Tutoriumsblatt 9

Diskussion: 13. + 14. Juli 2021

Aufgabe 9.1: Symmetrische und asymmetrische Verschlüsselung

a) Nennen und erläutern Sie einen *wichtigen Unterschied* zwischen *symmetrischen* und *asymmetrischen* Verfahren.

b) Angenommen, N Personen wollen paarweise mittels symmetrischer Verschlüsselung kommunizieren. Alle Kommunikationspartner können die ausgetauschen, verschlüsselten Nachrichten mitlesen, aber keiner außer den zwei kommunizierenden Personen soll in der Lage sein, die mitgelesene Kommunikation zu entschlüsseln.

   (i) *Wie viele Schlüssel werden benötigt?*

   (ii) Nehmen Sie nun an, dass *asymmetrische Verschlüsselung* genutzt wird. *Wie viele Schlüssel werden benötigt?*

c) Warum verwenden die meisten Protokolle *sowohl symmetrische als auch asymmetrische* Verfahren?

d) Was ist ein *Man-in-the-Middle-Angriff (MITM)*? Kann dieser Angriff durchgeführt werden, wenn *symmetrische Schlüssel* benutzt werden?

e) Gegeben sei RSA mit $p = 5$ und $q = 13$.

   i) Was sind n und $\varphi(n)$?

   ii) Sei $e = 5$. Warum ist dies eine *gute* Wahl?

   iii) *Finden* Sie ein d, so dass $d \cdot e = 1 \mod \varphi(n)$.

   iv) *Verschlüsseln* Sie die Nachricht $m = 8$ mit dem Schlüssel $\langle e, n \rangle$.

Aufgabe 9.2: Diffie-Hellman

a) Zur gesicherten Kommunikation wollen Alice und Bob einen geheimen Schlüssel vereinbaren. Sie verwenden den Algorithmus von Diffie-Hellman mit den Parametern $p = 31$ und $g = 15$; diese Parameter sind Alice und Bob bereits bekannt. Als Geheimzahl generiere Alice die Zahl 3, Bob die Zahl 4.

   Berechnen Sie den geheimen Schlüssel unter Verwendung des Algorithmus' von Diffie-Hellman. Geben Sie als Lösung an, welche Operationen/Berechnungen Alice und Bob jeweils ausführen und welche Informationen an den jeweiligen Kommunikationspartner übermittelt werden.

b) Die Wahl der Werte in Teil a) war nicht optimal – einer der Werte macht es einem Angreifer einfacher, den geheimen Schlüssel zu ermitteln. *Welcher der Werte war schlecht gewählt, und welche Probleme verursacht diese Wahl?*

   Anmerkung: dass alle Werte zu klein sind, ist hier nicht gemeint.

Aufgabe 9.3: Schlüsselvereinbarung

In der Vorlesung wurde der Diffie-Hellman-Algorithmus vorgestellt, mit dessen Hilfe zwei Parteien sich auf einen geheimen, gemeinsamen Schlüssel einigen können. In dieser Aufgabe soll jetzt alternativ ein sehr einfaches Protokoll zum Austausch geheimer Schlüssel bezüglich seiner Sicherheit analysiert werden. Das Protokoll arbeitet wie folgt ($\oplus$ steht für die XOR-Verknüpfung):

i) Alice wählt zufällig $k, a \in \{0,1\}^n$ und sendet $s = k \oplus a$ an Bob.

ii) Bob wählt eine Zufallszahl $b \in \{0,1\}^n$ aus und sendet $u = s \oplus b$ an Alice.

iii) Alice berechnet $w = u \oplus a$ und sendet w an Bob.

iv) Alice benutzt k und Bob $w \oplus b$ als geheimen Schlüssel.

Beantworten Sie nun folgende Fragen:

a) Zeigen Sie, dass Alice und Bob im Besitz des gleichen Schlüssels sind.

b) Bietet das Protokoll einen sicheren Schlüsselaustausch, falls ein Angreifer die Nachrichten zwar mitlesen, aber nicht modifizieren kann? Begründen Sie Ihre Antwort.