**Antwoorden les 6: Het grote publiek**

**Opgave 1**

GD DO GD RQ AR KY GD HD NK PR DA MS OG UP GK IC QY
De link die gebruikt wordt in opgave 2 geeft een ander antwoord, maar maakt een fout in het tweede diagram.

**Opgave 2**

Het Playfair geheimschrift werd voor het eerst toegepast in de boerenoorlog.

**Opgave 3**

25 onderzeeërs en 1 admiraal: ieder zou over 25 blokken moeten beschikken om te kunnen communiceren met de 25 anderen. Hierbij is steeds een tweetal blokken hetzelfde. Het totaal aantal blokken is dus ½ x 26 x25 = 325 blokken.

**Opgave 4**

Zodra er één bericht verstuurd is, moet iedereen een pagina afscheuren en vernietigen. Als er iemand een fout maakt loopt het in de soep. Als bovendien één blok in de handen van de vijand valt dan is het hele systeem gekraakt.

**Opgave 5**Het hergebruik van een eenmalig blokcijfer zou een vijandelijke cryptoanalist in staat stellen berichten te ontcijferen door aan te nemen dat bepaalde woorden in de tekst vaak voor zouden moeten komen. In het Nederlands zijn dit bijvoorbeeld de lidwoorden *de*, *het* en *een*. Door nou de hele tekst 'terug te rekenen' alsof de hele tekst uit *een'*s zou bestaan krijgen we een blokcijfer dat we over de tweede tekst kunnen leggen. Daar vinden we dan de match met de *een'*s in de tweede tekst. Op deze manier wordt langzaamaan het blokcijfer ontrafeld en daarmee de tekst ontcijferd.