# MA080G Cryptography Assignment Block 1

Viktor Rosvall

April 8, 2019

## Question 6

### (a)

Explain what Friedman's Index of Coincidence measures and compute it for the ciphertext below, hence explain how you can see that the cipher used to encrypt it was not monoalphabetic.

**Answer (a)**

### (c)

Decrypt the first line of the ciphertext below, given that it has been encrypted by using a Vigen‘ere cipher with the keyword **fishy**.

KQJZR YPWMG XPEBQ YJWJY ZOZAR MILPQ JIKFY GITFG YPAUI HWMSB MINLA FCYOR

**Answer (c)**

Using the formula we can get the ciphertext $y_i$:

$$y_i = (x_i + k_{iMODn})MOD26$$

In this case, we are looking for the plaintext letters $x_i$.

The key: **fishy**, corresponds to the sequence (5,8,18,7,24) as $y_i$.

If we want to decrypt the cipher text "KQJZR", which in numeric corresponds to "10,16,9,25,17", we start by using $y_0 = 10$ to decrypt K:

$$\begin{aligned} 10 &= (x_0 + 5_{0MOD5})MOD26 \\ 10 &= (x_0 + 5_0)MOD26 \\ 5 &= x_0 MOD26 \\ x_0 &= 5 \end{aligned}$$

So the first letter "K" $\rightarrow$ "f". Using this formula for the remaining 4 ciphertext letters, we get "KQJZR" $\rightarrow$ "first".