12 Anwedungen kryptographischer Algorithmen

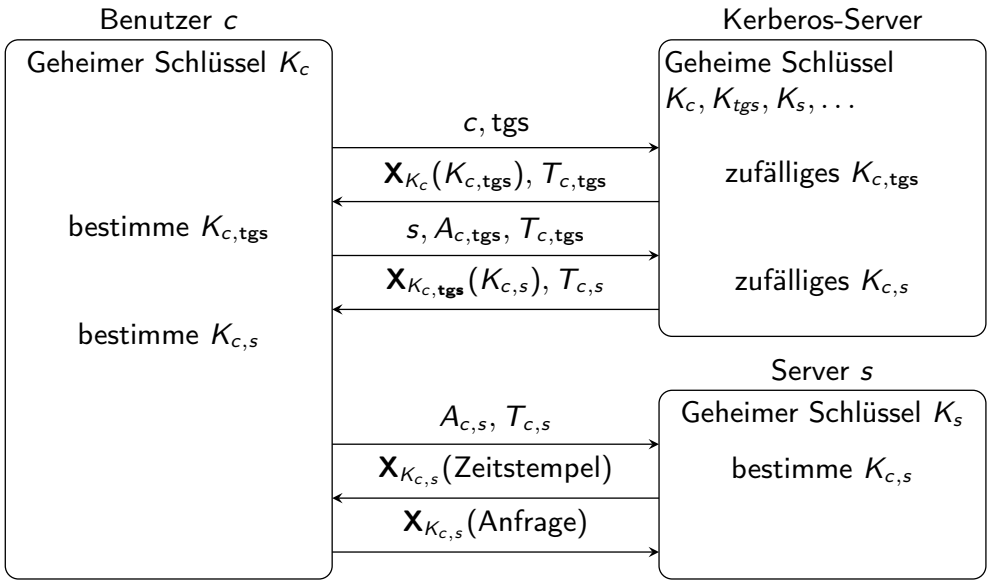
12.1 Secure Socket Layer/Transport Layer Security

- Protokollschicht zur sicheren Netzwerkkommunikation
- Einsatz insbesondere für WWW (https), aber auch Email (smtp/imaps) und andere Dienste
- Server wird über Zertifikate authentifiziert, signiert mit RSA oder DSA (Digital Signature Algorithm, Sicherheit über diskreten Algorithmus)
- RSA oder Diffie-Hellman wird verwendet, um Sitzungsschlüssel zu vereinbaren
- eigentliche Kommunikation mit DES, 3DES, RC4 oder AES im CBC-Modus

12.2 Kerberos

- Netzwerk-Authentifikations-Protokoll
- Einsatz u.a. in Microsoft Active Directory
- aus Benutzername + Passwort wird Hash gebildet und als geheimer Schlüssel verwendet
- bei Anmeldung wird ein Ticket-Granting-Ticket vom Kerberos-Server ausgestellt
- alle weiteren Zugriffe auf Server mit Tickets und Sitzungsschlüsseln; Passwort bzw. geheimer Schlüssel muss auf Client nicht gespeichert werden
- Verschlüsselung mit DES oder AES

Anmeldung von Benutzer c und Zugriff auf Server s:



tgs: Ticket Granting Service

$T_{c,s}$: $\mathbf{X}_{K_s}(c, K_{c,s}, \text{Geltungsdauer})$

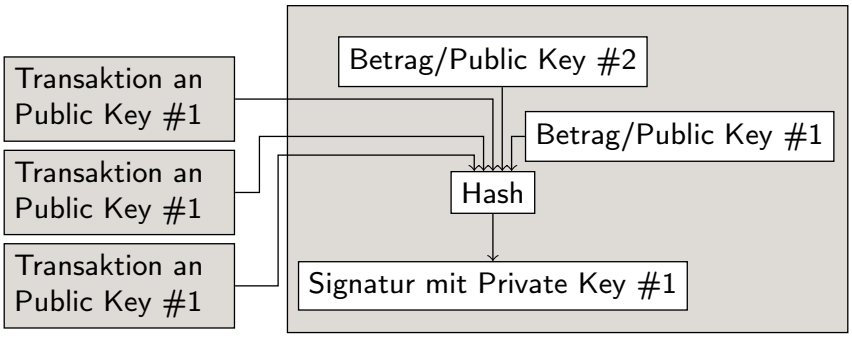
$A_{c,s}$: $\mathbf{X}_{K_{c,s}}(c, \text{Zeitstempel})$

12.3 DVB Conditional Access

- Digital Video Broadcast erlaubt Senden verschlüsselter Video-Datenströme
- proprietäre Verschlüsselung (Content Scrambling Algorithm), Kombination von Block- und Stromchiffre
- 64 bit Schlüssel (Kontrollwort), wird häufig gewechselt ($\approx$ Minuten)
- jeweils gültiges Kontrollwort wird über Entitlement Control Messages (ECM) an Empfänger gesendet
- SmartCard im Empfänger kann aus den ECMs das Kontrollwort bestimmen
- Entitlement Management Messages (EMM) können einzelne SmartCards gezielt aktivieren/deaktivieren
- Details zu ECMs und EMMs unterscheiden sich zwischen Anbietern und sind nicht öffentlich

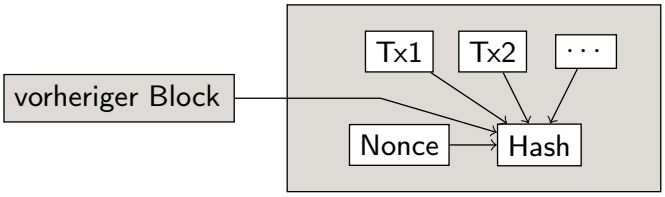
12.4 Bitcoin

- Digitale Währung, krytographisch abgesichert
- Transaktionen erfolgen zwischen asymmetrischen Schlüssel-Paaren
  - Sender/Empfänger durch öffentliche Schlüssel identifiziert
  - Transaktion durch Signatur mit geheimem Schlüssel des Senders bestätigt



- Mehrere Quell-Transaktionen; gesamter Betrag der Transaktion = Summe der Quell-Beträge
- Mehrere Empfänger; in der Regel "Wechselgeld" an Auftraggeber
- Problem: Sicherstellen, dass jede Transaktion nur einmal als Quell-Transaktion verwendet wird (kein "double-spending")

- "double-spending" wird verhindert, wenn
  - alle Teilnehmer alle Transaktionen kennen – skaliert nicht
  - eine zentrale Instanz alle Transkationen kennt und überwacht – Bitcoin-Erfinder wollte dezentrales System
- Lösung: viele verteilte Knoten kontrollieren Transaktionen und bestätigen in Blöcken



- Nonce wird so gesucht, dass Hash mit bestimmer Zahl an Null-Bits beginnt (Rechenaufwand!)
- Knoten, der passende Nonce findet, veröffentlicht neuen Block
- andere Knoten nutzen diesen nach Kontrolle als Basis für nächsten Block
- längste so gebildete Block-Kette ist die gültige
- Transaktion ist unumkehrbar bestätigt, wenn in Block-Kette aufgenommen
- Angreifer müsste mehr Rechenleistung als alle anderen Knoten zusammen haben, um Block-Kette mit gefälschten Transaktionen zu erzeugen, die länger ist als andere
- Belohnung für Knoten: "geschürfte" Bitcoins oder Transaktionsgebühren für jede gefundene Nonce