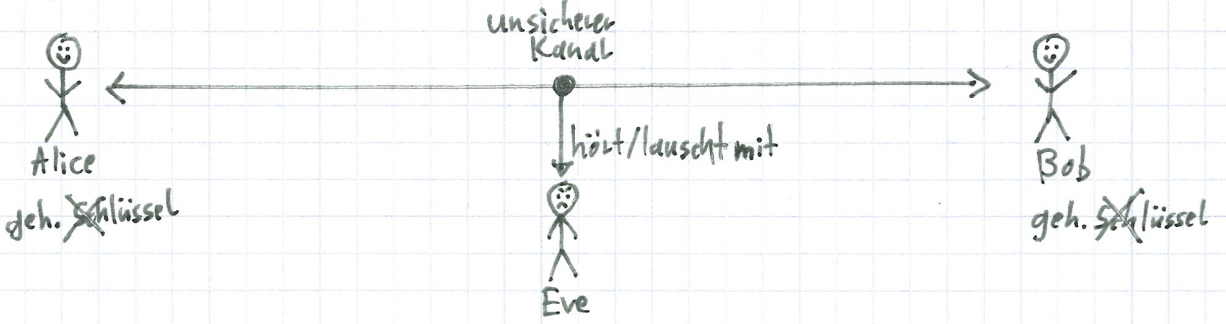
Eigenes „Gesamtbild" CRYPTO1 – „Überblick & Einführung" (VL vom 27.4.22) 14.5.22

Problem:



Unlösbar?! Ralph Merkle sagte 1974/78: Nein!
↳ „Secure Communications over Insecure Channels"

Vorschlag 1: Schlüssel raten (benötigt Einwegfunktion f)

Alice:	Bob:	Eve:
a_1 → $f(a_1)$ $f(a_2)$ ← a_2 a_3 → $f(a_3)$ $f(a_4)$ ← a_4 a_5 → $f(a_5)$ $f(a_6)$ ← a_6 ⋮ $f(a_{2j+1}) = f(a_{2i}) \Rightarrow a_{2j+1} = a_{2i}$ gemeins. Schlüssel		Eve hat: $f(a_1)$, $f(a_2)$, $f(a_3)$, ⋮ und $f(a_{2j+1}) = f(a_{2i})$, kennt aber nicht $a_{2j+1} = a_{2i}$. Dieses muss sie über Brute-Force herausfinden und hat dabei Aufwand $O(N)$.

Wenn $a_k \in [1, N]$, dann tritt nach $O(\sqrt{N})$ Schritten eine Kollision auf (Geburtstagsparadoxon). Der Aufwand von Alice & Bob beträgt also $O(\sqrt{N})$.

Vorschlag 2: Merkle-Puzzle

Alice:	Bob:	Eve:
Erstellt eine Menge von Rätseln und schickt diese an Bob: $R_1, R_2, R_3, R_4, R_5, \dots R_N$ Die Schwierigkeit eines Rätsels ist $O(N)$.	Wählt R_i und löst es: K_i	Eve hat: R_1, R_2, R_3, ⋮ und $f(K_i)$, kennt aber weder K_i noch i. Dieses muss sie über Brute-Force durch Lösen aller (im Schnitt der Hälfte aller) Rätsel herausfinden. Aufwand: $O(N^2)$
$f(K_i)$ → (gemeinsamer Schlüssel)		
Aufwand Alice: $O(N)$ zum Erstellen von N Rätseln.	Aufwand Bob: $O(N)$ zum Lösen eines Rätsels.	

„Rätsel" = mit symmetr. Verschlüsselg. verschlüsselt

Wichtige Details:
- Eine Einwegfunktion f ist nicht zwingend notwendig. Die Rätsel können auch in zufälliger Reihenfolge von Alice versendet und der Index mitverschlüsselt werden. Dann kann Bob den Index i im Klartext zurücksenden.
- Die Chiffrate müssen Redundanz enthalten, damit Bob sie erkennt.