

---

# Cryptology - handin 1

---

Peter Burgaard - 201209175

September 14, 2016

## 1 STINSON 1.21.C

We are given the following cipher text:

KQEREJEBPCPCJCRKIEACUZBKRVPKRBCIBQCARBJCVFCUPKRIOFKPACUZQEPB  
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 <sup>1</sup>, 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 <sup>2</sup>:

---

<sup>1</sup><https://www.mtholyoke.edu/courses/quenell/s2003/ma139/js/count.html>

<sup>2</sup><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 ciphertext is C with 32 appearances and B with 21 appearances. 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  $\mathcal{C} = \mathcal{P} = \mathbb{Z}_{26}$ . 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 deciphering the text, and as a first guess, we might hypothesize that e encrypts to C and s encrypts to K, which implies  $e_k(4) = 2$  and  $e_k(18) = 10$ , where  $k \in \mathcal{K}$  being a key from the keyset and  $e_k(\cdot)$  being the encryption function, using key  $k$ . We find this This yields two linear equations with two unknowns:

$$\begin{aligned} 4 * a + b &= 2 \\ 18 * a + b &= 10 \end{aligned}$$

which implies by gaussian elimination

$$a = 5 \quad \text{and} \quad b = 8$$

We see that  $\gcd(5, 26) = 1$  which means this key (5, 8) is valid. To decrypt the text we gotta find the inverse to our a, which is  $5^{-1} = 21$  in  $\mathbb{Z}_{26}$ . The first letter in the ciphertext is an K, so by Cryptosystem 1.3 in Stinson, we decrypt.

$$d_K(10) = 21(10 - 8) \bmod 26 = 16$$

which means  $d_K(K) = Q$ , etc. Using this method we get:

QMUHUVUJERREVEHQAUOESTJQHNQRHJEAJMEOHJVENPESRQHAWPQROESTM  
URJQHDRUAAUOJZQRJERPEZEEOPAUOJZQRJERPUMRQOTJQHFOAJQOREEASHE  
EZQZEEVEAZPSADROPPUHJAETZPQOJAEJJUBUPESRVENQOJREYZEEZRQJEWERUH  
QANQCERAEJHQA VRQOJA

Which doesn't seem to be the encrypted plaintext.

Next we'll guess e still being encrypted to C and t to B, which will give us

$$4 * a + b = 2$$

$$19 * a + b = 1$$

which implies by gaussian elimination

$$a = 19 \quad \text{and} \quad b = 4$$

Again we see that  $gck(19,26) = 1$  which means (19,4) is valid. Using it, we get the solution

OCANADATERREDENOSAIEUXTONFRONTTESTCEINTDEFLEURONSGLORIEU  
XCARTONBRASSAITPORTERLEPEEILSAITPORTERLACROIXTONHISTOIREEST  
UNEEPOPEEDESPLUSBRILLANTSEXPLOITSETTAVALEURDEFOITREMPEEPROT  
EGERANOSFOYERSETNOSDROITS

which is the french translation of the canadian national anthem, and we will assume we are done.