Cryptografie en Codetheorie:
ADFGVX

Robin Verachtert - s0121405

10 march 2015

Contents

1 ADFGVX

1.1 Undoing the single column transposition

1.2 Vinden van de taal.

Door eerst een frequentie analyse te doen op de 4 meest waarschijnlijke teksten, kregen we de tabel in Figure 1. 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 en daze staan niet in de frequentie tabellen van de talen, maar dit is niet echt een probleem, aangezien de frequentie van deze zeer klein zijn.

1.3 Vinden van de bron tekst

Het digram 'FV' komt het veel vaker voor dan de rest. De enige talen waar dit geval is zijn Frans en Duits. Aangezien de Enigma code in het Duits is het zeer waarschijnlijk dat deze tekst in het Frans is geschreven.

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. (@JAKOB: GIJ hebt dees gedaan, dus kunde gij da uittypen).

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:

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

[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`

'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

Figure 1: Tabel met de digram frequenties voor de tekst verkregen door de 4e kolom transpositie. De andere frequentie tabellen zijn bijna identiek, alleen zijn de digrammen anders.

	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 2: 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 3: Vierkant van de 2e tekst