Geheimschrift door H. Kost, Kolonel G.S.

Geheimschrift is schrift, dat zijn ontstaan en zijn toepassing heeft te danken aan de wenselijkheid of de noodzakelijkheid mededelingen te kunnen doen, die alleen verstaanbaar zijn voor een bijzondere daartoe in aanmerking komende kring van personen.

Naar hun wezen kunnen de verschillende soorten van geheimschrift worden gerangschikt in twee grote groepen. De eerste groep bevat het geheimschrift in engere zin, het eigenlijke geheimschrift, waaronder men verstaat het gebruik van zichtbare of zichtbaar te maken schriftteekens, van welke aard dan ook, waarvan de beteekenis of zin niet voor iedereen verstaanbaar is of verstaanbaar geacht wordt.

De tweede groep omvat de onzichtbare of latente schriften, waarbij de door chemische reacties weder zichtbaar te maken teekens òf onmiddellijk algemeen verstaanbaar zijn òf wel op zich zelf weder eigenlijk geheimschrift vormen. Beide groepen van geheimschrift hebben in haar ontwikkeling gelijken tred gehouden met de vorderingen der aan die groepen ten grondslag liggende wetenschappen en hebben het aanzijn geschonken aan een nieuwe tak van wetenschap, de cryptografie.

Verstond men vroeger onder cryptografie slechts de kunst van geheimschrift te schrijven, volgens de huidige stand dezer materie is het juister het begrip „cryptografie" uit te breiden tot die tak van wetenschap, die tot voorwerp zijner studie rekent niet alleen de verschillende methoden om een oorspronkelijke of „klare" tekst in geheimschrift om te zetten (te chiffreeren of versleutelen), doch ook de middelen om dergelijke in geheimschrift gestelde teksten (cryptogrammen, cryptotekxten) in klare taal terug te zetten door langs zgn. cryptoanalytische weg de sleutel ervan te ontdekken. Deze cryptoanalytische wijze, waarop door derden geheimschrift weder in klaar schrift wordt teruggezet, wordt ter onderscheiding van het ontcijferen (dechiffreren) door bevoegden met behulp van de hun toevertrouwde sleutel, in de moderne cryptografische literatuur ontsluiering genoemd.

Indien het eigenlijk geheimschrift onmiddellijk als zodanig is te herkennen, spreekt men van openlijk geheimschrift ter onderscheiding van verborgen geheimschrift, waarbij het de bedoeling der correspondenten is hunne mededeelingen uiterlijk als onschuldig en onopvallend voor te stellen.

Alle cryptografische systemen, zowel openlijk als verborgen geheimschrift, van de eenvoudigste tot de ingewikkeldste, kunnen worden ondergebracht in twee grote groepen en wel op grond van de daaraan ten grondslag liggende cryptografische beginselen.

De eerste groep omvat de vervangingssystemen.

Hierbij worden de elementen van de klare tekst als: letters, lettergroepen, cijfers, cijfergroepen, woorden dan wel groepen van woorden vervangen door cryptoëlementen, in de regel geheel verschillend van het klare element, doch waarbij de opeenvolging der crypto-elementen in de cryptotekst gelijk blijft aan de oorspronkelijke volgorde der betrokken klare elementen in de klare tekst.

De tweede groep omvat de verplaatsingssystemen: dit zijn die systemen, waarbij de klare elementen ook in de cryptotekst hun oorspronkelijke voorstelling behouden, doch waarbij hun oorspronkelijke opeenvolging is gewijzigd.

Beide systemen van vervanging en van verplaatsing kunnen gelijktijdig in eenzelfde cryptogram worden toegepast (bij de gecombineerde vervangings- en verplaatsingssystemen).

Naast deze onderscheiding maken verschillende cryptografische schrijvers nog een onderscheiding in cijferschrift enerzijds, codes anderzijds. Onder cijferschrift vat men dan samen al die geheimschriften, waarbij men een cryptografische bewerking toepast op gewoonlijk de enkele letters, soms op tweeletter-groepen, bij uitzondering op 3- of meer-lettergroepen, waarin de klare tekst kan worden verdeeld, deze klare elementen daarbij vrijlatende in betekenis, in waarde dan wel in volgorde met behulp van een overeengekomen formule, schema, sleutel enz.

Onder code verstaat men dan een meer of min uitgebreide lijst van cijfers, letters, lettergroepen, woorden of zinnen, die kunnen worden vervangen door een codegroep (coderen) bestaande uit letters, cijfers of tekens. In hun eenvoudigste vorm naderen cijferschrift en code elkaar.

Afhankelijk van het daaraan ten grondslag gelegde cryptografische beginsel kunnen de vervangingssystemen weder onderverdeeld worden in twee groepen, te weten:

a. vervangingssystemen met enkelvoudige sleutel, dat zijn die systemen, waarbij een cryptoteken, dat ter vervanging van een klaar teken dient, steeds dezelfde betekenis heeft volgens een enkele van de voren overeengekomen sleutel, hetzij dat deze sleutel aangeeft de vervanging van letters, van cijfers, van letter- of cijfergroepen, van woorden of zinnen;

b. vervangingssystemen met dubbelen sleutel, dat zijn die systemen, waarbij de klare betekenis van een cryptoteken niet steeds dezelfde is, doch afhankelijk is van een door middel van een tweede sleutel vastgestelde plaats in het cryptogram.

De eenvoudigste vorm van een vervangingssysteem met enkelvoudigen sleutel is de zgn. eenvoudige vervanging met enkelvoudige cryptovoorstelling,

waarbij elke klare letter door eenzelfde cryptoteken wordt vervangen, onverschillig of dit teken is een letter, een combinatie van letters, een cijfer een combinatie van cijfers, een teken of combinatie van tekens.

Hiervan is weder het eenvoudigste voorbeeld het stelsel, dat zo niet uitgedacht dan toch gebezigd is door Julius Caesar en naar hem Julius Caesar-systeem wordt genoemd. Men vervangt daarbij de letters van het klare, normale alphabet met behulp van een zgn. normaal, verschoven vervangingstabel of -schema als hieronder in fig. 1 aangegeven.

Klaar alphabet : A B C D ..... U V W X Y Z

Crypto-alphabet : D E F G ..... X Y Z A B C

fig. 1. Vervangingstabel.

Enkele schrijvers vatten onder de benaming Julius Caesar- of Caesariaanse systemen niet alleen het bovengenoemde stelsel doch ook, indien voor de vervanging niet gebruik wordt gemaakt van verschoven normale alphabetten; ter onderscheiding noemt men het stelsel in fig. 1 het echte Julius Caesar-systeem. Men kan bij de vervanging als crypto-alphabet ook aannemen een geheel onregelmatig alphabet (fig. 2, regel a) dan wel een door middel van een sleutelwoord onregelmatig gemaakt alphabet (fig. 2, regel b). De onregelmatigheid van een crypto-alphabet kan ook op andere wijze met behulp van een sleutelwoord worden verkregen (fig. 3).

Klaar alphabet : 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 ..... C X H I Z K L Y P S A J D M F N T B O U G Q W E R V crypto-alph.

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

fig. 2. Vervangingstabel.

R O T E D A M
6 5 7 3 2 1 4

Men schrijft het sleutelwoord, hier ROTTERDAM, op een regel met weglating van de sleutelletters, die in het sleutelwoord herhaald worden.

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

De overblijvende letters van het alphabet schrijft men in haar alphabetische volgorde in regels onder de zgn. sleutelletters, die genummerd zijn volgens haar alphabetische volgorde en aldus een sleutel getal leveren, nl.: 6 5 7 3 2 1 4.

De letterkolommen, afgelezen elk van boven naar beneden in haar numerieke volgorde 1, 2, 3, 4, 5, 6 en 7 geven het crypto-alphabet als hieronder aangegeven:

klaar alph. A B C D E F G H I J K L M

crypto-alph. A I S D H Q Z E G P Y M J

fig. 3.

Geven de bovenstaande vervangingstabellen voorbeelden van een vervanging van elke klare letter door een enkele cryptoletter, soms ontmoet men vervangingsschema's als in fig. 4, waarbij elke klare letter wordt vervangen door 2 cijfers of

	1	2	3	4	5
6	R	O	T	E	D
7	A	M	B	C	F
8	G	H	I	J	K
9	L	N	P	S	U
Ø	V	W	X	Y	Z

In een vierkant van 5 bij 6 worden de 25 letters van het alphabet (met weglating bijv. van de letter Q, die in de klare tekst eventueel wordt vervangen door K of W) ingeschreven met behulp van het sleutelwoord, hier ROTTERDAM. Elke klare letter kan worden weergegeven in ons fijnmw door een getal van twee cijfers, waarvan bijv. het eerste cijfer de regel en het tweede cijfer de kolom van de betrokken letter aangeeft, zo bijv. klaar R: crypto 61; klaar O: crypto 62 enz. evenzo zou men kolom en regel kunnen benoemen in plaats van met een cijfer, met een letter waardoor elke klare letter vercijferd wordt tot een cryptobigram.

fig. 4.

Worden letters of cijfers als cryptotekens geberigd, dan wordt gewoonlijk de cryptotekst, van links naar rechts gelezen, in groepen van 5 letters respectievelijk cijfers afgedeeld, waarbij de overblijvende groep eventueel met niets-betekenende cryptotekens (nieten of nonvaleurs) tot een volledige groep van 5 wordt aangevuld. Behalve dat men door een dergelijke indeling in groepen van 5 tekens het cryptogram pas klaar maakt voor telegrafische verzending, wordt de ontcijfering enigszins bemoeilijkt door het wegvallen van de voorspronkelijke woord-afscheidingen. Bij de ontcijfering van de hiervoren genoemde eenvoudigste vervangingssystemen met enkelvoudige cryptoweergave maakt men gebruik van de frequentie van de enkele letters, van die der bigrammen, soms van die der meest voorkomende trigrammen in de betrokken taal, welke frequentie-statistiek te vinden is neergelegd in frequentie-tabellen.
Naast deze analytische methode van ontcijfering, waarbij de betekenis der cryptotekens stuk voor stuk bepaald wordt in verband met hun frequentie als op zichzelf staand teken en als onderdeel van veel of weinig voorkomende crypto-bigrammen of -trigrammen, onderscheiden sommige schrijvers een ontcijfering met behulp van het waarschijnlijke woord.
Meermalen toch heeft men omtrent den waarschijnlijken inhoud van het cryptogram zulke vaste aanwijzingen, dat men het voorkomen van bepaalde woorden in de klare tekst als zeer waarschijnlijk mag aannemen.
In diplomatieke cryptogrammen is bijv. „regering" een dergelijk waarschijnlijk woord, in militaire cryptogrammen uit een actief gevechtsfront een woord als „vijandelijk", de betrokken „plaatsnamen" enz.
Gelukt het de vercijfering van een dergelijk waarschijnlijk woord in de cryptotekst te herkennen in verband met de karakteristieke plaats, frequentie, herhaling enz. van enkele letters daarin, dan kan de ontcijfering aanzienlijk worden bespoedigd; bij korte cryptogrammen is deze wijze van ontcijfering soms de enige

Het behoeft geen betoog, dat met de meerdere kennis omtrent de ontcijfering dezer systemen gelijkelijk ook een zekere ontwikkeling viel te onderkennen ten aanzien van de middelen om de ontcijfering te bemoeilijken, middelen, die in algemene zin beogen het maken van een juiste frequentie-statistiek der cryptoteksens te verhinderen.

De meest toegepaste onder deze middelen zijn:

a. het geven van een meervoudige crypto-voorstelling aan de letters met de grootste frequentie of wel aan alle letters;

b. het gebruik van nieten of nonvaleurs;

c. door bijv. bij gebruik van letter- of cijfergroepen ter verciffering van klare letters, deze groepen niet alle uit hetzelfde aantal letters respectievelijk cijfers te doen bestaan.

Als gevolg van deze verbeteringen ontstonden langzamerhand uit deze vervangingssystemen met enkelvoudige sleutel de onderscheiden stelsels, die samen de klasse vormen van de vervangingssystemen met dubbele sleutel.

De eenvoudigste vorm hiervan is het hieronder in fig. 5 beschreven Vigenère-systeem, dat ook bekend staat onder de naam van Tritheimse tabel, chiffre carré e.a.

26 crypto-alphabetten.

klaar alphabet

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	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
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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

klaar: HEDENVERTROKKEN.
sleutel: CYFERCYFERCYFER
crypto: JCIIEXCWXIQIPIE

fig. 5. Tabel van Vigenère.

Wil men met behulp van de hierboven gegeven tabel van Vigenère een klaar bericht verciferen met het woord C Y F E R als sleutel, dan wordt deze sleutel onder de klare tekst geschreven en over de gehele tekst herhaald. Elke klare letter wordt verciferd met de daaronder geschreven sleutelletter, de eerste klare letter H met de eerste sleutelletter C tot cryptoletter J, de tweede klare letter E met de tweede sleutelletter Y tot cryptoletter C, en zo vervolgens. De betrokken cryptoletter, vindt men op het snijpunt van kolom en van regel binnen het getrokken vierkant, waarbij de kolommen zijn benoemd met de erboven geschreven letter van het klare alphabet en de regels met de links en naast vermelde letter van het sleutelalphabet.

Van het hierboven beschreven systeem van de Vigenère treft men onder verschillende benamingen als: de Beaufort-systeem, systeem-Gronsfeld enz. varianten aan. Allereerst kan men het normale klare alphabet van fig. 5 vervangen door een onregelmatig alphabet, al of niet door een sleutelwoord onregelmatig gemaakt; evenzo kunnen de 26 verschoven normale cryptoalphabetten binnen het vierkant vervangen worden door even zovele verschoven onregelmatige alphabetten of wel door 26 geheel van elkaar onafhankelijke alphabetten, mits in elke kolom en op elke regel een cryptoletter slechts eenmaal voorkomt.

Wat de vorm betreft, treft men in plaats van een vierkante tabelvorm hetzelfde cryptografische stelsel aan in de zgn. Vigenère-schijven of Vigenère-klok, de oudste voorlopers van de moderne chiffreermachines.

Bij de lineaal van St. Cyr (aldus in Franse werken geheten naar de gelijknamige Franse militaire school), die ongeveer een gelijksoortige constructie vertoont als een rekenlineaal, is op een der verschuifbare latjes het enkele klare alphabet aangebracht, op het andere latje het dubbele cryptoalphabet.

Een der klare letters dan wel een der cryptoletters dient daarbij als aanwijzer van de sleutelletters, die men afleest op het cryptoalphabet respectievelijk klare alphabet. In plaats van 2 verschuifbare latjes kan men het systeem zien in de vorm van 2 om hetzelfde middelpunt draaibare schijven (Vigenère-schijven).

Kunnen de Vigenère-systemen zelfs in hun primitiefste vorm zich aanvankelijk verheugen in een hoge mate van onontcijferbaarheid, zo zelfs, dat het in de literatuur dier dagen „chiffre indéchiffrable" of „chiffre par excellence" werd genoemd, het bleek, zij het ook lange tijd na hun verschijning, dat ontcijfering zeer wel mogelijk was, indien het slechts gelukte de zgn. periodiciteit van het gebezigde systeem (d.i. het aantal sleutelletters) te onderkennen en indien het met eenzelfde sleutel vercijferde cryptomateriaal uitgebreid genoeg was om de gebezigde cryptoalphabetten met behulp van de frequentie der cryptoletters te reconstrueren.

Bij een cryptografische analyse van het stelsel blijft toch, dat identieke

klare groepen (als EN in het voorbeeld van fig. 5), die op een onderlinge afstand t (interval) van elkaar in de klare tekst staan gelijk aan de sleutellengte (periodiciteit) of een veelvoud daarvan, tot identieke cryptogroepen worden versleuteld (in fig. 5 de cryptogroepen IE).

Uit deze omstandigheden kon omgekeerd weder afgeleid worden, dat de periodiciteit bij genoegzaam cryptomateriaal als factor met de grootste frequentie naar voren zou treden onder de factoren, waarin de intervallen tussen identieke cryptogroepen konden worden ontbonden.

Is de periodiciteit gevonden, dan levert het cryptogram, in regels onder elkaar geschreven ter lengte van zijn periodiciteit, even zovele kolommen cryptoletters, die elk voor zich versleuteld zijn volgens eenzelfde cryptoalphabet.

De ontsluiering der cryptoletters heeft dan plaats op dezelfde wijze als hiervoren ten aanzien van de vervangingssystemen met enkelvoudige cryptovoorstelling werd uiteengezet.

Zekerheid tegen ontsluiering kunnen de Vigenère-systemen eerst geven, indien, met gebruikmaking van onregelmatige klare en cryptoalphabetten, de periodiciteit zo groot is, dat men nimmer genoegzaam cryptomateriaal zou kunnen verzamelen, waaruit de periodiciteit zou zijn af te leiden, dan wel indien er van periodiciteit in het geheel geen sprake is (aperiodische systemen).

Men zou dit o.m. kunnen verkrijgen door als sleutel de tekst van een boek te nemen, nadat bovendien voor elk cryptogram een afzonderlijk beginpunt van de sleutel kon worden genomen.

Een andere methode vormen de zgn. autoclave Vigenère systemen, waarbij men bijv. de klare tekst als sleutel bezigt, nadat men de eerste of de eerste paar letters daarvan heeft versleuteld met tevoren overeengekomen sleutelletter(s). Werden hiervoren onder de vervangingssystemen met enkelvoudige sleutel slechts vermeld systemen, waarbij de klare letters stuk voor stuk versleuteld werden, tot dezelfde klasse zijn ook te rekenen die systemen, waarbij de klare letters in paren versleuteld worden. Men kan hiervoor gebruik maken van een codeertabel, waarop de 26 mogelijke klare bigrammen alphabetisch zijn gerangschikt met vermelding daarnaast van de betrokken cryptobigrammen; het systeem vereist ook een decodeertabel, waarop de cryptobigrammen alphabetisch zijn gerangschikt met vermelding er naast van de betrokken klare bigrammen. Een eenvoudiger vorm van deze bigramsgewijze vervanging is bekend onder de naam van cijfervierkant of, in de Engelse literatuur, van Playfair-cipher.

ROTED
AMBCF
GHIJK
LNPQU

Men maakt hierbij gebruik van een vierkant van 5 bij 5 vakjes ter inschrijving van 25 letters van het alphabet (zonder de letter Q bijv.), waarbij de volgorde van inschrijving wordt bepaald door een sleutelwoord i.c. ROTTERDAM. De versleuteling der klare bigrammen geschiedt als volgt:

de letters van het klare bigram kunnen, afgelezen in het cijfervierkant, ten opzichte van elkaar de volgende plaatsen innemen:

a. zij liggen op dezelfde rij;
b. zij liggen in dezelfde kolom;
c. zij liggen op de diagonaal van een vierkant of rechthoek;
d. zij zijn dezelfde letters (verdubbeling).

Afhankelijk van haar plaatsen verciffert men de letters van een klaar bigram stuk voor stuk in geval:

a. door de letter onmiddellijk rechts ernaast;
b. door de letter onmiddellijk eronder;
c. door de letter gelegen op de hoekpunten van de andere diagonaal, gelegen op dezelfde rij;
d. door de letter onmiddellijk rechts ernaast gelegen.

Bevindt zich rechts naast of onmiddellijk eronder geen letter meer, dan neemt men als verciffering de meest linkse letter uit die rij, respectievelijk de bovenste letter uit die kolom. Zo wordt, nadat de klare tekst van links naar rechts in bigrammen is afgedeeld, daarin bijv. in geval:

a. TD verciffert tot ER ER tot DO OE tot TD
b. HN " " NW NW " WO NM " WH
c. MS " " CN NC " SM
d. HH " " II KK " GG

fig. 6 Cijfervierkant.

Bij de ontcijfering van een dergelijk cijfervierkant gaat men uit van de frequentie der cryptobigrammen, waarbij men tevens voor de reconstructie van het gebezigde cijfervierkant gebruik maakt van de wetenschap, dat de cryptoletters, gelegen op dezelfde rij en in de kolom van de letter met de grootste klare frequentie (in het Nederlands de E), zullen behoren tot die met de hoogste cryptofrequentie (in ons cijfervierkant de cryptoletters ROTEDCJSY).

Is dus de ontcijfering van het cijfervierkant in de aangegeven vorm wel mogelijk te achten, door combinatie van het systeem met een eenvoudig systeem van verplaatsing, zodat het moeilijk zo niet onmogelijk wordt de bij elkaar behorende letters van een crypto-bigram te herkennen, verhoogt men aanzienlijk zijn waarde.

Een cryptografisch beginsel geheel verschillend van de hiervoren behandelde groep van vervangingssystemen staat die der verplaatsingssystemen, waarbij de chiffreur als het ware een hutspot maakt van de letters van de klare tekst volgens een van te voren overeengekomen regel (verplaatsingssleutel), zonder enige verandering te brengen in de oorspronkelijke klare tekens. Op welke wijze de verplaatsing ook moge geschieden, deze kan steeds worden teruggebracht

Zulk een numerieke verplaatsingssleutel is een formule, waarin, afhankelijk van haar periodiciteit (deze bijv. stellende op n) alle getallen tussen 1 en n in een bepaalde volgorde voorkomen, in welke volgorde de overeenkomstige letters van de klare tekst dienen te worden verplaatst.

ANNA	klaar:	VERTREKONMIDDELLYK.
1342		1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18
VERT		
REKO	crypto:	VRNDYTODLEEMEKRKIL
NMID		
DELL	sleutel:	1 5 9 13 17 4 8 12 16 2 6 10 14 18 3 7 11 15
YK		

Zo kan het cryptogram van deze figuur tot uiteindelijke numerieke sleutel bij ontsluiering geven de formule als aangegeven onder de cryptoletters. Bij nadere crypto-analytische uitwerking blijkt deze formule met een periodiciteit van 18 vereenvoudigd te kunnen worden tot een primaire verplaatsingssleutel. (in getalsvorm uitgedrukt: 1342), indien men vindt, dat de verplaatsing even goed zou kunnen worden verkregen door onder de primaire woordsleutel bijv. ANNA de klare tekst te schrijven als hierboven aangegeven en daarna de letters kolomsgewijze af te schrijven, de kolommen van boven naar beneden in de volgorde als aangegeven door het er boven vermelde cijfer van de primaire sleutel.

fig. 7. Verplaatsingssystemen.

Meestal wordt dan ook verplaatsing verkregen door de klare letters in te schrijven in een meer of minder regelmatige geometrische figuur volgens een bepaald te voren overeengekomen regel van inschrijving, terwijl de versleuteling ontstaat door de aldus ingeschreven letters weder af te lezen volgens een andere, eveneens te voren overeengekomen, regel. Wordt een reeds eenmaal verplaatste tekst voor de tweede maal met behulp van dezelfde of van een andere sleutel verplaatst, dan spreekt men van dubbele verplaatsingssystemen.

Een klassieke groep van verplaatsingssystemen vormen de zgn. rooster- of grille-systemen, waarbij geperforeerde kartonnen figuren (roosters of grilles) de wijze van verplaatsing regelen. Voor de beschrijving en toepassing dezer weinig in gebruik meer zijnde stelsels moge worden verwezen naar de bestaande literatuur.

Vergeleken bij de vervangingssystemen hebben de verplaatsingssystemen het voordeel van eenvoud en van snelheid van versleuteling en ontcijfering. Zij hebben echter het nadeel van grote ontsluierbaarheid, indien het toeval den tegenstander in het bezit mocht brengen van 2 of meer cryptogrammen, die even lang zijn en verplaatst zijn met dezelfde sleutel, zelfs voor het geval men te doen heeft met een der veiligste onder deze systemen, te weten de dubbele vervanging.

In algemene zin berust de ontcijfering der verplaatsingssystemen hierop, dat men tracht zgn. compromitterende bigrammen en trigrammen te reconstrueren, uitgaande van de, in een bepaalde taal bestaande, compromitterende letters en letterverbindingen (bijv. in het Nederlands en Duits de CH, SCH enz., in het Frans de QU gevolgd door een klinker, enz.), dikwijls ook uitgaande van een in een bepaald cryptogram verondersteld waarschijnlijk woord, waarna men tracht op grond van deze letterverbindingen de verplaatsingsformule door berekening als anderszins te vinden.

Gecombineerd met een vervanging kan een verplaatsing, beide soorten van versleuteling zelf in een zeer eenvoudige vorm, aan moeilijk ontcijferbare, zij het ook meer of min tijdrovende, systemen het aanschijn schenken.

Reeds bij de oudste vervangingssystemen viel een zekere behoefte te onderkennen aan lijsten of nomenclaturen, waardoor het mogelijk werd veel voorkomende letterverbindingen en woorden, liefst verkort, weer te geven. Deze nomenclaturen zijn als de oudste voorlopers te beschouwen van de hedendaagse codes of codeboeken, waarmede het mogelijk is woorden, zinnen, getallen enz. uit de klare tekst (klare groepen) door codegroepen, bij voorkeur zo gecondenseerd mogelijk, te vervangen; deze codegroepen kunnen zowel uit letters als uit cijfers bestaan.

In verband met de geldende telegramtarieven alsmede ter vermindering van het gevaar van schrijffoutige telegramverminkingen, bestond en bestaat er nog een zekere voorkeur, althans voor wat betreft de handelscodes, voor het gebruik van codegroepen uit letters samengesteld. Naast deze codegroepen in letters vermelden de meeste handelscodes tevens codegroepen uit cijfers bestaande, waardoor het mogelijk is met behulp van code-condensors kortere lettercodegroepen te vormen, ten einde daarmede de condensatiemogelijkheid van de code te verhogen.

Beoogen de handelscodes in hoofdzaak besparing van telegramkosten, in het diplomatieke en militaire berichtenverkeer beoogt het gebruik van codes in de eerste plaats geheimhouding.

Tegenover de niet geheime, in de handel verkrijgbare, handelscodes onderscheidt men uit een cryptografisch oogpunt de geheime militaire en regeringscodes. Een andere onderscheiding is nog ten aanzien van de laatste groep codes te maken, nl. die in alphabetische codes, waarbij de klare groepen in alphabetische numerieke of begripsmatige volgorde staan met daarnaast de codegroepen eveneens in numerieke of alphabetische volgorde, anderzijds de niet-alphabetische of zgn. loterij-codes, waarbij als het ware door het lot willekeurig een codegroep aan een klare groep is toebedeeld.

In tegenstelling met de alphabetische codes, die uit een enkel

codeer- levens decodeer-deel bestaan, bestaan de niet alphabetische codes uit een afzonderlijk codeer- naast een decodeer-deel, waarin de klare groepen respectievelijk de codegroepen in alphabetisch- numerieke volgorde zijn opgenomen. Een tussenvorm zijn de codes, die grotendeels alphabetisch om cryptografische redenen compromitterende groepen als zgn. zaailingen los van enige alphabetisch-numerieke volgorde bevatten.

Evenals bij de letter- en bigram-vervangingssystemen berust de ontcijfering van code-cryptogrammen op de frequentie, thans niet van letters of bigrammen, doch van woorden, leestekens, voorzetsels enz. Uit een oogpunt van cryptografische zekerheid staan de alphabetische codes verre ten achter bij de niet-alphabetische, doordat de ontcijferde groepen uit alphabetische codes met haar numerieck-alphabetische plaatsen in de code levens de structuur van de gehele code en daarmede andere codegroepen compromitteren. Een soortgelijke evolutie als bij de literale vervangingssystemen valt ook bij de geheime codes op te merken, nl. de noodzakelijkheid de ontcijfering te verzwaren of te beletten door het verwisselen of het geheel te niet doen gaan van de frequentie der codegroepen.

Deze noodzakelijkheid riep de verschillende methodes van herver-cijfering, ~~op zijn hoogst met een zeer primitieve, verwacht mag worden dat ook in deze systemen van hervercijfering grote verbeteringen zullen worden aangebracht uit cryptografisch zowel als uit practisch oogpunt. In deze ontwikkeling zullen, naar mede verwacht mag worden chiffreer-~~ in het leven, waarbij de oorspronkelijke cijfers of letters der codegroepen een tweede bewerking ondergingen volgens een der hiervoren genoemde systemen van verplaatsing, van vervanging of beide tegelijkertijd toegepast; de zgn. methode van het optelgetal, waarbij bij gebruik van cijfercodes bij de cijfers van de crypto-tekst op bijzondere wijze een periodisch optelgetal wordt opgeteld, vindt daarbij veel toepassing.

Trof men vóór en gedurende de 1e wereldoorlog nog het gebruik aan van alphabetische zowel als niet-alphabetische codes zonder enige hervercijfering, op zijn hoogst met een zeer primitieve, verwacht mag worden dat ook in deze systemen van hervercijfering grote verbeteringen zullen worden aangebracht uit cryptografisch zowel als uit practisch oogpunt. In deze ontwikkeling zullen naar mede verwacht mag worden chiffreer-machines een belangrijke rol spelen.

Reeds thans zijn dergelijke chiffreermachines in de handel verkrijgbaar, ten einde niet alleen te voorzien aan de behoefte aan snel en feilloos ver-cijferingswerk doch daarnevens aan deze snelheid te kunnen paren grote mate van cryptografische veiligheid.

In verband met het korte bestek van dit artikel en de betrekkelijke jeugd der moderne chiffreermachines moge worden volstaan met slechts te vermelden, dat voor zover thans reeds bekend, de bestaande chiffreermachines, al of niet met gebruikmaking van electriciteit, alle berusten op het Vigenère - beginsel. Dank zij de huidige techniek is het thans reeds de uitvinders gelukt de periodiciteit van het stelsel zeer hoog op te voeren niet alleen, doch de mogelijkheid te scheppen van een afzonderlijke sleutel voor elk cryptogram door toepassing van zeer eenvoudige handgrepen.

Bij mechanisatie van het chiffreerwerk dient als nadeel rekening te worden gehouden met de mogelijkheid van mechanische weigeringen met alle daaraan verbonden kosten voor reserve - machines en - onderdelen.

Historisch overzicht

Al bestaan er vermoedens voor een veel oudere oorsprong, reeds in het boek Jeremia (25:26) vindt men sporen van een geheimschrift, waarbij in het te verciferen woord de 1ste, 2de enz. letter van het gebruikelijke alphabet door de laatste, een-na-laatste enz. letter daarvan vervangen worden.
Het woord BABEL (de letters B, B, L, in haar normale volgorde de 2de en 12de letter van het Hebreeuwse alphabet) werd weergegeven met het woord SESACH (S, S, CH, de 2de en 12de letter, gerekend van het eind).

Evenzo heeft men in Boedjoedse amuletten een geheimschrift ontdekt, waarbij de letters van het alphabet door de in rangorde naastvolgende vervangen worden, een geheimschrift dat zich, wat zijn cryptografisch beginsel betreft, tot op de huidige dag bij het ook in meerdere vormen, heeft kunnen handhaven.

De Lacedaemoniers kenden een geheimschrift, scytale genoemd naar de gelijknamige staf, waarvan het cryptografisch beginsel thans nog is terug te vinden in de verplaatsingssystemen.

Ook de oude Grieken maakten reeds gebruik van een geheimschrift, waarbij de letters van het alphabet op de een of andere wijze door getalteekens werden vervangen, een geheimschrift, dat uit het Oosten stammend, vooral voor het versluieren van handteekening tot in de XVIde eeuw zijn invloed deed gelden.

Omtrent het gebruik van geheimschrift bij de Romeinen kan men o.m. bij Suetonius, in zijn levensbeschrijving der eerste Romeinse keizers, de sleutel vinden van de door Julius Caesar en Augustus gebezigde geheimschriften. Bezigde Caesar een verciffering, waarbij het cryptо-alphabet ten opzichte van het klare normale alphabet 3 plaatsen was verschoven, zodat een klare letter D werd vervangen door de cryptо-letter G, bij het door keizer Augustinus gebruikte

systeem bedroeg deze verschuiving slechts één plaats.

Gedurende de Middeleeuwen was het vooral aan de Pauselijke Curie en aan de kleine Italiaanse hoven, waar het gebruik en de beoefening van het geheimschrift in hoog aanzien stonden, dat in deze tijd in de aanvang meest verbreide geheimschrift vertoont in zijn cryptografische beginselen onmiskenbaar zijn afstamming uit de Romeinse keizertijd, met dit verschil nochthans dat aanvankelijk slechts de klinkers in de klare tekst werden vervangen door de in rangorde naastvolgende letters, terwijl de medeklinkers onveranderd behouden bleven.

Daarnaast bevatten vele Middeleeuwse handschriften een geheimschrift, waarbij de klinkers werden vervangen door een voor elke klinker variërend aantal punten of ander overeengekomen teken. Eerst tegen het einde der Middeleeuwen, doch in het bijzonder in de XVI de eeuw, ontwikkelden zich uit en naast deze vocaal- of klinker-systemen, waarbij alleen de klinkers versijferd werden, die systemen, waarbij de versijfering ook werd toegepast op de medeklinkers.

Gelijktijdig met deze letter-vervangingssystemen kwamen de woord-vervangingssystemen in zwang, zgn. nomenclaturen, met behulp waarvan persoonsnamen, plaatsnamen en andere woorden door minder compromitterende konden worden vervangen (de oudste vorm der moderne codes). Uit het eind der Middeleeuwen stammen de oudste verhandelingen over cryptografie van de hand van twee pauselijke geheimsecretarissen, G. de Lavinde (liber siffarum, Rome 1375-1383) en L.B. Alberti (Trattati in cifra).

Lavinde was de eerste, die de systemen van letter-vervanging beschreef en hen aanbeval voor gelijktijdige toepassing ~~xxx~~ met een nomenclatuur.

Aan Alberti (gestorven 1472) wordt toegeschreven de uitvinding van de chiffreer-quadrant, in beginsel de voorloper der hedendaagse chiffreermachines. Zijn (o.m. in het Staatsarchief te Venetië) geschrift over geheimschrift, moet volgens Prof. A. Meister (Die Geheimschrift im Dienste der Päpstlichen Kurie) als de oudste theoretische verhandeling worden beschouwd over het vervaardigen en het verbeteren der toenmalige systemen, ouder zelfs dan het in 1474 te Milaan voleindigde cijfertractaat van Sicco Simonetta, dat echter nog als de oudste practische verhandeling beschouwd moet worden over het ontcijferen van de toenmalige systemen.

De Renaissance toont een verdere ontwikkeling der cryptografische systemen. De letters van het klare alphabet worden niet meer door een enkel teken doch door groepen van 2 of 3 tekens, letters of cijfers, vervangen, waarbij Griekse en Hebreeuwse letters als crypto-letters langzamerhand in onbruik geraken als gevolg van de grotere kennis in deze talen.

Tekerheid tegen ontcijfering trachtte men in deze tijd te verkrijgen door zgn. meervoudige crypto-voorstelling der klare letters, door het uitbreiden van het aantal nieten alsmede door invoering van cryptotekens voor de versijfering van de

meest voorkomende letterverdubbelingen, letterspreuken en woorden.

Het is evenzeer in de tijd der Renaissance, dat belangrijke cryptografische vindingen werden gedaan als het rooster-systeem, nl. door de 2de Italiaanse wiskundige J. Cardan en het systeem der vervanging met dubbele sleutel door de natuurkundige J.B. Porta en de Franse diplomaat de Vigenère.

De gedurende de Middeleeuwen geboren Italiaanse cryptografische school vond haar voortzetting in de XVde eeuw in de voor de republiek Venetië door zijn cryptografische werkzaamheden onschatbaren chiffreur Giovanni Soro. (Liber zifrarum, 1539), in de aan de Pauselijke Curie verbonden Jacobus Silvester (Opus novum, praefectis arcium, anno 1526), diens opvolger G.B. Bellaso (Il vero modo di scrivere in cifra, anno, 1553, 1557 en 1564).

Intussen begonnen ook de geschriften van den abt Johan Trithemius of Tritheim, van zijn waren naam Johann von Heydenberg, te weten Polygraphiae, libri sex (1518), Clavis Steganographiae (1498-1499) hun invloed op de Italiaanse beoefenaars der cryptografie te doen gelden, zij het ook niet onmiddellijk na het verschijnen dezer geschriften.

Ongetwijfeld moeten deze geschriften die zijner tijdgenoten en daarna beïnvloed hebben, o.m. Blaise de Vigenère (1525-1596, Traité des chiffres ou secrète manières de l'écrire) en J.B. Porta (1540-1645, De furtivis literarum notis; De Occultis litterarum notis).

Het naar Vigenère genoemde systeem, door hem zelf „chiffre carré" of „chiffre indéchiffrable" genoemd, is een verbetering van de naar Porta genoemde tabel, beide behorende tot de vervangingssystemen met dubbelen sleutel, door Duitse schrijvers eerder aan Tritheim toegeschreven.

Onder de regering van Hendrik IV (1589-1610) vonden de de Vigenère en Porta-systemen grote toepassing, in welke tijd cryptologen als F. Viète (1540-1603) in Frankrijk, Mattee Argenti aan de Pauselijke Curie door hun ontsluieringen en cryptografische kennis grote roep verwierven.

De beoefening der cryptografie zowel in practische als theoretische zin beleefde in de XVIIde eeuw haar hoogtepunt. Uit deze cryptografische bloeitijd stammen de geschriften van Sir Francis Bacon (Advancement of learning, in het Latijn uitgegeven als De Dignitate et augmentis scientiarum), wiens naar hem genoemd versleutelingsstelsel en daarmede versleutelde geschriften het voorwerp zijn geweest en nog zijn van onderzoek voor hedendaagse cryptologen.

Evenzo vallen uit die tijd de werkzaamheden te vermelden van de cryptoloog in dienst van Richelieu Rossignol (1590-1673), de geschriften van den Duitser Kaledi, den Italiaan A.M. Cospi, in de 2de helft der XVIIde eeuw vooral de geschriften van Kircher (Polygraphia nova et universalis ex combinatoria arte detecta) en van Schott (Schola steganographiae in classes octo distributa, Magia Universalis naturae et artis).

Na deze bloei beleefde de cryptografie in de XVIII de eeuw een periode van betrekkelijke stilstand, al hebben ook verschillende schrijvers als Breithaupt, Conrad in Duitsland, Vlandel in Frankrijk, Davys in Engeland zich op dit gebied bewogen.

Ook de XIX de eeuw kenmerkt zich ondanks schrijvers als Klüber (Kryptographik), Rees (art. Cypher in the New Cyclopaedia), Vesin de Romanini (Traité d'obscurigraphie; la cryptographie dévoilée), F. W. Kasiski (Die Geheimschriften und die Dechiffrirkunst), meer door grondige studie van reeds bekende stelsels dan door nieuwe vindingen.

— · —

Nederlandse Taal, spelling 1947.

Statistiek over 1000 woorden.

Beginletters per woord:		Eindletters per woord:	
A	40	A	4
B	47	B	1
C	11	C	-
D	153	D	51
E	65	E	198
F	7	F	6
G	43	G	47
H	80	H	6
I	50	I	3
J	3	J	-
K	17	K	26
L	20	L	27
M	53	M	7
N	38	N	308
O	64	O	1
P	23	P	14
Q	-	Q	-
R	11	R	83
S	26	S	70
T	51	T	129
U	9	U	8
V	92	V	-
W	48	W	4
X	-	X	-
Y	-	Y	7
Z	49	Z	-
	1000		1000

Aantal letters per woord:

176	woorden van	2	letters.
235	" "	3	"
111	" "	4	"
66	" "	5	"
100	" "	6	"
67	" "	7	"
60	" "	8	"
54	" "	9	"
37	" "	10	"
44	" "	11	"
24	" "	12	"
7	" "	13	"
7	" "	14	"
12	" "	15	"
		en meer.	

1000 woorden totaal

Statistiek per 1000 letters.

(opgemaakt over 5000 letters)

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
64	15	13	63	198	10	33	25	54	1	24	43	28	108	65	13	1	60	38	65	20	25	15	1	13	17

Gerangschikt naar de frequentie:

E	N	O	T	A	D	R	I	L	S	G	H	V	K	M	U	Z	B	W	C	P	Y	F	J	Q	X
198	108	65	65	64	63	60	54	43	38	33	26	25	21	20	20	17	15	15	13	13	13	10	1	1	1

Nederlandse Taal, spelling 1947.

Bigrammen per 1000 letters.

(opgemaakt over 5000 letters)

EN	52	ST	8	NH	5
DE	33	VA	8	NT	5
ER	29	VE	8	NZ	5
EE	19	AL	7	RS	5
ND	19	BE	7	SE	5
AN	18	EI	7	TA	5
TE	18	LA	7	TD	5
GE	17	LE	7	TI	5
IN	16	NI	7	TO	5
EL	15	NV	7	UI	5
ET	15	VO	7	EG	4
AA	11	ZE	7	EH	4
IE	11	AT	6	EK	4
NG	11	DA	6	HO	4
HE	10	DI	6	HT	4
NE	10	IS	6	ID	4
OO	10	IT	6	IG	4
OR	10	NO	6	LD	4
RE	10	RD	6	LI	4
ME	9	WE	6	LL	4
ON	9	YK	6	NN	4
ED	8	AR	5	NS	4
ES	8	EM	5	OP	4
CH	8	EV	5	PR	4
KE	8	LY	5	RI	4
OE	8	NA	5	RO	4

Trigrammen per 1000 letters.

NDE	10	EEL	2
AND	8	EGE	2
EEN	7	ENA	2
END	7	ERE	2
DER	6	ERI	2
ING	6	EST	2
OOR	6	EVE	2
VAN	6	MET	2
DEN	5	NDS	2
ENV	5	NHE	2
GEN	5	NIN	2
EDE	4	NNE	2
CHT	3	NVA	2
ENH	3	NZE	2
ERS	3	STE	2
HET	3	TER	2
LAN	3	UIT	2
LYK	3	YKE	2
NGE	3	ZEN	2
TEN	3		
VER	3		
VOO	3		

Het cijfer 1 moet altijd worden onderstreept

Het cijfer 0 moet altijd worden doorgestreept

Klare tekst: Confidential. Karel Doorman heeft verbleven in Portsmouth

E L R V II 6 1 3 2 7 11 9 10 8 5 4
A N F B C
G H I K M V E R T R O K K 6 1 3 2 7 11 9 10 8 5 4
O P Q S T E N U I T P O R R L V V V W O B L U S
U W X Y Z R V V O L S I M K I P M L Q Q T F G V
B C G H I L V W B U K P L T B W M Q F M Z F R V
K M O P Q T S M O U T H C C R R P V Q Y V A G Y
S T U W X O N F I K A R E N K A T N P
Y Z E L R Q T G T W Q M F
V II A N F Q F V B M F Z R
L II O O R M A N
H E II E N R M S
V R P Q V G N A N
C R V Y A Y K T P

~~. . . . . A P V G L F C B N D~~

L I B R K V M M P T V P W R A S V V Y U G R G R K T C N V L

Q V N L F F A Q Q M Y B T Z V W Q F Q P

4 no. 11.
1 to 6

6 1 3 2 7 11 9 10 8 5 4

R L/ V V/ V W/ O B/ L U/ S

K/ I P/ M L/ Q Q/ T F/ G V/

T B/ W M/ Q F/ M Z/ F R/ V

C/ R R/ P V/ Q Y/ V A/ G Y/

N K/ A T/ N R/

R V V O L S I M

L V W B U K P L

V E R T R O K K

E N U I T P O R

Q T G T W Q M F

Q F V B M F Z R

T S M O U T H/C

O N F I K A R E

V R P Q V G N A

C R V Y A Y K T

L D O O R M A N N

H E D E N ~~R M S~~ P

E L R V D

A N F B C

G H I K M

O P Q S T

U W X Y Z

B C G H I

K M O P Q

S T U W X

Y Z E L R

V D A N F