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:

Jeder der Kommunikationspartner muss dabei alle Schlüssel derjenigen Personen haben, mit denen er verschlüsselt kommunizieren möchte - und man muss dann auch wissen, für welchen Adressaten man welchen Schlüssel verwenden muss!

(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?
- Stell dir vor, du bist einer der Schülerinnen der 8a. Wie viele Schlüssel würdest du besitzen? Welche Schwierigkeiten hast du, wenn du eine Nachricht an „Fritz Meyer“ schreiben möchtest.

Lösung

Siehe Metcalfesches_Gesetz.

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

(A3)

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

Lösungsansätze für das Schlüsselverteilungsproblem

- Man kann die Schlüssel bei einem persönlichen Treffen oder per Telefon (Out-of-Band-Schlüsselaustausch) austauschen. Bei einer Gruppe wird dieses Verfahren aus einsichtigen Gründen nicht gut auf größere Gruppengrößen skalieren.
- Die Kommunikationspartner verwenden einen Authentifizierungsserver: Dieser stattet jeweils zwei Kommunikationspartner mit einem gemeinsamen Schlüssel aus. Ein Beispiel dafür ist Kerberos.
- Man verwendet **asymmetrische Kryptografie** darum geht es in diesem Wikiabschnitt.