# 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 könnt 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?

From:
https://www.info-bw.de/ -

Permanent link:
**https://www.info-bw.de/faecher:informatik:oberstufe:kryptographie:modell_asy:start?rev=1648648368**

Last update: **30.03.2022 13:52**