**Ablauf des Protokolls**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Alice** | **Eve** | **Bob** |
| *Phase 0* | *Bestimmt Schlüssellänge* |  |  |
| *Sendet die Schlüssellänge an Bob* | *🡪*  *🡨* | *Bestätigt die Schlüssellänge* |
| Phase 1  (initiale Kodierung) | Erzeugt Folge aus „0“ und „1“  Bsp.: 0101 1011 |  |  |
| Erzeugt die gleiche Anzahl an Polarisationsschemata    Bsp.: x++x +x+x |  |  |
| Bitfolge wird anhand von Polarisationsschemata in Photonen kodiert und gesendet  Bsp.: \ | -- / | \ | / | 🡪 |  |
| Phase 2  (Bob wählt sein Polarisationsschemata) |  |  | Wählt seine eigenen Polarisationsschemata aus  Bsp.: ++xx xx++ |
|  |  | Empfängt Photonen, die über den Übertragungskanal übertragen wurden |
| Phase 3 | Teilt unverschlüsselt Polarisationsschemata mit  Bsp.: x++x +x+x | 🡪 |  |
|  |  | Vergleicht mit seinem gewählten Polarisationsschemata und streicht die Stellen, bei denen er ein falsches Polarisationsschema ausgewählt hat |
|  | 🡨 | Teilt Alice mit, an welchen Stellen er falsche Polarisationsschemata verwendet hat  Bsp.: ?+?x ?x+? |
| Streicht die Stellen, bei denen Bob das falsche Polarisationsschema benutzt hat  Bsp.: +xx+ | 🡨  🡪 | *Streicht die Stellen, bei denen er das falsche Polarisationsschema benutzt hat*  *Bsp.: +xx+* |
| Phase 4  (Wurde-abgehört?-Phase) | Frägt nach bestimmten Bits („0“ oder „1“ und Position) |  |  |
|  | 🡨 | Bob sendet die angeforderten Bits |
| Wenn alle Bits mit ihren übereinstimmen, wurde die Übertragung nicht abgehört |  |  |
| Phase 5 | Das ausgehandelte One-Time-Pad kann verwendet werden, um Nachrichten zu verschlüsseln | 🡪  🡨 | Das ausgehandelte One-Time-Pad kann verwendet werden, um Nachrichten zu verschlüsseln |

* Wahrscheinlichkeit, dass Bob die Bits richtig interpretiert: 75 %
* Wahrscheinlichkeit, dass Bob den richtigen Filter verwendet: 50 %
* Wahrscheinlichkeit, dass Eve nicht erwischt wird:

**Grundlegende Begriffe**

* rektilinear (**+**) vs. diagonaler (**x**) Filter
* (+) und (x) sind **Polarisationsschema (Polsch)**
* (+x++ x+x+) sind **Polarisationsschemata (Polscha)**
* (0) und (1) sind **Bit**
* (0011 0110) ist ein **Bitstrom**

**Übungsszenarien**

* Nutzer kann zwischen einzelnen Phasen, der Kombination aus mehreren (aufeinanderfolgenden) Phasen oder dem kompletten Ablauf auswählen
* Nutzer kann eine/mehrere/alle Rolle(n) auswählen
* Nutzer kann einen Schwierigkeitsgrad auswählen
* Nutzer wählt zwischen den Szenen aus

|  |  |  |
| --- | --- | --- |
| Szene | | |
| Normaler Ablauf | Sniffing | MITM |