technische universität
dortmund

Fakultät für Informatik
Lehrstuhl 4

Dipl.-Math. Dipl.-Inform. Ingo Schulz
Dipl.-Inform. Christoph Borchert

Wintersemester 2011/12

Rechnernetze und verteilte Systeme
Übungsblatt 13

Ausgabe: 23. Januar, **Besprechung:** 31. Januar - 3. Februar, **keine Abgabe**

Aufgabe 13.1

Die beiden Parteien A und B haben jeweils einen privaten und einen zugehörigen öffentlichen Schlüssel $k_{A_{\text{secr}}}$, $k_{A_{\text{öff}}}$, $k_{B_{\text{secr}}}$, $k_{B_{\text{öff}}}$. Die öffentlichen Schlüssel sind allen Partnern bekannt. Beide Parteien können für jeweils eine Nachrichtenübertragung durch einen Zufallsgenerator symmetrische Schlüssel k_{sess} erzeugen. „$[X]_k$“ stehe für die Nachricht, die durch Verschlüsselung von X mit dem Schlüssel k entsteht.

Gehen Sie davon aus dass die Nachrichten

i) sehr kurz oder

ii) lang

sind.

Entwerfen Sie Nachrichten zur Übertragung des Datums D von A nach B, welche die folgenden Ziele gewährleisten:

a) B soll sicher sein können, dass die Nachricht authentisch und unverfälscht ist.

b) A soll sicher sein können, dass nur B diese Nachricht entziffern kann.

c) B soll sicher sein können, dass die Nachricht authentisch und unverfälscht ist und dass sie nicht von einem Angreifer unbemerkt eingeschleust werden kann.