1 ADFGVX

1.1 De opdracht

Om ADGFGVX te kraken moeten we eerst de morse code decoderen, daarna de kolom transpositie ongedaan maken en vervolgens het vierkant vinden om de oorspronkelijke tekst te bekomen.

1.2 Morse decoderen

Dit is snel gedaan door de tekst op te splitsen in de strings die tussen "/" staan en deze via een simpele map om te zetten naar hun bijbehorende characters.

1.3 De kolomtranspositie

Aangezien ADFGVX eindigt met een enkele kolomtranspositie, moesten we deze eerst ongedaan maken. Hiervoor gebruikten we hetzelfde systeem als beschreven bij Vigenre: voor alle mogelijke transposities tot een bepaald aantal kolommen werd de index of coincidence berekend, waarna die met de hoogte index gekozen werd. Merk op dat we hierbij de digrammen moesten gebruiken om de index te berekenen. Uiteindelijk vonden we 4 mogelijke kolomtranspositie met 4 kolommen, met elk een even grote IC.

1.4 Vinden van de taal.

Door eerst een frequentieanalyse te doen op de 4 meest waarschijnlijke teksten, kregen we de onderstaande tabel.

'FV'	16.93	'AA'	8.26	'DX'	8.02	'AD'	7.80
'XV'	7.32	'VD'	7.18	'AF'	6.15	'FF'	5.80
'GG'	5.64	'DD'	4.91	'XD'	3.64	'XG'	3.18
'FA'	3.10	'DG'	2.94	'VX'	1.59	'DF'	1.21
'VA'	1.16	'VG'	1.16	'GF'	0.99	'GD'	0.67
'AV'	0.56	'GX'	0.51	'FG'	0.32	'XX'	0.13
'AG'	0.13	'VV'	0.10	'FD'	0.08	'XF'	0.08
'FX'	0.05	'XA'	0.05	'DA'	0.05	'VF'	0.05
'DV'	0.05	'AX'	0.02	'GA'	0.0	'GV'	0.0

Om deze tabel te analyseren vergelijken we hem gewoon met gekende frequenties[1]. Dit kan omdat de digrammen in ADFGVX voor enkele characters staan. In ADFGVX kan men ook cijfers gebruiken. Deze staan niet in de frequentietabellen vermeld, maar dit is niet echt een probleem, aangezien deze waarschijnlijk een redelijk kleine frequentie hebben. Dit gaf ons wel een

[1] `http://en.wikipedia.org/wiki/Letter_frequency`

vervormde index of coincidence, waardoor we puur op deze waarde de taal niet konden bepalen. Het viel ons wel op dat het meest voorkomende digram, 'FV' bijna dubbel zo frequent was als het tweede. Van de waarschijnlijke talen voor deze tekst, zijn het Frans en Duits de enige met dit kenmerk. Aangezien de Enigma code in het Duits is, is het zeer waarschijnlijk dat deze tekst in het Frans is geschreven.

1.5 Vinden van de bron tekst

Voordat we begonnen met letters te vervangen hebben we eerst het aantal mogelijke teksten terug gebracht van 4 naar 2. We hebben dit gedaan door te kijken naar de digrammen die 2 maal op elkaar volgen. Bij twee van de vier mogelijke teksten kwam een opeenvolging van twee keer hetzelfde digram erg veel voor. Gezien dit in het Frans minder voorkomt, konden we deze teksten al elimineren.

Nu we nog 2 mogelijke teksten hadden, hebben we het werk opgesplitst onder Jakob en Robin, die elks een tekst probeerden te kraken.

Door eerst de meest frequente letters in te vullen (FV=e, DX=n, ...) en daarna met trial en error de andere redelijk frequente characters in te vullen, verschenen er Franse woorden, of strings die erg leken op een Frans woord, hierdoor konden we ook de minder frequente letters invullen. Eens ongeveer de helft van de digrammen was vervangen door een character, konden we zinnen lezen en zo de andere characters aanvullen, eens we de eerste zin zeker wisten konden we Google aanspreken [2] en vonden we dat het ging om het eerste hoofdstuk van *"Vingt mille lieues sous les mers"* van Jules Vernes.

Zoals reeds vermeld hadden we 2 teksten opgelost, beide gaven dezelfde tekst. Als we kijken naar de vierkanten die beiden gaven (Figure 2 en 3), zien we dat de ene de getransponeerde versie van de andere is. Dit betekent dat de digrammen voor de ene versie de omgekeerde zijn van de andere versie. Ene ene ciphertekst is dus gelijk aan de andere ciphertekst met elk digram omgedraaid, voor de kolomtranspositie. Gezien de kolomtranspositie met een even aantal kolommen gebeurde, kan door een verschillende kolomtranspositie toe te passen op beide teksten, dezelfde uiteindelijke ciphertekst bekomen worden.

[2] `https://www.google.be/search?q=l%27annee+1966+fut+marquee+par+une+evenement&oq=l%27annee+1966+fut+marquee+par+une+evenement&aqs=chrome..69i57.1740j0j7&sourceid=chrome&es_sm=122&ie=UTF-8#q=l%27annee+1966+fut+marquee+par+un+evenement+bizarre`

	A	D	F	G	V	X
A	a	5	c	?	q	w
D	s	o	2	x	i	d
F	r	g	l	b	0	1
G	6	m	y	u	f	p
V	h	3	e	?	z	t
X	4	n	8	j	v	k

Figure 1: Vierkant van de 1e tekst

	A	D	F	G	V	X
A	a	s	r	6	h	4
D	5	o	g	m	3	n
F	c	2	i	y	e	8
G	?	x	b	u	?	j
V	q	l	0	f	z	v
X	w	d	1	p	t	k

Figure 2: Vierkant van de 2e tekst