

Warum reicht symmetrische Kryptographie nicht aus?

Mit AES verfügen wir also heutzutage über einen sehr sicheren Verschlüsselungsalgorithmus, der in zahlreichen modernen Geräten sehr performant in Hardware implementiert ist. Man könnte also meinen, dass wir keine weiteren Verschlüsselungsmechanismen mehr benötigen - wären da nicht ein paar kleiner Probleme....

Bob und Alice wollen sich unterhalten

Bob und Alice möchten gerne verschlüsselt kommunizieren, dazu möchten sie gerne als Verschlüsselungsverfahren AES verwenden. Aus diesem Grund schreibt Bob eine Mail an Alice:

Liebe Alice,

ich schlage vor, dass wir von nun an alle unsere Mails mit dem AES verschlüsseln.
Als Schlüssel verwenden wir AF651177 8176AFF1 FE7FD9EF A368BB5F.

Bob

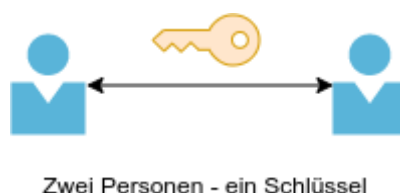


(A1)

Welche Probleme erkennst du bei diesem Vorgehen? Warum sollte man das keinesfalls so machen, wie Bob?

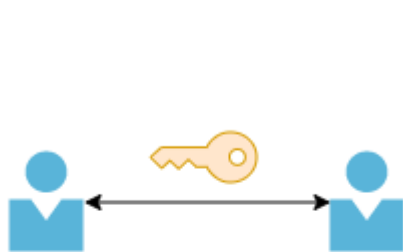
Die Klasse 8b möchte sich (verschlüsselt) unterhalten

Um ein symmetrisches Verschlüsselungsverfahren einzusetzen, müssen je zwei Teilnehmer einen gemeinsamen geheimen Schlüssel besitzen:

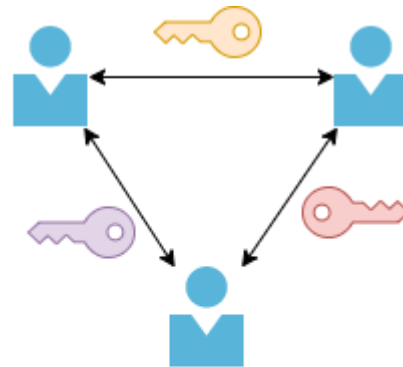


Wenn die Kommunikation jetzt innerhalb einer Gruppe von Personen erfolgen soll, steigt die Zahl der

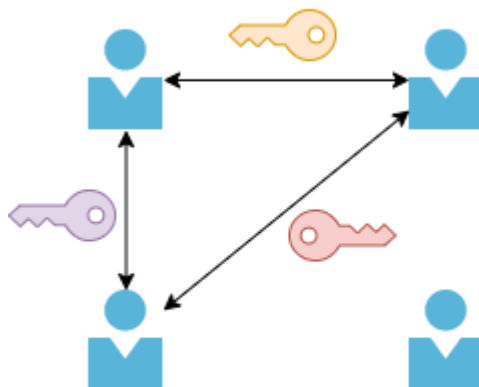
Schlüssel schnell an:



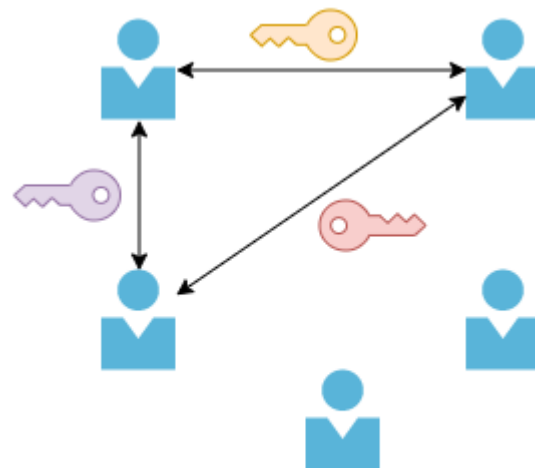
Zwei Personen - ein Schlüssel



Drei Personen - drei Schlüssel



Vier Personen - ?? Schlüssel



Fünf Personen - ?? Schlüssel

From:
<https://info-bw.de/> -

Permanent link:
https://info-bw.de/faecher:informatik:oberstufe:kryptographie:modell_asy:start?rev=1648649007

Last update: **30.03.2022 14:03**

