Der Text in der SMS ist eindeutig verschlüsselt. Um ihn zu verstehen, brauchen wir den passenden Schlüssel. Vielleicht findet sich in der E-Mail ja ein ***H****i****n***w***e***i***s*** auf diesen…

Der versteckte Hinweis in der E-Mail lautet: „Verschieben ABC gegen ABC! F ist A“. Wir brauchen also zwei Alphabete, die gegeneinander verschoben werden müssen.

Bei der vorliegenden (sog. Caesar-) Verschlüsselung wird jeder Buchstabe des Klartexts auf einen Buchstaben des Geheimtexts abgebildet. Die Abbildung (also der Schlüssel) besteht darin, dass die Zeichen eines geordneten Alphabets gegenüber einem anderen Alphabet verschoben werden. In diesem Fall wird das zweite Alphabet so nach links verschoben, dass der Buchstabe A des originalen auf den Buchstaben F des zweiten Alphabets abgebildet wird (A→F; B→G, C→H, …). Mit diesem Schlüssel ergibt sich die Nachricht: „UM ACHT AM HAFEN“.

Kapitel 1

Erster Hinweis

Kapitel 1

Zweiter Hinweis

Kapitel 1

Auflösung

Um das Rätsel zu lösen, solltest du dir das Handbuch genauer ansehen. Nicht alles darin stammt vom originalen Autor. Jemand hat darin **herumgeschmiert** und ein paar Stellen unleserlich gemacht. Vielleich verrät dir das etwas über den vierstelligen Code…

Der Hinweis „Der Schlüssel ist der Schlüssel“ weist darauf hin, dass das Passwort für den Laptop, dem Quantenschlüssel aus dem Beispiel im Handbuch entspricht. Das heißt, du musst zunächst die Tabelle 9 unter Anwendung des BB84-Protokolls wieder vervollständigen und dann den Schlüssel identifizieren.

Die vollständige Tabelle sieht wie folgt aus

Sender	Nr. Photon	1	2	3	4	5	6	7	8
	Messbasis	+	+	×	+	×	×	+	×
	Ergebnis	↔	↕	⤡	↔	⤡	⤢	↕	⤡
	Signal	0	1	1	0	1	0	1	1
Empfänger	Nr. Photon	1	2	3	4	5	6	7	8
	Messbasis	×	+	+	×	×	×	+	+
	Ergebnis	⤡	↕	↔	⤢	⤡	⤢	↕	↔
	Signal	1	1	0	0	1	0	1	0

Die grün markierten Einträge entsprechen den Photonen, die Sender und Empfänger mit der gleichen Basis gemessen haben und damit zur Schlüsselerzeugung genutzt werden. Demnach lautet der Schlüssel (und damit das Laptoppasswort): 1101

Kapitel 2

Erster Hinweis

Kapitel 2

Zweiter Hinweis

Kapitel 2

Auflösung

Um dieses Rätsel zu lösen, benötigst du die Simulation, den Notizzettel aus Kapitel 2 und das Handbuch. Außerdem solltest du dir überlegen, wie lang der Schlüssel mind. sein muss und wie viele Messungen du dementsprechend durchführen solltest.

Ziel des Rätsels ist, die Nachricht „PS“ zu verschlüsseln. Dafür musst du die Nachricht ins Binärsystem übertragen und den Schritten, welche in Kapitel 4 bzw. im Handbuch beschrieben wurden, folgen. Damit der Schlüssel lang genug ist - mindestens 10 Ziffern - müssen im Schnitt mindestens 20 Messungen durchgeführt werden.

Die Nachricht „PS“ im Binärsystem dargestellt, lautet:
0111110010.
Der Schlüssel, welcher mithilfe der Simulation generiert wird, lautet:
0101111001.
Damit ergibt sich für die codierte Nachricht, welche an Charles geschickt werden soll:
0010001011.

Kapitel 3

Erster Hinweis

Kapitel 3

Zweiter Hinweis

Kapitel 3

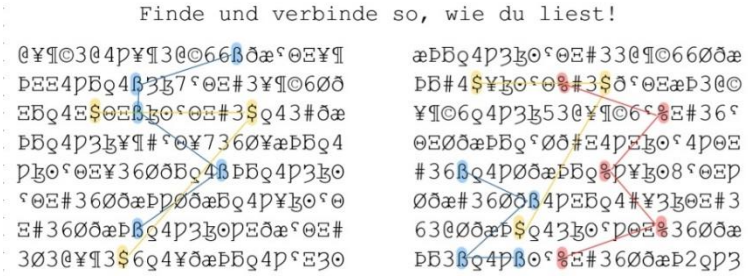
Auflösung

Den Messergebnissen in der E-Mail fehlen zwar die Photonen-Nummern, aber dafür ist jedem Ergebnis ein Sonderzeichen zugeordnet.

Die Anweisung „*Finde und verbinde so, wie du liest*“ ist wörtlich zu verstehen.

Die drei Sonderzeichen aus der E-Mail finden sich auch in dem Zeichenwirrwarr des angehängten Bildes wieder. *Finde* jeweils die gesuchten Sonderzeichen und *verbinde* sie miteinander. „*... so, wie du liest*“ sagt, dass die Reihenfolge der Verbindungen dem normalen Lesefluss entspricht, d.h. von links nach rechts und von oben nach unten. Die beiden Zeichenblöcke sind dabei nicht ohne Grund voneinander getrennt.

Zieht man alle Verbindungen, ergibt das:



Die Messergebnisse lauten also: 3 = ⤢ ; 52 = ↕ ; 77 = ↔

Vergleichst du die Messergebnisse mit deinen eigenen, stellst du fest, dass die Werte für das 77. Photon nicht übereinstimmen. Es gab also einen Spion.

Kapitel 4

Erster Hinweis

Kapitel 4

Zweiter Hinweis

Kapitel 4

Auflösung