1. Die SuS wird eine E-Mail zugespielt, welche einen Hinweis auf den Ort enthält, wo die nächste Floppy Disk gefunden werden kann. Ebenfalls enthält die E-Mail ein Passwort, welches später benötigt ist. Die E-Mail ist allerdings mit einer „unbekannten“ Verschlüsselung verschlüsselt.

2. Die SuS müssen mithilfe eines Kryptotools (selbst implementiert) die Verschlüsselung lösen.

3. Die entschlüsselte Nachricht für die SuS nach Berlin. Vorher müssen sie allerdings ihrem HQ eine Nachricht schicken, wo sie das HQ über ihre Reise informieren. Die zu versendende Nachricht muss verschlüsselt versendet werden. Verschlüsselung dürfen die SuS frei wählen, es gelten allerdings zwei Bedingungen:
    a. Die SuS müssen die Nachricht selbstständig ver- und entschlüsseln können
    b. Die Nachricht muss sicher verschlüsselt werden. (Was sehen wir als sicher an?/ Transferleistungen)

4. Sobald die Reise vom HQ bestätigt, befinden sich die SuS in Berlin. Dort wird ihnen ein verschlüsseltes Adressbuch zugespielt. Mithilfe des Schlüssels aus der E-Mail können die SuS das Adressbuch entschlüsseln und bekommen einen Hinweis, wo sie die letzte Floppy Disk in Berlin finden können.

5. Beim Ort angekommen, müssen die SuS einen Lückentext lösen. Diesen Lückentext müssen Sie anschließend verschlüsseln. Passt der entstehende Cypertext mit einem gespeicherten Text überein, erhalten die SuS ihre letzte Floppy Disk.
   (Idee: Schlüssel-Schloss-Prinzip)

6. Anschließend müssen die SuS eine verschlüsselte Nachricht ans HQ senden und mitteilen, dass alle Floppy Disks nun gefunden worden sind und die Suche beendet werden kann.