AARHUS UNIVERSITY, COMPUTER SCIENCE

Cryptology - handin 1

Peter Burgaard - 201209175

September 4, 2016

1 STINSON 1.21.C

We are given the following cipher text:

KQEREJEBCPPCJCRKIEACUZBKRVPKRBCIBQCARBJCVFCUPKRIOFKPACUZQEPB
KRXPEIIEABDKPBCPFCDCCAFIEABDKPBCPFEQPKAZBKRHAIBKAPCCIBURCCD
KDCCJCIDFUIXPAFFERBICZDFKABICBBENEFCUPJCVKABPCYDCCDPKBCOCPE
RKIVKSCPICBRKIJPKABI

and the knowledge that, it has been encrypted using the affine cipher. We have also been told that the plain text is in french, but we can not know for sure.

The first thing we do in order to crack the encryption is to gather some statistics about the text. By using a letter counting website [1], i gathered the following:

A	B	C	D	E	F	G	H	I	J	K	L
13	21	32	9	13	10	0	1	16	6	20	0

M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	20	4	12	1	0	6	4	0	2	1	4

next i found the letter frequency in french [2]:

[1] https://www.mtholyoke.edu/courses/quenell/s2003/ma139/js/count.html
[2] http://www.sttmedia.com/characterfrequency-french

A	B	C	D	E	F	G	H
8.13 %	0.93 %	3.15 %	3.55 %	15.10 %	0.96 %	0.97 %	1.08 %

I	J	K	L	M	N	O	P
6.94 %	0.71 %	0.16 %	5.68 %	3.23 %	6.42 %	5.27 %	3.03 %

Q	R	S	T	U	V	W	X	Y	Z
0.89 %	6.43 %	7.91 %	7.11 %	6.05 %	1.83 %	0.04 %	0.42 %	0.19 %	0.21 %

From this we get, the most two used letter in our cipertext is C with 32 apperences and B with 21 apperences. The two most common letters in french are E with 15.10 % and A with 8.13 %. Assuming Stinson only have been using the letters which are available in the english alphabet we assume $\mathscr{C} = \mathscr{P} = \mathbb{Z}_{26}$. At this point we will also assume that, A have been given the numerical value 0, and B given 1 etc. in the plain text.

First we might solve which number's x have $gcd(x, 26)$. From theorem 1.2 or simple by looking at page 10 in Stinson, we find there are 7 numbers, 1, 3, 5, 7, 11, 17 and 25. Now we can start decyphering the text, and as a first guess, we might hypothesize that E encrypts to C and A encrypts to B, which implies $e_k(4) = 2$ and $e_k(0) = 1$, where $k \in \mathscr{K}$ being a key from the keyset and $e_k(\cdot)$ being the encryption function, using key k. We find this This yields two linear equiations with two unknows:

$$4 * a + b = 2$$
$$0 * a + b = 1$$

which implies

$$4a \equiv 1 (mod 26)$$

But this doesn't have a solution.