**Fasen binnen de opdracht.**

**Eerste fase:**

Theoretische verkenning van het onderwerp. De tekst is zodanig opgesteld dat de leerling met de basiskennis van hoofdstuk 1 t/m 3 de tekst zelfstandig moet kunnen bestuderen. De aangeboden informatie bevat geen vragen.

Sommige boodschappen zijn niet voor ieders oren bestemd. Als je een boodschap wilt versturen die alleen bestemd is voor de ontvanger. Je wilt niet dat deze onderweg door derden gehoord wordt. Een briefje doorgeven in de tweede klas is een uiterst riskante onderneming. Bij het doorgeven is de verleiding is groot om het even open te vouwen voor het bij de geadresseerde komt. Als je niet uitkijkt weet iedereen behalve de ontvanger dat je verliefd bent. Om boodschappen priv\’e te houden zijn allerlei slimme trucs verzonnen. Er is een NLT-module over dit onderwerp (ref). Hoe geraffineerd ook, een encryptie kan altijd gekraakt worden. Het is een voortdurende wapenwedloop tussen versleutelaar en ontcijfereaar. Natuurlijk weet de ontvanger wel om te gaan met de versleuteling. De ontvanger heeft een sleutel. In klassieke encryptie zijn er tal van voor de hand liggende lekken te verzinnen. Je bankgegevens zijn door een pincode van vier cijfers beschermd. Deel deze nooit met een ander. Een typisch gevaar bij klassieke versleuteling.

Voor versleuteling is ook een omgekeerde operatie nodig. De uitdaging is om de versleuteling makkelijk te laten verlopen, maar de ontcijfering zo moeilijk mogelijk, echter als de sleutel in handen in moet het weer eenvoudig gaan.

Hoe ingenieus de trucs ook zijn, in klassieke encryptie blijft het gevaar bestaan van het lekken van de sleutel. Bij quantum encryptie is dit probleem te omzeilen door het no-cloning principe.

Onze kennis van H123 is ruim voldoende om het principe van quantum encryptie te begrijpen. Sterker nog zelfs zonder verstrengeling kunnen we dit probleem aanpakken. In 1984 stelden Bennet en Brassard hiervoor een protocol op. Dit protocol kunnen we in de klas simuleren en een boodschap overzenden. We kunnen er een wedstrijdje van maken.

**Tweede fase:**

In deze fase onderzoekt de leerling het thema dat tijdens de eerste fase is geïntroduceerd. Tijdens deze fase is sprake van vragen met een gesloten vraagvorm die van de leerling vragen de aangeboden kennis te reproduceren. De vragen vormen een aanvulling op de informatie uit de eerste fase. Ook kan aan de leerling gevraagd worden dingen op te zoeken op internet.

Opdracht: Wfsaom ffo mjtu

Bedenk enkele systemen die een versleuteling opleveren. Wat moet de ontvanger weten? Wat is de omgekeerde operatie?

Opdracht : BB84

Bestudeer het werkblad BB84. Beantwoord de vragen op het werkblad.

**Derde fase.**

In deze fase krijgt de leerling de vraag om de aangeboden kennis toe te passen in een nieuwe context met meer complexiteit. Hier kan sprake zijn van

Opdracht: Eve.

Eve ziet nog niet in het spelletje opgenomen …

Opdracht: Is it safe?

Wiskundig geen speld tussen te krijgen. De werkelijkheid is weerbasrstig. Kun je een zwakke plekken aanwijzen? Waarom hebben we dit niet allemaal in onze bankpas zitten?

**Vierde fase.**

In deze fase verzorgt de leerling een presentatie in een of andere vorm, PPT, youtubefilmpje, werkstuk etc.

Opdracht Bouw een systeem (boek spooky action)

Per opstelling

Optische rails zaklamp collimator lens, twee polaroids

Opdracht wie zendt als eerste de boodschap