Institut für Betriebssysteme und Rechnerverbund

Übungen zur Vorlesung "Verteilte Systeme", WS 02/03

http://www.ibr.cs.tu-bs.de/lehre/ws0203/vs/

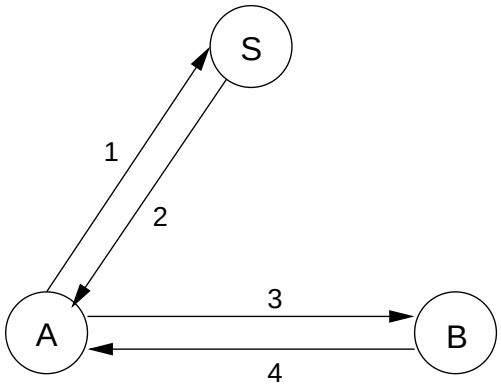
Dozent: Prof. Dr. Stefan Fischer <fischer@ibr.cs.tu-bs.de> · Übungsleiter: Frank Strauß <strauss@ibr.cs.tu-bs.de>

11 Sicherheit — Übung am 22.01.2003

11.1 Schlüsselverteilung — Kerberos

Ein verbreitetes Protokoll zur Verteilung symmetrischer Sitzungsschlüssel (vgl. Folie 10-33) ist der entsprechende Bestandteil des Authentifizierungsdienstes *Kerberos*, der am MIT entwickelt wurde und in vielen Systemen heutzutage eingesetzt wird. Das hier beschriebene vereinfachte Protokoll wurde in der Kerberos Version 4 benutzt. Die aktuelle Version von Kerberos benutzt eine verbesserte Variante des Protokolls.

Das Protokoll geht von zwei Parteien A und B aus, die jeweils einen geheimen Schlüssel K_{as} und K_{bs} mit einem Authentifizierungsserver S teilen.



Nachricht 1: $A \rightarrow S: \quad A, B$
Nachricht 2: $S \rightarrow A: \quad \{T_s, L, K_{ab}, B, \{T_s, L, K_{ab}, A\}_{K_{bs}}\}_{K_{as}}$
Nachricht 3: $A \rightarrow B: \quad \{T_s, L, K_{ab}, A\}_{K_{bs}}, \{A, T_a\}_{K_{ab}}$
Nachricht 4: $B \rightarrow A: \quad \{T_a + 1\}_{K_{ab}}$

- Die Partei A sendet die erste Nachricht an den Server S um den Authentifizierungsvorgang einzuleiten.
- Der Server S erzeugt daraufhin den Sitzungsschlüssel K_{ab} und verschlüsselt mit K_{bs} unter Verwendung eines Zeitstempels T_s und einer Lebensdauer L das Ticket $\{T_s, L, K_{ab}, A\}_{K_{bs}}$, mit dem A eine Authentifizierung mit B innerhalb der Gültigkeitsdauer durchführen kann.
- Anschließend verschlüsselt S die zweite Nachricht mit K_{as} und sendet sie an A.
- Die Partei A merkt sich die zweite Nachricht, um damit eine Authentifizierung mit B innerhalb der Gültigkeitsdauer beliebig oft durchführen zu können.
- Nun generiert A die dritte Nachricht, die sich aus dem von S erhaltenen Ticket und dem Authentifizierer $\{A, T_a\}_{K_{ab}}$ zusammensetzt, und sendet sie an B.

- Die Partei B entschlüsselt zunächst das Ticket mit K_{bs} und überprüft mit dem Zeitstempel T_s und der Lebensdauer L, ob das Ticket noch gültig ist.
- Ist das Ticket gültig, so entnimmt B dem Ticket den Sitzungsschlüssel K_{ab}. Damit entschlüsselt B den Authentifizierer in der dritten Nachricht.
- Anschließend erzeugt B die vierte Nachricht, die den um eins erhöhten Zeitstempel aus dem zuvor empfangenen Authentifizierer enthält, und sendet sie an A.
- Die Partei A entschlüsselt die vierte Nachricht und überprüft $T_a + 1$, um festzustellen, ob B im Besitz des Sitzungsschlüssels K_{ab} ist.

(a) Wozu benutzt man überhaupt einen Schlüsselverteilungsdienst, wenn im obigen Schema sogar zwei Schlüssel (K_{as} und K_{bs}) statt nur einfach einem K_{ab} vorausgesetzt werden?

(b) Wozu dienen Zeitstempel und Lebensdauer im Kerberos Protokoll?

(c) Worin könnte im Zusammenhang damit eine "Angriffsvereinfachung" bestehen?

(d) Warum wird im letzten Schritt $T_a + 1$ und nicht T_a verschlüsselt an A zurück übermittelt?

11.2 Anwendung — PGP (Pretty Good Privacy)

Um die drei Ziele *Vetraulichkeit*, *Integrität* und *Authentizität* im Austausch und bei der Speicherung von Daten zu erreichen, kann man PGP (Pretty Good Privacy) verwenden.

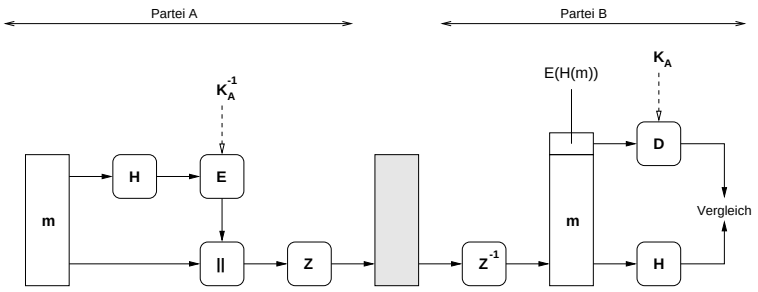
Die "Bausteine" von Kryptosystemen sind

- *Einweg-Hash-Funktionen* (z.B. MD5, SHA-1),
- *symmetrische Chiffren* mit einem geheimen Schlüssel (z.B. DES, IDEA, AES), und
- *asymmetrische Chiffren* mit einem Paar aus privatem und öffentlichem Schlüssel (z.B. RSA)

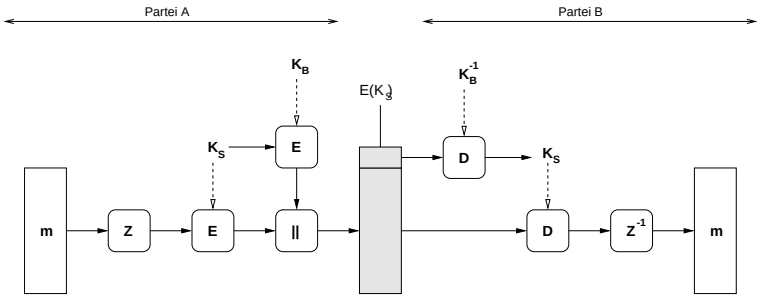
PGP bedient sich dieser Bausteine, um die zwei wichtigsten Anwendungen von PGP zu realisieren: *Verschlüsselung* und *Signatur*. Diese wollen wir uns anhand der folgenden Diagramme veranschaulichen.

A, B	Parteien A und B
m	Original-Nachricht
H	Hash-Funktion
E, D	Verschlüsselung, Entschlüsselung
$\|\|$	Konkatenation
Z, Z^{-1}	Komprimierung, Dekomprimierung
K_A, K_B	Öffentliche Schlüssel von A und B
K_S	Sitzungsschlüssel
K_A^{-1}, K_B^{-1}	Private Schlüssel von A und B

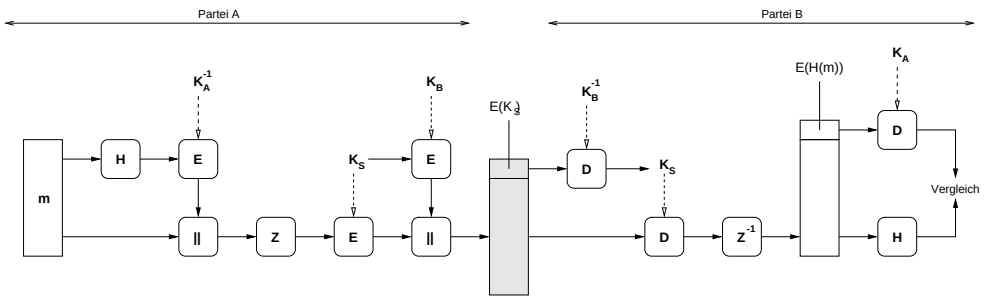
Signatur



Verschlüsselung



Signatur und Verschlüsselung



Frage: Warum benutzt man zur Verschlüsselung der Nachricht m den extra generierten symmetrischen Schlüssel K_S und nicht einfach den öffentlichen Schlüssel K_B von Partei B?

11.3 Verteilung und Vertrauenswürdigkeit von öffentlichen Schlüsseln

- Woher bekommt Partei A den öffentlichen Schlüssel von Partei B?
- Welche Gefahren bestehen, wenn Partei A nicht sicher sein kann, dass der angebliche öffentliche Schlüssel von B auch wirklich zu B gehört?
- Wozu dient im Zusammenhang mit dieser Problematik die Signatur von öffentlichen Schlüsseln (Zertifikate)?
- Die Beziehungen zwischen sich zertifizierenden Parteien können hierarchisch strukturiert (Zertifizierungshierarchie bestehend aus *Certification Authorities*) oder auch beliebig (bei PGP typisch: *Web of Trust*) sein. Welche Konsequenzen entstehen aus diesen Strukturen?