**Antwoorden les 7: Cijfermachines**

**Opgave 1**
De drie scramblers kunnen op **6** manieren in de Enigma geplaatst worden: a-b-c; a-c-b; b-a-c; b-c-a; c-a-b en c-b-a.
Door de 6 kabels kun je 6 paren verwisselen. Het resultaat van de verwisselbare scramblers is daarom een factor 6.

Het resultaat van de 6 kabels berekenen we op 2 verschillende manieren:
*Manier 1*: Op **9657700** manieren kun je12 letters kiezen uit 26 letters (dat is het aantal combinaties van 12 uit26).
Met die 12 letters kunnen er op **7484400** manieren verschillende tweetallen gevormd worden
(**=12x11/2 x 10x9/2 x 8x7/2 x 6x5/2 x 4x3/2 x 2x1/2**),
maar de volgorde van die tweetallen (**6!=720)** is niet belangrijk.
Het resultaat van de 6 kabels is daarom een factor 100.391.791.500

*Manier 2*: Het aantal permutaties van 12 letters uit 26 is 26!/14!. Volgens het Mississppi-model zijn er 6 tweetallen die hetzelfde resultaat geven. Bovendien is de volgorde van die tweetallen (**6!=720)** niet belangrijk.
Het resultaat van de 6 kabels is daarom een factor **26!/14!/26/6!**=100.391.791.500

Het aantal verschillende cijferalfabetten wordt aldus
**17576\*6\*9657700\*7484400/720= 17576\*6\*100.391.791.500=1,06\*1016** verschillende manieren.

Als de ontsleutelaar 1 sleutel per minuut uit zou kunnen proberen, dan had hij daar ruim **200 miljard jaar** voor nodig.

**Opgave 2**Het probleem van de kabels is dat dit slechts een monoalfabetische substitutie is met minder dan de helft van de letters. Bij elke aanslag blijft de instelling hetzelfde en daarmee ontstaat een vercijfering die gemakkelijk met frequentieanalyse te kraken is. De scramblers zorgen ervoor dat het alfabet steeds verandert en daarmee beschermen de scramblers het systeem tegen frequentieanalyse.

**Opgave 3**a. **KJWYQ IVRYJ GFZRW E**
b. Dit is per tweetal verschillend. Missie geslaagd?