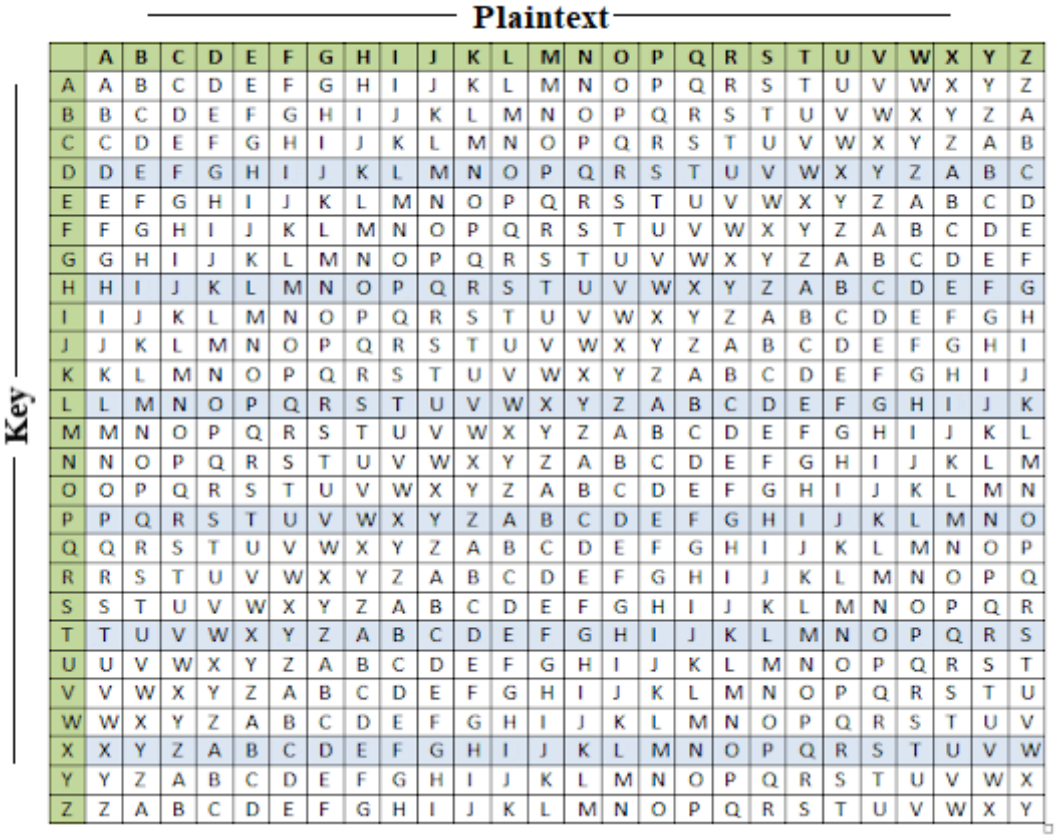
Gegevensbeheer en beveiliging – Les 4

Vignère cipher

Het Vignère cipher kan je zien als een uitbreiding op het Caesar cipher. In plaats van met 1 verschuiving te werken zijn er meerdere verschuivingen. De verschuivingen worden bepaald door een sleutelwoord en de Vignère-tabel (hieronder).



Key \ Plaintext	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

Versleutelen met Vignère cipher

We nemen bijvoorbeeld als sleutelwoord “GEHEIM” en we willen hiermee volgende zin versleutelen:

DITISEENGEHEIMETEKST

We kiezen dan voor de eerste letter van de zin (de letter “D”) als eerste verschuiving de rij met de letter “G”. De “D” wordt dan een “J” (zoek in de Vignère-tabel de letter die op het kruispunt staat van de rij met de “G” en de kolom met de “D”).

Om de tweede letter te versleutelen kijken naar de rij met de letter “E” en de kolom met de “I”. De “I” wordt een “M”.

Zo gaan we verder. Als het sleutelwoord teneinde is herhalen we het woord.

```
DITISEENGEHEIMETEKST
GEHEIMGEHEIMGEHEIMGE
```

De versleutelde tekst wordt:

```
JMAMAQKRNIPQOQLXMWYX
```

Ontsleutelen met Vignère cipher

Om een versleutelde tekst terug om te zetten in leesbare tekst moeten de verschuivingen, net als bij het Caesar cipher, omgedraaid worden. Via het (ver)sleutelwoord kunnen we een omgekeerd (ont)sleutelwoord maken. De letter “G” van ons versleutelwoord is eigenlijk een verschuiving van 6 plaatsen, als we 6 plaatsen terugschuiven (-6 of 20) krijgen we terug de originele letter. Voor de andere letters doen we net hetzelfde.

```
GEHEIM => 6.4.7.4.8.12

-6.-4.-7.-4.-8.-12 => UWTWSO

JMAMAQKRNIPQOQLXMWYX
UWTWSOUWTWSOUWTWSOUW
```

Vignère cipher kraken

Denk je dat de Vignère versleuteling te kraken is? Een tijdlang werd de Vignère versleuteling als onkraakbaar beschouwd. Het is alleszins moeilijker dan het Caesar cipher, maar onmogelijk is het niet *als de sleutel niet te lang is*.

Een brute-force-attack is moeilijker aangezien het aantal mogelijkheden heel groot is. Door een sleutel te kiezen uit een woordenboek (bijvoorbeeld het woord “GEHEIM”) maak je een brute-force-attack wel veel gemakkelijker.

Om een tekst te kraken kan je gebruik maken van het feit dat in een normale tekst er waarschijnlijk woorden of letters herhaald worden. Sommige woorden komen gemiddeld meer voor dan anderen. Een aantal van de meest voorkomende woorden zijn: ja, dat, van, de, het, een en en (https://onzetaal.nl/taaladvies/woordfrequentie/). Deze vaak voorkomende woorden zullen door ons sleutelwoord (“GEHEIM”) maar op een aantal verschillende manieren versleuteld kunnen worden. Een drieletterwoord zoals “HET” kan slechts op 6 manieren versleuteld worden met het sleutelwoord “GEHEIM”:

Tekst	HET	HET	HET	HET	HET	HET
Sleutel	GEH	EHE	HEI	EIM	IMG	MGE
Versleutelde tekst:	NIA	LLX	OIB	LMF	PQZ	TKX

Als we onderstaande tekst versleutelen:

HETVIGENERECIJFERISINDECRYPTOGRAFIEEENVANDEKLASSIEKEHANDCIJFERSHETWERDU
ITGEVONDENDOORGIOVANBATTISTABELLASOMAARHETWASDOORBLAISEDEVIGENEREDATHET
ALGEMEENBEKENDRAAKTEWAARDOORHETZIJNNAAMKREEGHETWERDECHTERLANGETIJDZELDE
NGEBRUIKTVANWEGEZIJNCOMPLEXITEIT

Krijgen we deze cijfertekst (met een aantal herhalende fragmenten):

NIAZQSKRLVMOONMIZUYMUHMOXCWXWSXEMMMQKRCEVPKOSEAEOIRIPMTHJMRRKVZ**LMF**CIYHC
UZKLZWZJIUHWAXKPSDMTFHXBUYXHFMXREZSUMGV**OIB**IGWKSWDHPHMAQJICMOQTIYILMZ**LLX**
IXMITIMZHIRIVPXEHOBQCEHVLAUV**OIB**LONURIMSOYIMS**NIA**AMDJIJLBQXPHROQZMQHHQRHL
ROQHVBMSFBEUAMSKDPNVOUQWPMJOXLMB

Uit de afstand van de herhalende fragmenten kan een veelvoud van de lengte van de sleutel worden afgeleid en na wat puzzelen mogelijk de lengte van de sleutel.

Als je de lengte van de sleutel hebt kan je uit de cijfertekst al de letters bekijken die door het eerste karakter van de sleutel worden vercijferd en deze kraken via letter-frequentie-analyse. Vervolgens doe je hetzelfde met al de letters die door het tweede karakter van de sleutel worden vercijferd enzoverder tot je heel de sleutel bent afgegaan.

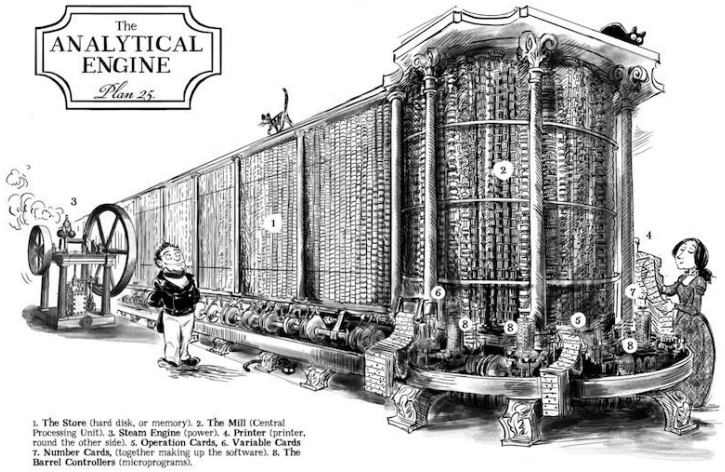
Om wat meer inzicht te krijgen in hoe je een cijfertekst, versleuteld met Vignère versleuteling, kan ontcijferen kan je zelf eens een poging wagen op deze site:

https://www.simonsingh.net/The_Black_Chamber/crackingprinciple.html
https://www.simonsingh.net/The_Black_Chamber/vigenere_cracking_tool.html

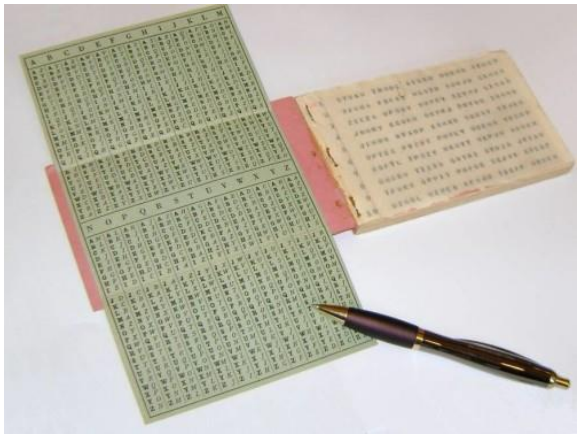
Charles Babbage

Een pionier in het ontcijferen van de Vingère versleuteling was **Charles Babbage**. Hij is ook een computer-pionier die in 1837 (!) een mechanische computer bedacht: de “analytical engine”. De analytical engine is ontworpen, maar nooit gebouwd. Hij zou op stoom werken omdat er toen nog geen sprake was van een elektriciteitsnet. Voor meer info over de machine:

https://www.youtube.com/watch?v=XSkGY6LchJs
https://www.youtube.com/watch?v=5rtKoKFGFSM
https://en.wikipedia.org/wiki/Analytical_Engine



One-time pads



Het kraken van de Vignère versleuteling werkt enkel als er een korte sleutel wordt gebruikt die herhaald wordt. Daardoor zullen er herhalende stukken in de cijfertekst komen te staan. Als er een sleutel wordt gekozen die volledig willekeurig is en even lang (of langer) als de tekst wordt het ontcijferen onmogelijk. De cijfertekst is dan volledig willekeurig en heeft geen structuur meer. Belangrijk is dan dat de sleutel niet hergebruikt wordt om verschillende teksten te gaan versleutelen, anders wordt het toch weer mogelijk om de tekst te gaan ontsleutelen. Het is ook een uitdaging om de sleutel veilig te bewaren.

Als men een voldoende lange sleutel (even lang of langer dan het bericht zelf) slechts eenmaal gebruikt spreekt men van een *one-time pad*. Deze versleuteling werd onder andere gebruikt door de KGB. De pad was een gedrukt boek met pagina's met sleutels voor eenmalig gebruik. Voor gebruik in grotere computer-systemen met veel data is het onhandig omdat de data zou verdubbelen in omvang. Het veilig bijhouden van de grote paswoorden is ook problematisch.

https://en.wikipedia.org/wiki/One-time_pad

Oefening: Vingère cipher

Maak een programma waar je een sleutel kan ingevenen en een bestand kan versleutelen (met Vignère versleuteling). Voorzie ook een optie om te ontsleutelen.