Institut für Angewandte und Numerische Mathematik
Sommersemester 2019
Dr. Daniel Weiß

Schnupperkurs Mathematik 2019
Verschlüsselung - Von Caesar bis zum TXDQWHQFRPSXWHU
Übungsblatt 5

Aufgabe 1 (Einwegfunktion zur Schlüsselerzeugung) (1+1+3 Punkte)
Eine Einwegfunktion $f\colon \mathcal{M} \to \mathcal{N}$, wobei $\mathcal{M}$ und $\mathcal{N}$ beliebige Mengen sind, ist eine Funktion, für welche sich $f(x)$ für $x \in \mathcal{M}$ sehr leicht berechnen lässt, zu gegeben $y \in \mathcal{N}$ ein $x \in \mathcal{M}$ mit $f(x) = y$ jedoch nur schwer zu bestimmen ist.

Ein typisches Beispiel ist $a^x \bmod m$ für gegebene $a, m \in \mathbb{N}$ wie zum Beispiel $453^x \bmod 21997$. Das *Diffie-Hellman-Merkle-Verfahren* nutzt Einwegfunktionen dieses Typs, um einen gemeinsamen Schlüssel zu erzeugen:

- Alice und Bob einigen sich (sogar öffentlich) auf Zahlen $a, m \in \mathbb{N}$.
- Alice wählt eine Zahl $x_A \in \mathbb{N}$, berechnet $f(x_A) = a^{x_A} \bmod m$ und schickt $f(x_A)$ an Bob.
- Parallel wählt Bob eine Zahl $x_B \in \mathbb{N}$, berechnet $f(x_B) = a^{x_B} \bmod m$ und schickt $f(x_B)$ an Alice.
- Alice berechnet mit x_A den Schlüssel $a^{x_B x_A} \bmod m$.
- Parallel berechnet Bob mit x_B den Schlüssel $a^{x_B x_A} \bmod m$.

(a) Begründe, warum Alice und Bob durch dieses Verfahren genau denselben Schlüssel erzeugen.

(b) Erkläre grob, unter welchen Bedingungen Eve (von engl. *eavesdropper*) mit dem Erlauschen der Größen a^{x_A} bzw. a^{x_B} nichts anfangen kann. Betrachte dazu: Bestimme x mit $453^x = 12839$, was sehr, sehr schwierig ist.

(c) Wir gehen nun davon aus, dass Mallet (von engl. *malicious*) diese Größen nicht nur erlauschen sondern sogar ersetzen kann. Damit kann Mallet einen sogenannten „Man-in-the-middle"-Angriff ausführen. Überlege dir, wie ein solcher Angriff aussehen könnte, bei dem Mallet tatsächlich alles, was Bob und Alice sich später verschlüsselt zusenden, lesen kann.
Hinweis: Wenn Du selbst keine Idee hast, kannst du dir im Internet Hinweise ergoogeln.

Aufgabe 2 (Anzahl der Schlüssel einer Enigma) (1+1+2+1 Punkte)
Wir betrachten eine Enigma in ihrer Grundausstattung mit 3 Walzen, welche entnommen und beliebig in die Enigma eingesetzt werden können, und einem Steckbrett, bei welchem 6 Buchstabenpaare vertauscht werden können.

(a) Bestimme die Anzahl der möglichen Anordnungen der Walzen.

(b) Bestimme die Anzahl der Stellungen der drei Walzen einer solchen Anordnung.

(c) Bestimme die Anzahl der Vertauschungen realisiert durch die sechs Buchstabenpaare im Steckbrett.

(d) Bestimme die Gesamtanzahl von Schlüsseln einer solchen Enigma.

Beachte: Wir besprechen die Aufgaben in der nächsten Vorlesung.
Infos: http://www.math.kit.edu/ianm3/~dweiss/seite/schnuppernmathe2019/