12.05.2021

Dr. Felix Heuer
fheuer.lba@fh-salzburg.ac.at

Kryptographie und Mediensicherheit

Sommersemester 2021

Übungszettel 5

Abgabe: 25.05.2021 vor der Vorlesung

Bei allen Aufgaben, bei denen Sie etwas von Hand durchrechnen sollen, können Sie natürlich trotzdem einen Rechner verwenden, ich möchte die Rechenschritte von Ihnen nur gerne auf Papier sehen.

1 DH Schlüsselaustausch (10 Punkte)

In dieser Aufgabe sollen Sie einen DH Schlüsselaustausch von Alice und Bob per Hand durchrechnen. Alice und Bob verwenden dazu die zyklische Gruppe

$$\mathbb{Z}_{23}^* = \{1, 2, \ldots, 22\} \text{ mit der Multiplikation } .$$

a) Rechnen Sie zunächst nach, dass 5 ein Generator der Gruppe $\mathbb{Z}_{23}^*$ ist.

b) Alice zieht sich nun zufällig einen Exponenten $\texttt{x} \leftarrow \mathbb{Z}_{23}^*$ und erhält $\texttt{x} = \texttt{17}$. Bob zieht sich ebenfalls zufällig einen Exponenten $\texttt{y} \leftarrow \mathbb{Z}_{23}^*$ und erhält $\texttt{y} = \texttt{3}$. Rechen Sie die Werte aus, die Alice und Bob miteinander austauschen werden.

c) Alice und Bob haben nun ihre Werte ausgetauscht. Leiten Sie für Alice und Bob jeweils den gemeinsamen Schlüssel ab.

2 Angriff auf DH Schlüsselaustausch (10 Punkte)

Eve hat Alice und Bob belauscht und weiß, dass sie für ihren DH Schlüsselaustausch die Gruppe

$$\mathbb{Z}_{12345701}^* = \{1, \ldots, 12345700\} \text{ mit der Multiplikation}$$

verwenden. Allerdings haben Alice und Bob den verwendeten Generator der Gruppe nicht öffentlich ausgetauscht, es ist aber bekannt, dass Alice und Bob den kleinsten Generator der Gruppe verwenden. Eve sieht nun, wie Alice und Bob sich gegenseitig die Werte `157212` bzw. `3780113` schicken.

Schreiben Sie ein C# Programm, um den DH Schlüsselaustausch anzugreifen und den gemeinsamen Schlüssel von Alice und Bob zu berechnen.

3 Elgamal (10 Punkte)

In dieser Aufgabe sollen Sie eine Elgamal Schlüsselerzeugung und Ver-, bzw. Entschlüsselung von Hand nachrechnen. Wir verwenden die zyklische Gruppe

$$\mathbb{Z}_{23}^* = \{1, 2, \ldots, 22\} \text{ mit der Multiplikation}$$

mit Generator 5.

a) Alice führt die Schlüsselerzeugung aus. Diese wählt $\mathtt{x} \leftarrow \mathbb{Z}_{23}^*$ und erhält $\mathtt{x} = 11$ als geheimen Schlüssel *sk*. Berechnen Sie den öffentlichen Schlüssel *pk*.

b) Bob erhält *pk* und möchte die Nachricht $\mathtt{m} = 19$ verschlüsseln. Der Verschlüsselungsalgorithmus zieht sich nun $\mathtt{y} \leftarrow \mathbb{Z}_{23}^*$ und erhält $\mathtt{y} = 3$. Berechnen Sie die Verschlüsselung $(\mathtt{c}_1, \mathtt{c}_2)$ der Nachricht.

c) In Teil d) benötigen Sie das Inverse von $c_1^x \bmod 23$. Rechnen Sie nach, dass c_1^{22-x} das Inverse von $c_1^x \bmod 23$ ist.
Hinweis: Folgerung vom Satz von Euler.

d) Alice erhält nun die Verschlüsselung $(\mathtt{c}_1, \mathtt{c}_2)$. Entschlüsseln Sie die Nachricht.

4 Textbook RSA (10 Punkte)

In dieser Aufgabe sollen Sie eine Textbook RSA Schlüsselerzeugung und Ver-, bzw. Entschlüsselung von Hand nachrechnen.

a) Alice führt die Schlüsselerzeugung aus. Diese wählt $\mathtt{p} = 11$ und $\mathtt{q} = 17$. Zusätzlich wählt sie $\mathtt{e} = 13$. Bestimmen Sie mit dem erweiterten Euklidischen Algorithmus das benötigte Inverse von $\mathtt{e}$ und geben Sie sowohl den öffentlichen Schlüssel *pk*, als auch den geheimen Schlüssel *sk* an.

b) Bob hat *pk* von Alice erhalten und möchte die Nachricht $\mathtt{m} = 42$ verschlüsseln. Berechnen Sie die Verschlüsselung $\mathtt{c}$, die Bob an Alice schickt.

c) Alice erhält die Verschlüsselung $\mathtt{c}$. Entschlüsseln Sie die Nachricht.