technische universität
dortmund

Sicherheit: Fragen und Lösungsansätze

Thomas Ruhroth

Übung 5

- HA 4
- HA 5
- Wissenslücken füllen

HA4

Aufgabe 1.1

- Programmierstil
  - Sprechende Variablennamen
  - Große Case-Blöcke
    - Keine Sprungvorhersage möglich
    - Werte lassen sich einfach berechnen
  - Stringbuffer verwenden
    - Effiziente innere Umsetzung
    - Weniger „tote Objekte“
      - Müssen nicht vom GC aufgesammelt werden
  - Häufiger ?: statt if
    - Direkte Unterstützung im Bytecode und im Assembler (JIT)

Aufgabe 1.2-4 - Hash1

- One-Way-Eigenschaft
  - Ja, zu jedem Hash gibt es eine Vielzahl von Eingaben, die diesen Hash erzeugen. Wegen dem Informationsverlust (Reihenfolge, Groß/kleinschreibung, etc) kann die Nachricht nicht aus dem Hash geschlossen werden.
- Kollisionsresistenz
  - (Strings, Deutsch) Weder schwach noch stark kollisionsresistent
  - Zu jeden Nachricht kann durch Vertauschen der Buchstaben (bzw. Wörter) eine neue Nachricht mit gleichem Hashwert erstellt werden
  - (Shakespeare-Sonette) Da es keine zwei Sonette mit den gleichen Buchstabenanzahlen gibt, ist Hash1 hier sowohl schwach noch stark kollisionsresistent
- Werte:
  - Sicherheit: Fragen und Loesungsansaetze 30116122200104100242200001
  - Dies ist ein Beispiel für eine kryptographische Hash-Funktion. 21117313802104220353100010
  - SFL 100000100000010000000

Aufgabe 1.2-4 - Hash2

- One-Way-Eigenschaft
  - Ja, zu jedem Hash gibt es eine Vielzahl von Eingaben, die diesen Hash erzeugen. Wegen dem Informationsverlust (Reihenfolge, Groß/kleinschreibung, etc) kann die Nachricht nicht aus dem Hash geschlossen werden.
- Kollisionsresistenz
  - (Strings, Deutsch) Weder schwach noch stark kollisionsresistent
  - Anhängen oder weglassen von Zeichen im letzten unvollständigen Block
  - (Shakespeare-Sonette) Sowohl schwach noch stark kollisionsresistent
- Werte:
  - Sicherheit: Fragen und Loesungsansaetze 8342
  - Dies ist ein Beispiel für eine kryptographische Hash-Funktion. 786451
  - SFL – nichts

Aufgabe 1.2-4 - Hash3

- One-Way-Eigenschaft
  - Nein, es handelt sich um die Cäsar-Verschlüsselung. Hierfür gibt es eine einfach zu berechnende Umkehrfunktion.
- Kollisionsresistenz
  - (Strings, Deutsch,Shakespeare-Sonette) Sowohl schwach noch stark kollisionsresistent – es gibt keine Kollisionen da die Funktion umkehrbar ist
- Werte:
  - Sicherheit: Fragen und Loesungsansaetze
    Vlfkhukhlw: Iudjhq xqg Orhvxqjvdqvdhwch
  - Dies ist ein Beispiel für eine kryptographische Hash-Funktion.
    Glhv lvw hlq Ehlvslo iüu hlqh nubswrjudilvfkh Kdvk-Ixqnrq.
  - SFL
    VIO

Aufgabe 2

Schritte	Teilnehmer A	Teilnehmer B
Wähle geheimen Schlüssel	$K_{priv\_A} \in \{2,...,q-2\}$	$K_{priv\_B} \in \{2,...,q-2\}$
Berechne öffentlichen Schlüssel und	$K_{pub\_A} = (\alpha^{K_{priv\_A}}) \bmod q$	$K_{pub\_B} = (\alpha^{K_{priv\_B}}) \bmod q$
tausche ihn aus		
Berechne **gemeinsamen** Schlüssel K_{AB}	$K_{AB} = (K_{pub\_B}^{K_{priv\_A}}) \bmod q$	$K_{AB} = (K_{pub\_A}^{K_{priv\_B}}) \bmod q$
Angreifer: Welche Kentnisse?	Aufwand K_{AB} Problem:	zu berechnen? Man-In-The-Middle

Aufgabe 2.1

- P = 19, a = 3
- K_{priv_A}=11
- K_{pub_B}=14
- $K_{BA} = 14^{11} \bmod 19 = 13$

Aufgabe 2.2

- P = 19, a = 3
- $K_{priv\_A}=11$
- $K_{pub\_B}=14$
- $K_{priv\_C}=17$

- $K_{?} = 2$

- Lösung: C und A kommunizieren

- $K_{pub\_A}=3^{11} \bmod 19 = 10$
- $K_{pub\_B}=14$
- $K_{pub\_C}=3^{17} \bmod 19 = 13$
- $K_{BC}= 14^{17} \bmod 19 = 15$
- $K_{AC}= 10^{17} \bmod 19 = 2$

HA 5

Aufgabe 1 I a

- n =
  p*q = 19*29
  = 551
- v
  = s^2 mod n = 1337^2 mod 551
  = 125
  sind zu übermitteln

Aufgabe 1 I b-c

Bobs Anfragen

- $r1 = 7 \Rightarrow x1 = 7^2 \mod 551 = 49$
- $r2 = 23 \Rightarrow x2 = 23^2 \mod 551 = 529$
- $r3 = 30 \Rightarrow x3 = 30^2 \mod 551 = 349$
- $r4 = 550 \Rightarrow x4 = 550^2 \mod 551 = 1$

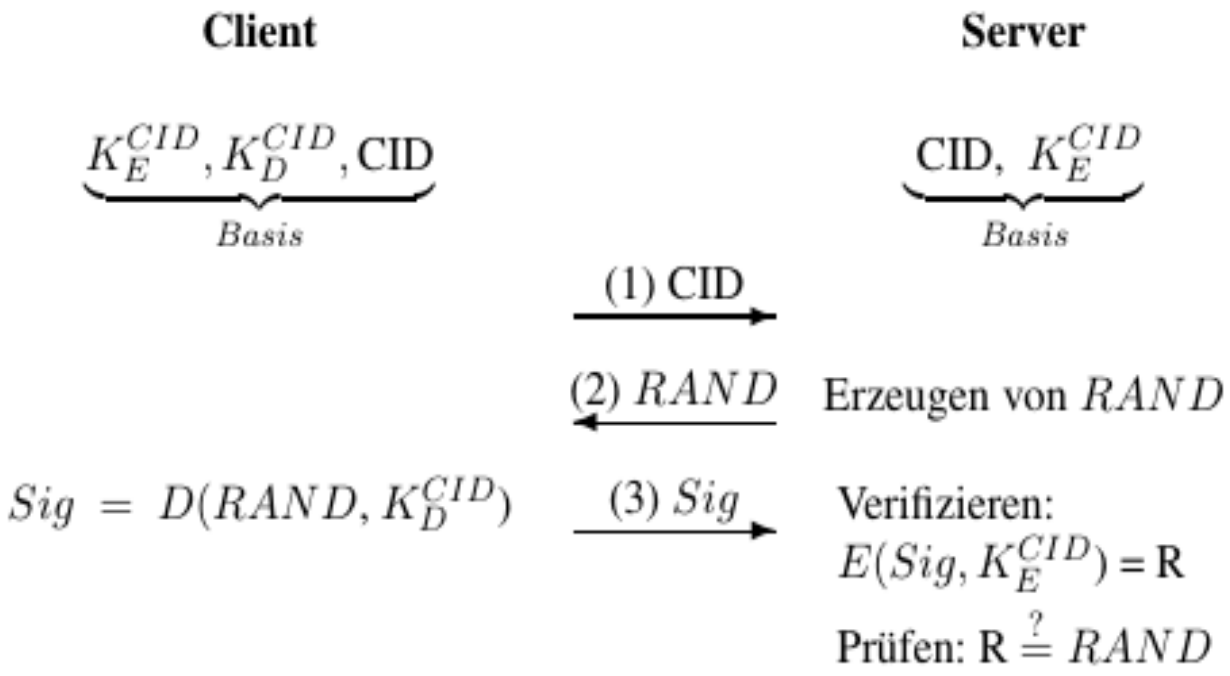
Alices Antworten

- $r1 = 7 \Rightarrow y1 = 1337 * 7 \mod 551 = 543$
- $r2 = 23 \Rightarrow y2 = 1337 * 23 \mod 551 = 446$
- $r3 = 30 \Rightarrow y3 = 1337 * 30 \mod 551 = 438$
- $r4 = 550 \Rightarrow y4 = 1337 * 550 \mod 551 = 316$

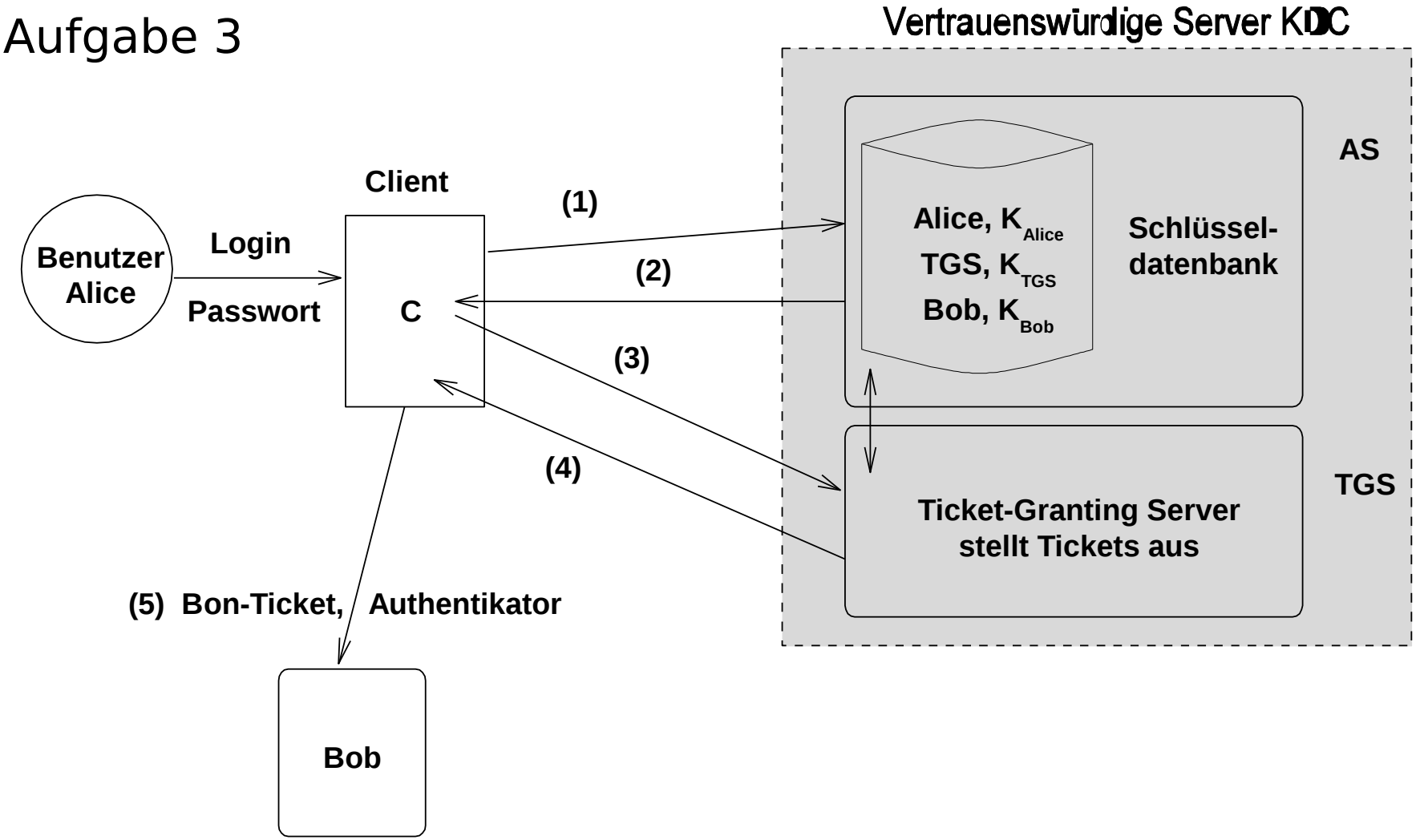
Aufgabe 1 II a - c

- Glaubwürdig
  - (900*653) mod 1111 = 1092= 149^2 mod 1111
- Glaubwürdig
  - 529=78^2 mod 1111
- Unglaubwürdig
  - (308*953) mod 1111 = 33
  - 808^2 mod 1111 = 707
  - Werte nicht gleich!
- Deshalb glaubt sie nun, dass Bob das Geheimnis nicht kennt.

Aufgabe 2


Client
Server
$\underbrace{K_E^{CID}, K_D^{CID}, \text{CID}}_{Basis}$
$\underbrace{\text{CID},\ K_E^{CID}}_{Basis}$
(1) CID
(2) $RAND$
Erzeugen von $RAND$
$Sig = D(RAND, K_D^{CID})$
(3) Sig
Verifizieren:
$E(Sig, K_E^{CID}) = \text{R}$
Prüfen: $\text{R} \stackrel{?}{=} RAND$

Aufgabe 3


Vertrauenswürdige Server KDC
AS
Alice, K Alice
TGS, K TGS
Bob, K Bob
Schlüssel-
datenbank
TGS
Ticket-Granting Server
stellt Tickets aus
Client
Benutzer
Alice
Login
Passwort
C
(1)
(2)
(3)
(4)
(5) Bon-Ticket, Authentikator
Bob

	Von	An	Nachricht
1.	Client	KDC	Alice, TGS, *Nonce*1, E([Alice, Time]), K_{Alice})
2.	KDC	Client	E([$K_{Alice,TGS}$, *Nonce*1], K_{Alice}), E($T_{Alice,TGS}$, K_{TGS})
3.	Client	TGS	E(A_{Alice}, $K_{Alice,TGS}$) E($T_{Alice,TGS}$, K_{TGS}) Bob, *Nonce*2
4.	TGS	Client	E([$K_{Alice,Bob}$, *Nonce*2], $K_{Alice,TGS}$) E($T_{Alice,Bob}$, K_{Bob})
5.	Client	Bob	E(A_{Alice}, $K_{Alice,Bob}$), E($T_{Alice,Bob}$, K_{Bob})

Aufgabe 3b

- Sie versucht sich beim KDC als Bob ein Ticket ausstellen zu lassen, welches dieser ablehnt.
- Sie lässt sich vom KDC ein Ticket als Eva ausstellen, was Alice merkt, sobald sie dieses entschlüsselt.
- Sie gibt vor, vom KDC ein Ticket erhalten zu haben, und sendet Alice ein gefälschtes Ticket. Diese kann das Ticket nicht mit ihrem Schlüssel K_{Alice} entschlüsseln, und identifiziert es so als Fälschung.
- ...
- Angriffe gegen den Client
- ...

Lückenabfrage

- Bitte auf einen Zettel eine Wissenslückenfrage.
- Die Frage sollte nicht zu generisch sein.
- Antwort sollte in wenigen Minuten gegeben werden können.

Fragenverlosung!

- Ein Jeder eine Frage
- 5 Min Vorbereitungszeit

Themenbeziehungen

- Erstellen Sie einen Graph mit den Themen der (bisherigen) Themen der Vorlesung als Knoten.
- Die Kanten sollen Beziehungen zwischen den Themen darstellen.
- Welche Kantentypen benötigen Sie?