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 kleinere 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:

(A2)

- Vervollständige die Schlüsselzahlen für die beiden letzten Diagramme (4 Personen/5 Personen)
- Kannst du eine Formel finden, wieviele Schlüssel für n Personen nötig sind?
- Wieviele Schlüssel sind nötig für die Kommunikation zwischen den 25 Schülerinnen der 8b?

Lösung

Siehe Metcalfesches_Gesetz.

Die in den Beispielen oben auftretenden Schwierigkeiten werden **Schlüsselvereinbarungsproblem** und **Schlüsselverteilungsproblem** genannt.

(A3)

Versuche für die beiden Begriffe **Schlüsselvereinbarungsproblem** und **Schlüsselverteilungsproblem** eine Definition zu finden. Die Definitionen sollten nicht länger als 2 bis 3 Sätze sein und als Merksatz dienen können.