MA080G Cryptography Assignment Block 1

Viktor Rosvall

April 8, 2019

Question 4

(a)

Define Euler's Φ-function.

Answer (a)

Euler's Φ function on the natural numbers $n \geq 2$ given by:

$$\Phi(n) = \#\text{ congruence classes } [a] \in Z_n \text{ such that } gcd(a, n = 1)$$

Counts the number of invertible elements of Z_n.

(b)

Compute $\Phi(17)$, $\Phi(289)$ and $\Phi(221)$.

Answer (b)

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)

The *Index of Coincidence* (IOC) I, measures the likelihood of picking 2 identical letters, from a text.

We can calculate the IOC I, by using the counted letters, given in the assignment. Where the letters: a,b,c...,z are represented as $n_0, n_1, ..., n_{25}$, and n

is the total number of letters.

$$\begin{aligned} I &= \frac{\sum_0^{25} n_i(n_i-1)}{n(n-1)} \\ &= \frac{26(26-1)+20(20-1)+...+25(25-1)}{444*443} \\ &= \frac{8638}{196692} \\ &\approx 0.44 \end{aligned}$$

(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".