JULIUS CAESAR
Het eerste bewijs dat geheimschrift werkelijk werd gebruikt voor militaire doeleinden vinden we in het boek van Julius Caesar over de Gallische oorlogen. Hij beschrijft hoe zijn brief, bevestigd aan een speer, het Romeinse kamp binnen gegooid werd. Het geheimschrift van de Romeinse keizer noemen we het Caesar-alfabet en bestaat uit het drie plaatsen opschuiven van alle letters van het alfabet (Rot3). Augustus, de eerste keizer van Rome vond het afdoende de letters slechts één plaats op te schuiven (Rot1).

ROT13
Afgeleid van het Caesar-alfabet is de methode Rot13. Hierbij zet men de eerste 13 letters van het alfabet op de bovenste rij met daaronder de laatste 13 letters. Zo zijn het versleutelings- en het ontsleutelingsmechanisme gelijk. Deze methode word tegenwoordig gebruikt in nieuwe media als Usenet.

POLYBIUS
De Griekse schrijver Polybius zette voor het eerst letters om in cijfers met behulp van een vierkante tabel. Elke letter werd vervangen door twee cijfers, namelijk het nummer van de rij gevolgd door het nummer van de kolom waar de letter in staat. SCRYPTION wordt dus: 43 13 42 54 35 44 24 34 33.
Dit vierkant wordt het ‘schaakbord’ genoemd en lag aan de basis van latere cijfersystemen. De letters I en J werden samengevoegd omdat het veld slechts ruimte gaf aan 25 letters. Het systeem van Polybius gaf de mogelijkheid een boodschap over grote afstand door te seinen met behulp van toortsen. Bijvoorbeeld: de toorts eenmaal rechts omhoog zwaaien en vier maal links = D.

ATBASH
Ook in het Oude Testament komen we lettervervangingen tegen. De naam Sesach werd gebruikt waar Babel werd bedoeld. Deze -van oorsprong Hebreeuwse- versleuteling wordt Atbash genoemd en verving de eerste letter van het alfabet door de laatste, de tweede door de voorlaatste, dus A werd Z, B werd Y enzovoort. Atbash inspireerde middeleeuwse monniken en schrijvers tot het gebruik van systemen waarbij een letter werd vervangen door een andere, vaste letter.

SPARTANEN
Het eerste militaire cryptografische systeem werd in de 5e eeuw voor Christus bedacht door de Spartanen. Daarbij gebruikten zij voor het eerst een hulpmiddel: de Skytale. Dat was een stok waar een lange strook papyrus of perkament omheen werd gewikkeld zodat de hele stok bedekt werd. De boodschap schreef men over de hele lengte van de stok, waarna de strook werd afgewikkeld en verzonden. De boodschap werd pas weer leesbaar wanneer de strook door de ontvanger om een stok van gelijke dikte werd gewikkeld. In die tijd hadden mensen vaak een staf bij zich die als Skytale kon dienen; om die reden wordt de Skytale-methode ook wel ‘stafversleuteling’ genoemd. Het is niet bekend of dit systeem ooit echt is gebruikt.

SUMERIËRS
In Mesopotamië was rond 2600 voor Christus het oudste, bekende geheimschrift in gebruik. Het heette UD GAL NUN en kon slechts door een kleine groep ingewijden

worden gebruikt. Het was een geheimschrift in spijkerschrift.

EGYPTENAREN
Het geheime karakter van het hiërogliefenschrift werd versterkt doordat een deel in rebusvorm kon worden gezet of doordat de schrijfrichting kon variëren.
Als men de tekst moeilijker leesbaar wilde maken, verving men gemakkelijk leesbare tekens door nieuwe of minder gebruikte hiërogliefen.
Op de steen van Rosette (196 voor Chr.) staat dezelfde tekst in 3 talen; in hiërogliefen, in demotisch schrift en in het Grieks. Door deze 'codesleutel' heeft men voor het eerst in de 19e eeuw hiërogliefen kunnen ontcijferen.

TRITHEMIUS
In 1506 schreef de beroemde geleerde Trithemius een boek in zes delen over cryptologie met de titel: 'Polygraphia'(veel schrijfmethoden).
Onder de verschillende geheimschriftsystemen die hij beschreef was de polyalfabetische vervanging, waarbij in een tekst een en dezelfde letter door verschillende letters kan worden vervangen. Daardoor werd het ontcijferen van een codetekst vele malen moeilijker dan wanneer een letter steeds door dezelfde letter werd vervangen.
Met behulp van de 'Tabula Recta', de vierkante tabel, werd de eerste letter van de klare tekst vervangen door de letter die er onder stond op de tweede regel, de tweede letter door die op de derde regel, enzovoort.
Zo werd 'EEN' bijvoorbeeld omgezet in 'FGQ'.

DE ARABISCHE WERELD
In de Middeleeuwen kwam de Arabische cultuur tot grote bloei. Doordat de Koran afbeeldende kunsten verbood, hield men zich vooral bezig met taal en schrift. Woordraadsels, rebussen, anagrammen en geheimschrift waren een onderdeel van de taalstudie. De Arabische wetenschappers hielden zich als eerste bezig met cryptanalyse. Rond 1400 schreef Qalqashandi een hoofdstuk in zijn encyclopedie over onzichtbare inkt, geheimschrift en cryptanalyse.

SPIEGELSCHRIFT
Een van de meest bekende geheimschriften is dat van Leonardo da Vinci.
Hij was als uitvinder van de helikopter, het verrijdbare kanon en de onderzeeër bang dat hij gek verklaard en gedood zou worden, of dat zijn ideeën in verkeerde handen zouden vallen. Hij had dus een goede reden om deze uitvindingen geheim te houden, daarom beschreef hij zijn studies in spiegelschrift.

FREQUENTIEANALYSE
Om een cryptogram te kunnen kraken is onderzoek nodig naar hoe vaak iedere letter van een alfabet in de gebruikte taal voorkomt; hoe vaak in combinatie met andere letters; hoe vaak bepaalde uitgangen van woorden voorkomen, enzovoort. Deze kenmerken worden onderzocht in het te ontcijferen geheimschrift, waarna de gevonden kenmerken met elkaar vergeleken worden. Zo kan een begin worden gemaakt met het vinden van de betekenis van de meest voorkomende tekens in dat bepaalde schrift.
PORTA
Belangrijk voor de ontwikkeling van de moderne cryptologie was Giovanni

Porta. Hij adviseerde zo veel mogelijk opzettelijke schrijffouten te maken en woorden niet steeds te herhalen om frequentieanalyse bij ontcijfering extra moeilijk te maken. Hij legde de basis voor het polyalfabetische systeem dat later in de 20ste eeuwse geheimschriftmachines werd toegepast, door verschillende bestaande systemen te combineren.

CARDANO
Girolamo Cardano ontwierp in het begin van de 16e eeuw een geheimschriftrooster dat naar hem werd genoemd. Dit rooster werd gemaakt van stevig materiaal waarin verspreid over het oppervlak rechthoekige gaten werden uitgesneden met de hoogte van één regel, maar van verschillende lengte. De woorden van de boodschap werden in de gaten geschreven, Het rooster werd weggehaald en de ruimte tussen de woorden werd met onschuldige tekst volgeschreven. Door een identiek rooster over de vol geschreven brief te leggen kon men het bericht lezen.

DE TURNING GRILLE
Gebaseerd op het principe van het rooster van Cardano was de turning Het verschil was dat dit rooster ronde gaten had en vier maal om zijn as gedraaid werd, waardoor alle letterposities eenmaal beschreven werden. Men legde het rooster op het papier en beschreef de gaten letter voor letter, regel voor regel, van linksboven naar rechtsonder. Vervolgens draaide men het rooster een kwart slag en beschreef opnieuw de gaten. De posities die open bleven na invulling van de boodschap werden met losse letters opgevuld. Om de boodschap te kunnen lezen had de ontvanger eenzelfde rooster nodig. Het rooster kon verschillende aantallen gaten hebben.

NOMENCLATUUR
In het algemeen verstaan we onder ‘nomenclatuur’ de afspraken die we maken over termen binnen een bepaald systeem. Een bekend voorbeeld daarvan zijn de namen van planten en dieren. Wanneer we spreken over een Picea Abies weet natuurlijk iedereen dat we het hebben over een Fijnspar en wie het niet uit het hoofd weet kan het opzoeken in een plantenboek of natuurgids. Zo stonden in een codeboek namen, woorden of lettergrepen met de daarbij behorende geheime code. De code was vaak een getal of lettercombinatie. Volgens dit codeboek betekent de geheimeboodschap: 10 41 96 00 ‘Hélène is om 6 uur op het stadhuis in Le Havre’.

REBUS
Wij kennen rebussen tegenwoordig als leuke spelletjes die je als kind oplost. Maar de Egyptenaren waren meesters in het maken van rebussen om boodschappen door te geven. Hun hiërogliefenschrift was immers helemaal opgebouwd uit plaatjes.
Ook de schrijver Willem Bilderdijk, die in de 18e eeuw gedwongen werd Nederland te verlaten, schreef vanuit Engeland rebusbrieven aan zijn familie in Amsterdam. Het waren ware kunstwerken en voor de ontcijfering bestond geen codeboek!

ZWARTE KAMERS
Vrijwel alle westerse landen hadden zwarte kamers; organisaties waar cryptanalisten zich vaak dag en nacht bezighielden met het openen, kopiëren

en weer onzichtbaar sluiten en –als het nodig was- ontcijferen van onderschepte post uit en voor het buitenland. In Nederland had het Haagse postkantoor van 1751 tot 1803 een zwarte kamer waarvan maar enkele ambtenaren het bestaan kenden. Hier werd alle post van de Franse en Pruisische ambassadeurs onderschept en door de ‘secretaris van de cijfers’ overgeschreven, waarna hij het bericht thuis decodeerde. Tijdens de Franse overheersing werd zelfs alle Nederlandse post door de Franse postkamer gecontroleerd.

KONINKLIJKE BOODSCHAP

In de 16e, 17e en 18e eeuw was het gebruik van geheimschrift in het vorstelijk huis heel gewoon. Van veel brieven die in code zijn verstuurd zijn alleen de ontcijferde teksten bewaard gebleven. De originele codeberichten werden direct na ontcijfering vernietigd. Prins Willem I schreef op 21 september 1572 een brief aan zijn broer Jan, deels in klare taal, deels in cijfercode. De brief was ondertekend met ‘Guille de Nassau’. In het Koninklijk Huisarchief bevindt zich deze brief, gedateerd op 21 juni 1800, geheel geschreven met behulp van een turning grille. Max Divoys probeerde eind 18e eeuw in België een opstand uit te lokken. Op 20 november 1801 schreef hij een brief in nomenclatuur aan de erfprins van Oranje, later koning Willem I. Deze brief is nog altijd niet ontcijferd.

Z.O.P.

Zie Onder Postzegel kwam in opkomst in 1871 bij de invoering van de briefkaart. Op een briefkaart, waarop men een verhaal mocht schrijven, moest 2,5 cent worden geplakt en op een prentbriefkaart 1 cent. Maar een prentbriefkaart mocht naast naam en adres van geadresseerde en afzender, geen geschreven tekst bevatten. Dit tariefverschil leidde tot een veel gepleegde vorm van fraude: de Z.O.P. Men schreef met potlood een bericht onder de postzegel, die losgeweekt moest worden door de ontvanger en schreef op de kaart: Z.O.P. Deze methode werd niet alleen gebruikt om portokosten te ontduiken, maar ook om geheime boodschappen te verzenden.

POSTZEGELTAAL

Door de postzegel op een bepaalde plaats en in een bepaalde stand te plakken, kon men een boodschap doorgeven. Men kon aan de voorkant of de achterkant van de enveloppe plakken, de enveloppe op zijn kop, de postzegel in verschillende hoeken, op zijn kop of op zijn kant. Elke stand en plaats had een andere betekenis.

DIPLOMATIE

In de diplomatieke diensten bediende men zich voor de correspondentie van en naar de ambassades, sinds de 16e eeuw van geheimschrift. Door het bestaan van ‘zwarte kamers’ in de diverse Europese landen was men genoodzaakt diplomatieke geheimen in code te versturen. Eeuwenlang heeft men hiervoor nomenclatuur gebruikt omdat berichten er sneller en zekerder mee te coderen en decoderen waren dan met behulp van een cijferschijf of een tabula recta. Het was daarbij wel van belang de ambassadeurs regelmatig van een nieuwe sleutel te voorzien, want over hoe meer onderschepte en gedecodeerde brieven van eenzelfde nomenclatuur de zwarte kamer van een vijandig land beschikte, hoe gemakkelijker het werd de sleutel te vinden.

BLAISE DE VIGENÈRE

De fransman Blaise de Vigenère verbeterde de Tabula Recta van Trithemius aanzienlijk, door de alfabetten op de beide assen door elkaar te plaatsen en door er een sleutelwoord aan toe te voegen.

Voorbeeld: het sleutelwoord is ‘SCRYPTION’ (vertikaal) en het woord ‘GEVAAR’ (horizontaal) moet worden versleuteld. Men neemt van beide woorden de eerste letter (S en G). Op het kruispunt van deze letters vindt men de letter O, het woord ‘GEVAAR’ wordt zo ‘OMARYS’.
Het sleutelwoord herhaalt zich voortdurend.

CSA SCHIJF

In de Amerikaanse Burgeroorlog wordt in het veld deze koperen geheimschriftschijf met een doorsnede van 6 centimeter gebruikt voor het versleutelen van boodschappen. Ook in WO I hadden Amerikaanse soldaten deze schijfjes in hun uitrusting. CSA staat voor ‘Confederate States of America’ en SS voor ‘Secret Service’

ALBERTI

Leon Batista Alberti was de eerste die in de 15e eeuw een polyalfabetische sleutel bedacht. Hij ontwierp een cijferschijf, bestaand uit twee op elkaar liggende schijven, met op de buitenste schijf de letters in alfabetische volgorde en op de binnenste schijf de letters in een willekeurige volgorde. Door aan het begin van een geheime boodschap aan te geven welke letter tegen een van te voren afgesproken letter moest worden gelegd, kon elke boodschap, of deel er van met een andere sleutel worden geschreven en gelezen. De cijfers op de buitenste ring stonden voor een bepaalde nomenclatuur, en deze cijfers werden nog eens versleuteld door gebruik van de schijf.

VIGENÈRE

Vigenère schreef in 1585 zijn boek ‘Traicté des chiffres’ waarin hij liet zien dat het mogelijk was met tekens die allemaal gelijk zijn, zoals punten, sterretjes of bladeren van bomen, een geheime boodschap te schrijven die er niet als geheimschrift uit zag. Het principe van zijn methode was de ordening van 5 vlakken in een vakje.