V. Schlüsselaustausch

Verschlüsselung und Authentifikation benötigen einen gemeinsamen geheimen Schlüssel:

V.1. 3-Pass

(Schlüssel-/Nachrichtenaustausch mit mittelalterlichen Mitteln)

FIXME: Bild 3-Pass oben, S. 14

Problem: Man-in-the-Middle-Angriff möglich (Bote befestigt eigenes Schloss, statt Kiste zu Bob zu bringen) → Abhilfe: z.B. schwer fälschbare Siegel auf dem Schloss

modernere Idee:

Nachrichtentransfer über authentifizierten, aber nicht abhörsicheren Kanals mittels OTP (One-Time-Pad):

FIXME: Bild 3-Pass unten, S. 14

Problem: das funktioniert so nicht, da

$$(M \oplus OTP\_Alice) \oplus (M \oplus OTP\_Alice \oplus OTP\_Bob) = OTP\_Bob$$

V.2. Wide-Mouth-Frog

FIXME: Bild Wide-Mouth-Frog, S. 15

Probleme:

- benötigt vertrauenswürdige Zentrale
- Zentrale zuständig für Verbindungsaufbau zu Bob → DoS-Attacke möglich
- Alice benötigt guten Zufallsgenerator

V.3. Kerberos

FIXME: Bild Kerberos, S. 15

1. $(\text{alice}, \text{bob})$
2. $(Enc_{k_{AZ}}(T_Z, L, K_{AB}, \text{bob}), Enc_{k_{BZ}}(T_Z, L, K_{AB}, \text{alice}))$

3. $(Enc_{k_{AB}}(\text{alice}, T_A), Enc_{k_{BZ}}(T_Z, L, K_{AB}, \text{alice}))$
4. $Enc_{k_{AB}}(T_A + 1)$

Probleme:

- benötigt synchrone Uhren
- Chiffre muss non-malleable[1] sein, sonst evtl. $Enc_{T_{AB}}(T_A{+}1)$ aus $Enc_{T_{AB}}(T_A)$ berechenbar $\rightarrow$ Confidentiality $\not\Rightarrow$ Non-Malleability!

Die ältere Variante Needham-Schroeder hatte noch keine Zeitstempel, sondern Zufallszahlen. $\rightarrow$ Replay-Attacken möglich (z.B. Alice ist eine Kamera und der Angreifer spielt alte Aufnahmen wieder ein)

V.4. Merkle Puzzle

Alice wählt zufällig k Paare von Schlüssel und zufälliger Schlüsselnummer und verschlüsselt die Paare mit einer symmetrischen Chiffre mit immer neuem Schlüssel. Sie schickt alles an Bob zusammen mit genügend Hinweisen, sodass Bob jedes der verschlüsselten Paare „brechen“ kann. Bob entschlüsselt eines der Paare und antwortet Alice mit der Schlüsselnummer des von ihm gebrochenen Paares und die beiden kennen nun einen gemeinsamen Schlüssel.
Der „Vorteil“ von Alice und Bob gegenüber einem Lauscher ist leider nur gering (quadratisch).

V.5. Diffie-Hellman-Schlüsselaustausch (DH)

Seien eine (öffentlich bekannte) Gruppe G sowie ein Erzeuger g dieser Gruppe gegeben[2] (z.B. $\mathbb{F}_p^\times, p \in \mathbb{P}$ oder eine Gruppe auf einer Elliptischen Kurve):

FIXME: Bild DH, S. 16

Diffie-Hellman ist (beweisbar) sicher relativ zur Decisional-Diffie-Hellman-Annahme.

V.5.1. Decisional-Diffie-Hellman-Annahme

Asymptotisch ist es nicht in Polynomialzeit möglich, folgende Verteilungen zu unterscheiden: (g, g^a, g^b, g^{ab}) und (g, g^a, g^b, g^c) mit a, b, c zufällig.

V.5.2. Man-in-the-Middle-Angriff

FIXME: Bild Man-in-the-Middle-Angriff, S. 17

Verhindern von Man-in-the-Middle-Angriffen:

- symmetrische Authentifikation (s. IV.6) mit einem Langzeitgeheimnis
- digitale Signaturen (s. VII)

[1] aus einem Chiffrat darf sich kein anderes gültiges berechnen lassen
[2] hier muss der diskrete Logarithmus schwierig zu berechnen sein!