LEITFADEN: ESCAPE-GAME QUANTENKRYPTOGRAPHIE

RAHMENBEDINGUNGEN

Zielgruppe: Klasse 12 (Grund- und Leistungskurs) Lernbereich „Quantenobjekte“

Dauer: 70 min Spielzeit + 20 min Vor-/Nachbesprechung

Material:
- Smartphone oder Tablet mit der App *Actionbound* (+ Internetzugang)
- Stift und Papier für Notizen
- Hinweise zu Rätseln

Lernziel: Die Schüler wenden in dem Escape Game ihr Wissen zu den Grundlagen der Quantenphysik auf das Konzept der Quantenkryptographie an, um dieses zu festigen.

VORBESPRECHUNG

Spielziel: Im Escape-Game bist du als Polizist undercover in einer Verbrecherorganisation. Ziel ist, vor den Verbrechern zu fliehen, deine gesammelten Beweise in Sicherheit zu bringen und die Organisation hinter Gitter zu bringen.

Gruppen: zwei Schüler pro Gruppe

Zeitvorgabe: 70 Minuten

Hinweise: Zu jedem Rätsel gibt es je drei gestaffelte Hinweise, wobei der dritte die Auflösung des Rätsels beinhaltet. Die Hinweise können in analoger Form zur Verfügung gestellt werden. Die Schüler entscheiden selbst über die Inanspruchnahme der Hinweise.

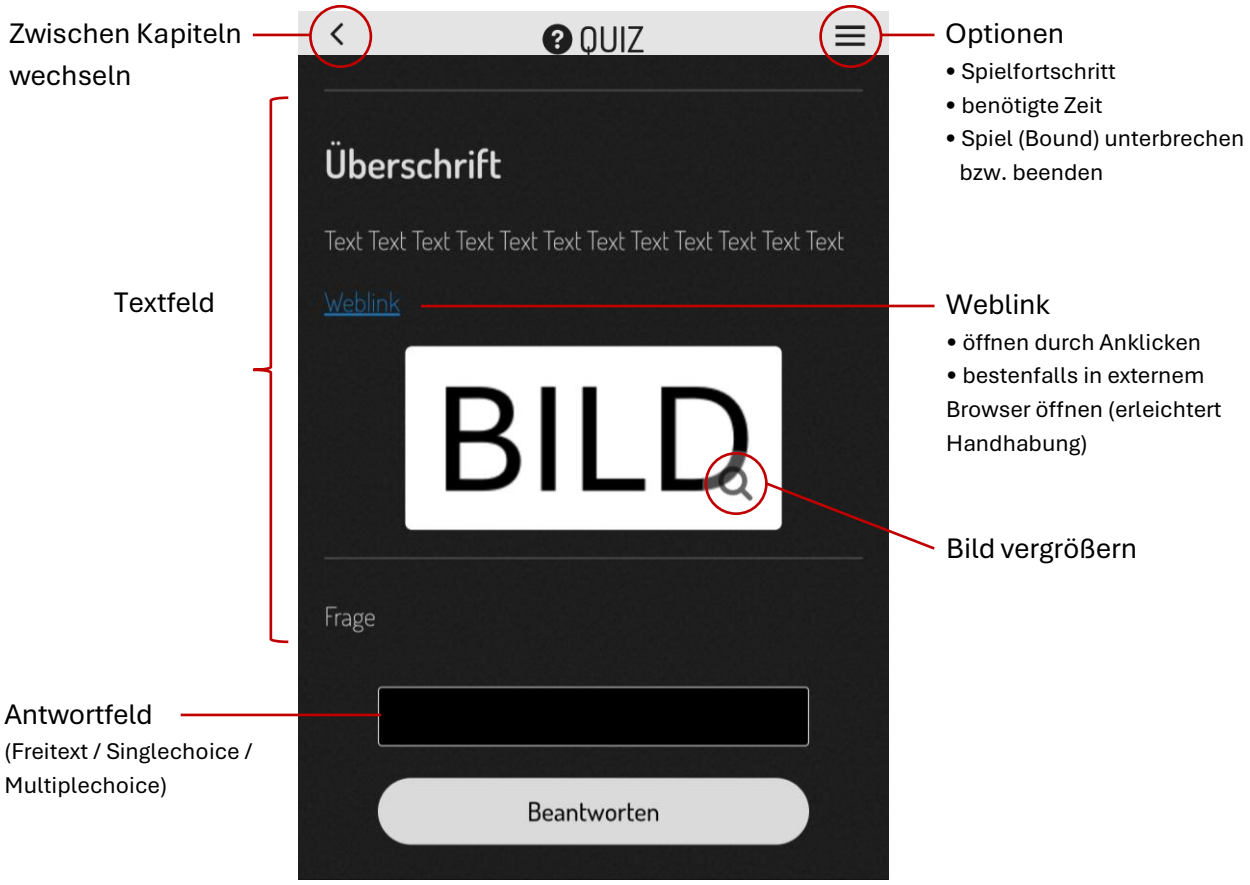
<u>Hinweise zur Durchführung:</u>

- Vor dem Start des Escape-Games sollten die allgemeinen Funktionen der *Actionbound*-App erklärt werden (siehe *Benutzeroberfläche*).
- Weiterhin sollte sichergestellt werden, dass den Schülern der Begriff „Kryptographie“ bekannt ist.
- Sollte eine Gruppe das Spiel eher als geplant beenden, dann können diese sich schon mit den Fragen der Nachbesprechung beschäftigen (siehe *Nachbesprechung*).

<u>Escape-Game starten</u>

Um das Escape-Game zu starten, wird der nebenstehende QR-Code in der *Actionbound*-App gescannt.

Benutzeroberfläche *Actionbound*-App



NACHBESPRECHUNG

In der Nachbesprechung sollten die Spielinhalte (v.a. die Rätsel und das Handbuch) nochmals reflektiert und in Zusammenhang mit den zu lernenden Inhalten gebracht werden. Auch deren Anwendung in der realen Welt sollte besprochen werden.

Im Folgenden sind verschiedene Anregungen für die Gestaltung der Nachbesprechung aufgeführt.

Mögliche Fragen an Schüler (Antworten):

a) Welche Vorteile bietet die Quantenkryptographie bzw. das BB84-Protokoll im Vergleich zu klassischen Verschlüsselungsverfahren? Wieso gilt es als ein sicheres Verfahren?

- Durch die Eigenschaften der Quantenphysik können echte Zufallsfolgen generiert werden (bei klassischen Computer sind nur pseudo-zufällige Folgen realisierbar).
- Abhörangriffe können zwar nicht verhindert werden, aber dank der Unbestimmtheit quantenphysikalischer Eigenschaften können sie aufgedeckt werden.

→ Löst damit das Problem der sicheren Schlüsselübertragung bei One-Time-Pads (siehe unten)

b) Welche Wesenszüge der Quantenphysik oder quantenphysikalische Prinzipien werden für das BB84-Protokoll genutzt?

- Statistischer Charakter
- Komplementarität
- Eindeutige Messergebnisse
- weitere Prinzipien: Superposition

c) Können für das BB84-Protokoll nur die +-Basis und ×-Basis verwendet werden?

- Es können beliebige Basenpaare verwendet werden, solange sich alle Basiszustände voneinander unterscheiden und sie sich innerhalb der Basen gegenseitig ausschließen (sonst keine Basis).

d) Welche Möglichkeit könnte ein Spion noch haben, um die Kommunikation abzuhören bzw. zu stören?

- Der Spion könnte die Photonen „kopieren“, das kopierte messen und das ursprüngliche an den Empfänger unverändert weiterschicken (Widerspruch zum No-Cloning-Theorem - siehe unten).
- Der Spion könnte den Übertragungskanal stören (fluten mit Photonen o.Ä.) und so eine Kommunikation verhindern.

<u>Weitere zu besprechende Aspekte:</u>

- Bei einem One-Time-Pad muss der Schlüssel zufällig und mindestens so lang wie die Nachricht sein. Zudem darf er nur ein einziges Mal verwendet werden. Das Verfahren gilt als absolut sicher. Das einzige Problem dabei bildet der sichere Austausch des Schlüssels.
- Der Austausch über die Basen erfolgt über einen klassischen Kanal (bspw. Telefon).
- In der Praxis werden sehr viele Messprozesse pro Sekunde durchgeführt. Das macht eine automatische Auswertung notwendig. Zudem wird bei den Messprozessen eine Liste von Zufallszahlen verwendet, welche die Messbasis wählt.
- Das No-Cloning-Theorem besagt, dass es keinen quantenphysikalischen Prozess gibt, mit welchem der Zustand eines Quantenobjektes exakt auf ein anderes Quantenobjekt „kopiert“ werden kann, ohne dabei den Zustand des ersteren zu verändern.
- Neben dem BB84 gibt es auch andere Protokolle für die Quantenkryptographie. Ein Beispiel ist das E91-Protokoll, welches das Prinzip der Verschränkung zur Erzeugung und Übertragung des Schlüssel nutzt. (Sender und Empfänger erhalten dabei immer je ein Photon eines verschränkten Photonenpaars und führen jeweils an ihrem Photon eine Messprozess durch. Sie können anhand ihres Messergebnisses Rückschlüsse auf das des Kommunikationspartner ziehen.)

VIEL SPAß!