**Antwoorden les 4: Vigenère**

**Opgave 1**
a. CLBXT IJZAZ LMIMF WOFAY
b. Zolang je het codewoord niet weet zijn de C op de eerste plek, de T op plek 5, enz., gewoon toevallige letters. Ze verraden in principe niets.

**Opgave 2**a. Je weet niet hoe lang het sleutelwoord is en dus ook niet op welke letters je de frequentie-analyse moet toepassen.
b. Als je weet dat de sleutellengte *n* is, komt het kraken neer op *n*keer een schuif cryptosysteem kraken.
c. De boodschap is zo kort dat frequentieanalyse niet zinvol is

**Opgave 3**
Vogel.

**Opgave 4**a.*P(a)·P(a)+ P(b)·P(b)+P(c)·P(c)+ P(d)·P(d)+... P(z)·P(z)*
b. 1/26
c. Letters die een veelvoud van de sleutellengte uit elkaar staan, komen steeds uit een alfabet dat over hetzelfde aantal posities verschoven is. Omdat bepaalde letters daar vaker voorkomen, is de kans groter dat je juist die letters aantreft.

**Opgave 5**
Sleutellengte 4, want bij 4 en 8 posities verschoven zijn er meer overeenkomsten en 4 en 8 zijn veelvouden van 4. Het zijn ook veelvouden van 2 maar dan had je bij 2, 6, 10, enz. meer overeenkomsten verwacht.

**Opgave 6**
Je moet dan een sleutelwoord gebruiken dat heel lang is ten opzichte van de lengte van de tekst. Het beste is het natuurlijk om een sleutelwoord te nemen dat even lang is als de tekst die je wilt vercijferen. Je zou bijvoorbeeld kunnen afspreken dat je als sleutelwoord steeds de volgende bladzijde uit een boek neemt dat je allebei hebt. Je moet dan alleen wel geheim houden waar je je sleutel vandaan haalt en het is veel werk!

**Opgave 7**
Het is wel moeilijker, maar niet veel moeilijker als je bijv. een computer kunt gebruiken. Achterhalen van de sleutellengte werkt hetzelfde als bij Vigenère. Daarna moet je *n*keer een mono-alfabetische substitie ontcijferen i.p.v. *n*keer een schuifsysteem, maar met behulp van letterfrequentie-analyse en/of een computer is het wel binnen niet al te lange tijd te doen.

**Opgave 8**
Na de sleutel één keer gebruikt te hebben, wordt hij niet meer herhaald. De truuk waarbij je kijkt na hoeveel posities weer met dezelfde sleutel vercijferd wordt is hier dus niet te gebruiken.