Oude cryptografie: Caesarcijfer en Vigenèrecijfer

door Hugo Bosland

Samenvatting:
Er zijn vroeger verschillende cryptografiemanieren bedacht, zoals het Caesarcijfer en het Vigenèrecijfer. Bij beide methoden worden letters vervangen door een andere letter uit het alfabet, maar via een bepaalde sleutel.

Al eeuwenlang versturen mensen geheime berichten. Een bekende manier om geheimschrift te gebruiken is met het zogenoemde Caesarcijfer.

Caesarcijfer

Bij het Caesarcijfer wordt elke letter van het bericht vervangen door een letter die een bepaald aantal plaatsen verder in het alfabet staat. Als bijvoorbeeld als sleutel 'rotatie 4' wordt gebruikt, wordt elke 'a' vervangen door een 'e', elke 'b' door een 'f', enzovoorts. Wiskundig kan dit als volgt beschreven worden: Voor versleuteling: E_n (x) = (x+n) mod 26. Voor de ontsleuteling geldt: D_n (x) = (x-n) mod 26. Omdat er gewerkt wordt met modulo 26, zijn er maar 26 verschillende versleutelingsmogelijkheden, waarvan 1 (n=26 of n=0) geen versleuteling is, omdat hier het gecodeerde bericht gelijk is aan het origineel. Deze code is dus gemakkelijk te kraken, zeker met behulp van frequentieanalyse (bij lange teksten). Bij frequentieanalyse wordt gekeken naar hoe vaak een letter in een bepaalde taal voorkomt. In het Nederlands is bijvoorbeeld 19,06 % van de gebruikte letters een 'e'. Als in het geheimschrift de letter 'f' 19,06 % van alle tekens is, is het waarschijnlijk dat er een 'rotatie 1' is gebruikt.

Vigenèrecijfer

In de 16e eeuw is het Vigenèrecijfer bedacht. Bij deze methode wordt ook elke letter vervangen door een andere letter uit het alfabet, maar deze staat niet op een vaste afstand van de originele letter. De positieverandering is afhankelijk van een sleutelwoord. Stel dit is het woord 'kat'. Het eerste letter van het te coderen bericht wordt dan vervangen door een letter die tien plaatsen verder in het alfabet staat, omdat de letter 'k' de elfde letter is. De tweede letter van het te coderen bericht blijft gelijk, omdat hier de tweede letter van de sleutel 'kat' wordt gebruikt, een 'a'. Dit is de eerste letter van het alfabet, dus wordt de letter vervangen door een letter die nul plaatsen verder in het alfabet staat, dus de letter zelf. Bij de derde letter wordt als sleutel de 't' gebruikt, en bij de vierde weer de 'k'. Deze methode maakt dus gebruik van verschillende Caesarcijfers na elkaar en is daarom lastig te kraken. De letter 'e' kan bijvoorbeeld de ene keer vervangen worden door een 'c', en de volgende keer door een 'r' (zie afbeelding 1). Hier is frequentieanalyse lastiger. Eigenlijk is het Caesarcijfer ook een vorm van het Vigenèrecijfer, maar dan met een sleutel van slechts één 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
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

De bovenste rij is de boodschap, de linkerkolom zijn de sleutelletters, het kruispunt is het geheimschrift. Bron: https://maizarti.wordpress.com/2011/04/02/vigenere-cipher-dan-hill-cipher/

Bij het Vigenèrecijfer kan toch ook frequentieanalyse worden toegepast. Als een sleutel van vier letters wordt gebruikt, heeft de eerste letter van het bericht dezelfde codering als de vijfde en de negende letter, en de tweede als de zesde, enzovoorts. Op zo'n groep van letters kan dan een frequentieanalyse worden uitgevoerd. Hierbij moet wel bekend zijn hoe lang de sleutel is, dit kan door simpel proberen ontdekt worden. Er is hier

een uitzondering op, namelijk als de sleutel even lang is als het te coderen bericht zelf. Dit is het geval bij het 'One-time-pad' van Vernam. Met deze methode is de codering volkomen onregelmatig, deze vorm van cryptografie is daarom perfect veilig.

Voor meer informatie: http://www.math.ru.nl/wiskundigdenken/2003/crypto1/stof2509-dut.shtml

Bronnen

- https://nl.wikipedia.org/wiki/Vigen%C3%A8recijfer
- http://www.wiskunde123.nl/?a=caesar
- http://www.math.ru.nl/wiskundigdenken/2003/crypto1/stof2509-dut.shtml