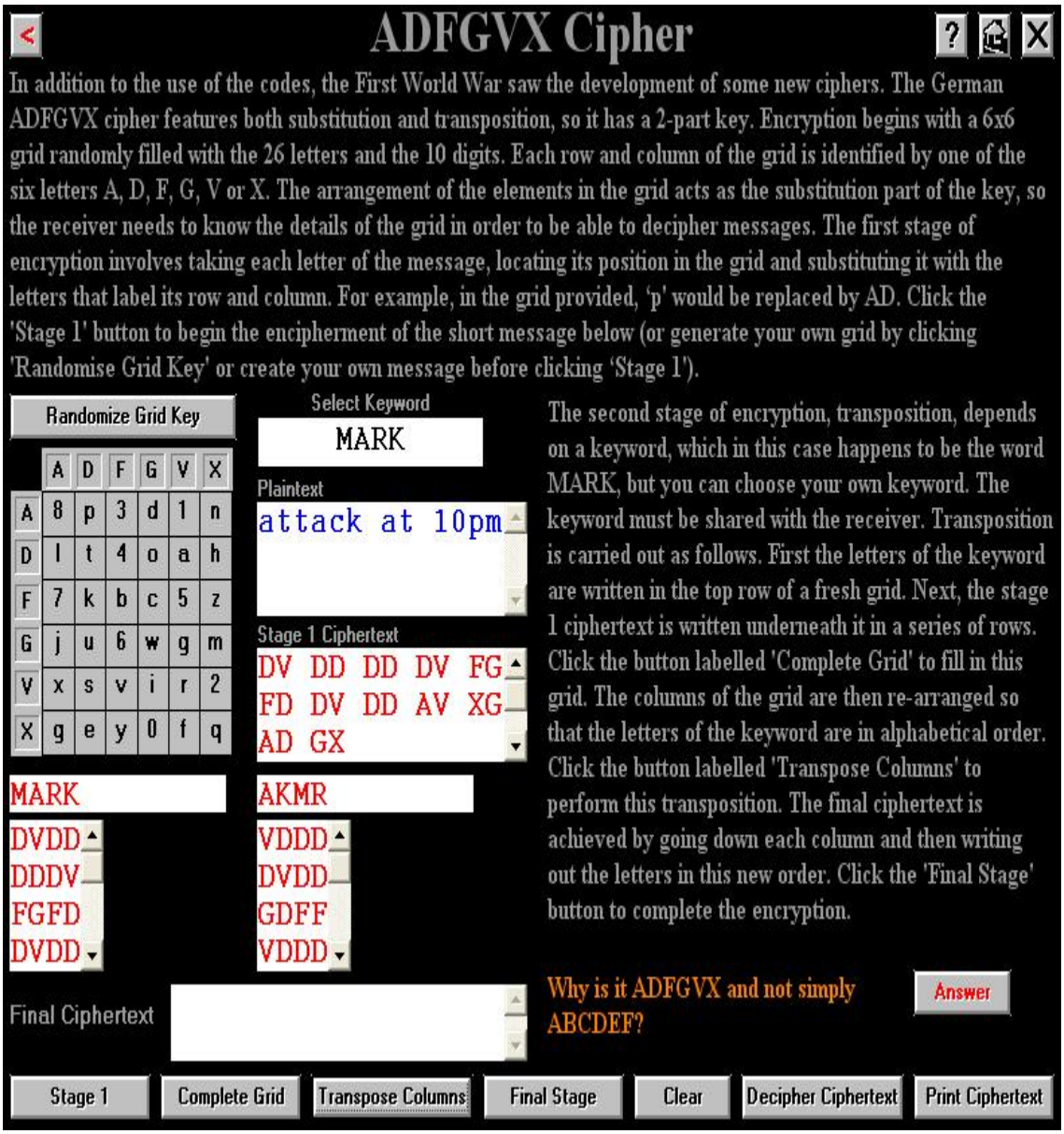
6.4 Het ADFGVX systeem

Op 5 maart 1918, tijdens de Eerste Wereldoorlog, voerden de Duitsers vlak voor het grote Duitse initiatief van 21 maart het ADFGVX systeem in. Het werd onbreekbaar geacht en was voor die tijd ook redelijk ingewikkeld. Het bestond uit een combinatie van het substitutieschrift en het transpositiesysteem. Op 2 juni 1918 werd het gekraakt door Georges Painvin, waardoor een grote hoeveelheid onderschepte berichten ontcijferd kon worden. Het verrassingselement van de aanval van de Duitsers op Parijs, die een week later gepland was, was verdwenen en het Duitse leger werd teruggeslagen.

Het ADFGVX systeem bestaat uit een 6x6 vierkant, waarin op willekeurige wijze de 26 letter- en 10 cijfersymbolen zijn opgenomen. Substitutie zorgt ervoor dat elke letter van de klare tekst wordt vervangen door de letters vóór de rij en bóven de kolom waarin de klare letter staat. Vervolgens wordt er een transpositie toegepast met gebruik van een sleutelwoord.

Hieronder is het ADFGVX systeem opgenomen in een leesactiviteit. Voer de opdracht die eronder staat uit met gebruik van de CD-rom. Onder Highlights/ADFGVX vind je een tool om met een afgesproken sleutelwoord een eigen tekst te sturen aan een andere deelnemer aan de cursus. Deze moet dit bericht met het afgesproken sleutelwoord weer kunnen ontcijferen.

 leesactiviteit



Beantwoord eerst onderstaande reflectievraag en maak de encryptie af met gebruik van de CD-rom onder Highlights/ADFGVX.

Bedenk een eigen tekst en spreek een sleutelwoord af met diegene aan wie je een bericht uitwisselt. Probeer zijn of haar antwoord te ontcijferen.

Kun je ook antwoord geven op de vraag 'Why is it ADFGVX and not simply ABCDEF?'

klik hier

Reflectie

Het ADFGVX systeem maakt gebruikt van transpositie (fase 2 in bovenstaande Engelse tekst). Hoe werkt de transpositie?

klik hier

Het Zimmermann telegram

Het verloop van de Eerste Wereldoorlog werd sterk beïnvloed door de cryptoanalyse. In de eerste twee

jaar van de oorlog smeekte Engeland bijna aan Amerika om zich te mengen in de strijd tegen de Duitsers, maar de Amerikaanse president Woodrow Wilson volhardde in een neutrale houding. In november 1916 werd een nieuwe Duitse minister van buitenlandse zaken benoemd, Arthur Zimmerman, die zei te streven naar vrede. De Duitse bevelhebbers geloofden dat de sterke Duitse vloot van 200 nagenoeg onkwetsbare U-boten (onderzeeboten) de doorslag zouden geven in de strijd tegen Engeland. Door de aanvoerlijnen af te snijden zou Engeland door uithongering op de knieën gedwongen worden. Belangrijk daarbij was het om Amerika ertoe te brengen neutraal te *blijven*. Daarvoor bedacht Zimmerman het plan om Mexico tot bondgenoot te maken en te verleiden om Amerika met steun van Duitsland aan te vallen. Het zou Texas, New-Mexico en Arizona, grondgebieden die vroeger van Mexico waren geweest, terugvorderen.
Bovendien zou Mexico kunnen bemiddelen in een poging om Japan zover te krijgen dat het Amerika aan zou vallen.
Op 16 januari 1917 verstuurde Zimermann het voornemen van een onbeperkte onderzeeoorlog in een telegram aan de Duitse ambassadeur in Washington. Deze paste het bericht aan en verstuurde het op zijn beurt naar de ambassadeur in Mexico, die het aan de Mexicaanse regering aan zou moeten bieden. De aanval zou op 1 februari worden ingezet.
De Duitse communicatielijnen met de buitenwereld waren aan het begin van de oorlog doorgesneden nadat een Brits schip de onderzeese kabels had opgevist. Daardoor werd het telegram verstuurd via de kabels van Zweden, die over Engeland liepen. En zo werd het bericht onderschept door de Britse geheime dienst en ontsleuteld door het cijferbureau, beter bekend als *Kamer 40*. De Britse geheime dienst voelde er echter weinig voor om het bericht openbaar te maken omdat daarmee duidelijk zou worden dat het Duitse cijfer was gebroken. Dit zou de Duitsers er ongetwijfeld toe brengen een nieuw geheimschrift te bedenken. In opdracht van admiraal Hall lieten de Britten de zeeoorlog beginnen zoals gepland zonder iets door te geven. Toen de eerste schepen werden getroffen bleven de Amerikanen desondanks neutraal.
Via een Britse agent in Mexico slaagden de Britten er in om bij het Mexicaanse telegraafkantoor de Mexicaanse versie van het Zimmermann telegram te bemachtigen. Het werd aan de Amerikaanse ambassadeur overhandigd en aan de pers vrijgegeven. De Duitsers waren ervan overtuigd, dat het bij de Mexicaanse regering was gestolen en Amerika kon weinig anders doen dan zich mengen in de oorlog.
Ondertussen plaatste de Britse admiraal Hall ter camouflage een stuk in de Britse pers, waarin hij zijn eigen organisatie afkraakte omdat deze het bericht niet zelf had kunnen onderscheppen.


Meerkeuzevraag

De Britse admiraal Hall gaf na het uitbreken van de zeeoorlog in de pers flink af op de Britse geheime dienst.
Wat was daarvan de reden?

a. De Britse admiraliteit was niet in staat geweest om te voorkomen dat de schepen werden getorpedeerd door de Duitsers.
a. De reactie van Hall was een soort excuus aan de Amerikanen omdat de Britten hen had moeten waarschuwen.
a. Hall voerde een show op om de Duitsers om de tuin te leiden.

6.5 Het blokcijfer

Tegen het einde van de Eerste Wereldoorlog bedachten wetenschappers in Amerika een verbetering op het Vigenère-systeem dat een onbreekbare code opleverde. De zwakheid van het Vigenère-cijfer is te wijten aan de periodiciteit, dat wil zeggen na het aantal letters ter grootte van het sleutelwoord wordt weer dezelfde schuiftabel gebruikt. Door nu het sleutelwoord langer te maken wordt dit probleem aanzienlijk verkleind. Het autokey-systeem gaf daar een eerste antwoord op, maar dit systeem bleek weer kwetsbaar doordat de tekst zelf wordt gebruikt voor de vercijfering. Hiermee worden de taaleigenaardigheden van de tekst in de sleutel opgesloten (zie les 5). Hetzelfde zou gebeuren als je als sleutel een lange tekst zou kiezen in de eigen taal.
De wetenschappers bedachten dat de sleutel even lang zou moeten zijn als de tekst en zou moeten bestaan uit willekeurige letters. Majoor Joseph Mauborgne, hoofd van de cryptografische dienst van het Amerikaanse leger, ontwierp zogenaamde codeblokken die bestonden uit honderden vellen met betekenisloze aaneenschakelingen van letters en daarmee is de vercijfering onbreekbaar. De zender en de ontvanger zouden uiteraard over dezelfde blokken moeten beschikken en dezelfde pagina moeten gebruiken. Na gebruik van een pagina werd deze vernietigd. Het systeem heet het *eenmalig blokcijfer*.
Een cijfertekst van 25 letters zou met 26^{25} verschillende sleutels vercijferd kunnen zijn, dat is meer dan 20.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000 of 20 triljard keer een biljard.

 Meervoudige selectie

Hoewel perfect kleven er toch een paar nadelen aan het systeem van het eenmalige blokcijfer.
Welke nadelen heeft het systeem?

a. Door simpelweg alle mogelijke sleutels uit te proberen is het cijfer te kraken ook al duurt dat wel erg lang.
a. Door de grote hoeveelheid berichten die verstuurd moeten worden ontstaat een probleem om de sleutels te versturen.
a. Het produceren van een grote hoeveelheid willekeurige letters is een lastige klus.

klik hier

Opgave 3

Als een admiraal aan 25 verschillende onderzeeërs een bericht wil kunnen sturen moet hij met elke marconist een apart blok blokcijfers uitwisselen. Stel dat iedere onderzeeër ook moet kunnen communiceren met de andere onderzeeërs, hoeveel verschillende blokken moeten er dan verspreid worden?

Opgave 4

Wat voor nadeel zou eraan kleven om één blok te gebruiken en dat over alle onderzeeërs te verspreiden?

Uit opgave 3 en 4 wordt duidelijk dat de admiraal welhaast gedwongen zou zijn om de pagina's met de blokcijfers te hergebruiken. In de cryptografie is dat echter een doodzonde.

Opgave 5

Waarom wordt het hergebruiken van *eenmalige blokcijfers* gezien als een doodzonde?

Noot

Het eenmalige blokcijfer is eigenlijk alleen maar te gebruiken tussen mensen die ultrageheime informatie moeten uitwisselen en die het zich kunnen veroorloven om de vellen willekeurige letters te laten produceren.
De *hotline* van de presidenten uit Rusland en Amerika is beveiligd met een *eenmalig blokcijfer.*

Over dit lesmateriaal

Colofon

Dit materiaal is achtereenvolgens ontwikkeld en getest in een SURF-project (2008-2011: e-klassen als voertuig voor aansluiting VO-HO) en een IIO-project (2011-2015: e-klassen&PAL-student). In het SURF project zijn in samenwerking met vakdocenten van VO-scholen, universiteiten en hogescholen e-modules ontwikkeld voor Informatica, Wiskunde D en NLT. In het IIO-project (Innovatie Impuls Onderwijs) zijn in zo’n samenwerking modules ontwikkeld voor de vakken Biologie, Natuurkunde en Scheikunde (bovenbouw havo/vwo). Meer dan 40 scholen waren bij deze ontwikkeling betrokken. Organisatie en begeleiding van uitvoering en ontwikkeling is gecoördineerd vanuit Bètapartners/Its Academy, een samenwerkingsverband tussen scholen en vervolgopleidingen. Zie ook www.itsacademy.nl De auteurs hebben bij de ontwikkeling van de module gebruik gemaakt van materiaal van derden en daarvoor toestemming verkregen. Bij het achterhalen en voldoen van de rechten op teksten, illustraties, en andere gegevens is de grootst mogelijke zorgvuldigheid betracht. Mochten er desondanks personen of instanties zijn die rechten menen te kunnen doen gelden op tekstgedeeltes, illustraties, enz. van een module, dan worden zij verzocht zich in verbinding te stellen met de programmamanager van de Its Academy (zie website). Gebruiksvoorwaarden: creative commons cc-by sa 3.0 Handleidingen, toetsen en achtergrondmateriaal zijn voor docenten verkrijgbaar via de bètasteunpunten.

Auteur	Its Academy
Laatst gewijzigd	18 december 2014 om 14:07
Licentie	Dit lesmateriaal is gepubliceerd onder de Creative Commons Naamsvermelding-GelijkDelen 3.0 Nederland licentie. Dit houdt in dat je onder de voorwaarde van naamsvermelding en publicatie onder dezelfde licentie vrij bent om: • het werk te delen - te kopiëren, te verspreiden en door te geven via elk medium of bestandsformaat • het werk te bewerken - te remixen, te veranderen en afgeleide werken te maken • voor alle doeleinden, inclusief commerciële doeleinden. Meer informatie over de CC Naamsvermelding-GelijkDelen 3.0 Nederland licentie

Aanvullende informatie over dit lesmateriaal

Van dit lesmateriaal is de volgende aanvullende informatie beschikbaar:

Leerniveau	; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ;
Leerinhoud en doelen	; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ;
Eindgebruiker	leerling/student
Moeilijkheidsgraad	gemiddeld
Trefwoorden	e-klassen rearrangeerbaar