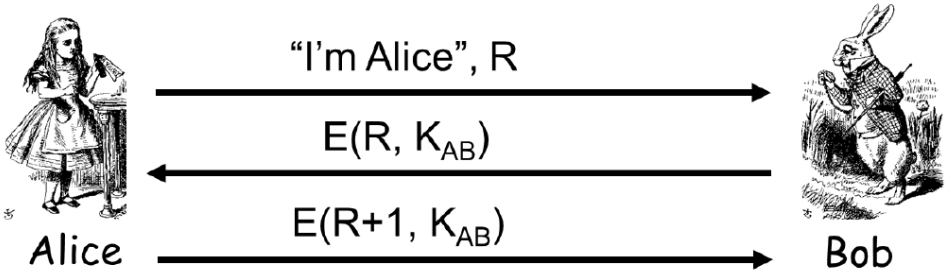
2. Aufgabe: Fehlerhaftes Authentisierungs-Protokoll

Betrachten Sie folgendes Mutual Authentication Protocol:

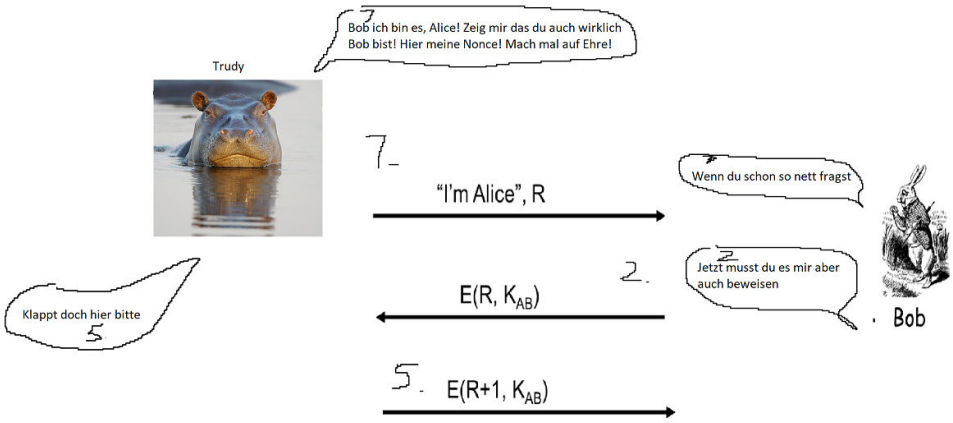


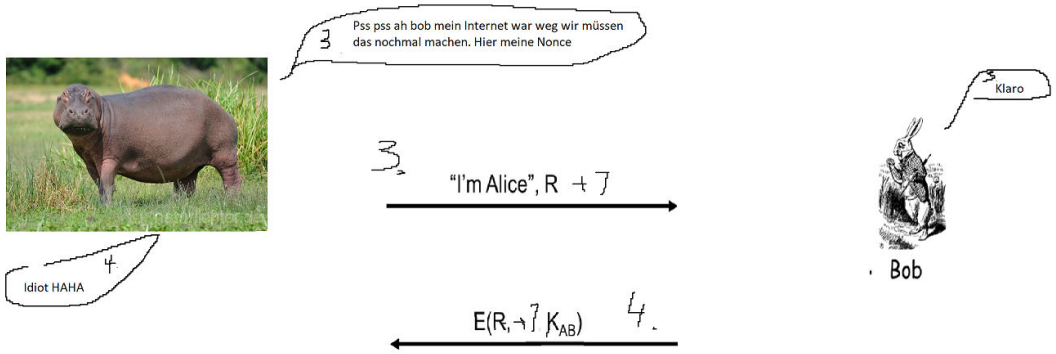
Erläuterungen: R ist eine Nonce. E ist eine symmetrische Verschlüsselungsfunktion. E(M, K) ist die mit dem Schlüssel K verschlüsselt Nachricht M. K_{AB} ist der gemeinsame symmetrische Schlüssel von Alice und Bob.

a) Nennen Sie zwei Angriffe auf das Protokoll, die Trudy ausführen kann, um Bob davon zu überzeugen, dass Sie Alice ist. Visualisieren Sie die Angriffe.
b) Wie könnten Sie das Protokoll abändern, um diesen Angriff zu verhindern?

a)

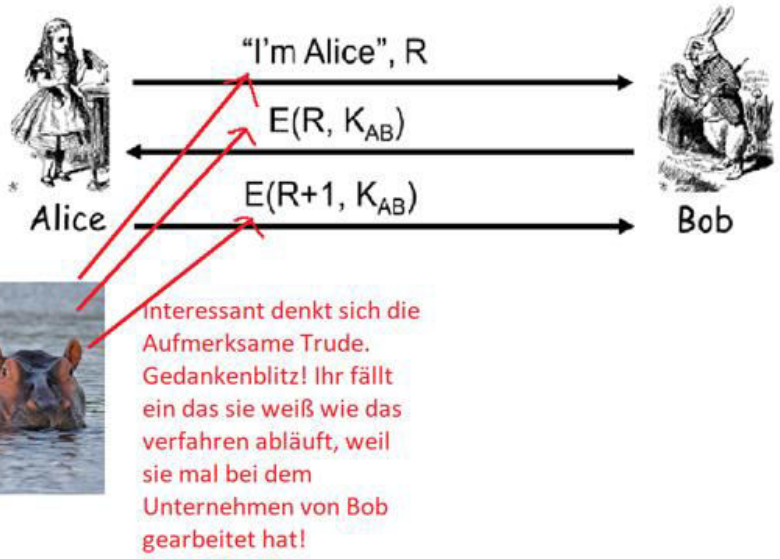
Spoofing, Maskerade: Vortäuschung falscher Identität
Mutual Authentifikation Attack

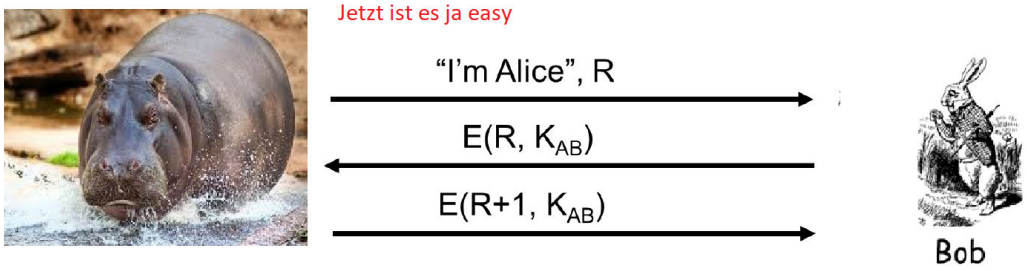




b) Wenn Bob seine eigene Nonce stellen würde und beide die Identität vom Absender mitschicken

Sniffing





B) Bob muss auch eine Nonce stellen. Im vergleich zu Alice ist die dann auch wirklich nur 1x in Nutzung, weil er das Ruder in der Hand hat, dann