Adrian Häfliger GYMINF Fachdidaktik, HS21

Aufgabenblatt 1

- Die Aufgabe ist in 3-er-Gruppen zu bearbeiten.
- Sie wollen zwischen zwei Stationen eine verschlüsselte Nachricht mit 8 Buchstaben mit dem Schlüssel 24715938 versenden. Bevor Sie dies tun können, müssen Sie aber zwischen den zwei Stationen den Schlüssel austauschen, ohne dass die beiden Stationen Kontakt über eine sichere Verbindung miteinander haben. Wie können Sie dies tun?
- Sie haben das folgende Material zur Verfügung: Ein Fahrradschloss mit Schlüssel, eine abschliessbare Kiste, eine Karte mit dem symmetrischen Schlüssel 24715938.

Adrian Häfliger GYMINF Fachdidaktik, HS21

Aufgabenblatt 2

1. Öffnen Sie das Programm RSA.py in einem Editor, studieren Sie den groben Aufbau des Programms und führen Sie das Programm aus.

2. Wie Sie vielleicht bereits feststellen konnten, hat RSA.py drei verschiedene Funktionen: Sie können mit dem Programm einen Schlüssel für die RSA-Verschlüsselung generieren, Sie können eine Nachricht mit einem öffentlichen Schlüssel verschlüsseln und Sie können eine Chiffre mit einem privaten Schlüssel entschlüsseln. In der Folge sollen Sie diese drei Funktionen der Reihe nach verwenden:

   (a) Generieren Sie einen Schlüssel. Kopieren Sie die drei Zahlen in ein Textfile.

   (b) Verschlüsseln Sie eine Nachricht (wählen Sie dafür eine beliebige Zahl) mit Hilfe des öffentlichen Schlüssels. Notieren Sie sich die erhaltene Chiffre.

   (c) Entschlüsseln Sie die Chiffre mit dem privaten Schlüssel. Haben Sie wieder Ihre ursprüngliche Nachricht erhalten?

3. Überlegen Sie sich nun, wie Sie mit Hilfe dieses Programms mit einer anderen Person einen Schlüssel für eine symmetrische Verschlüsselung austauschen können. Stellen Sie den Ablauf möglichst detailliert dar.

Adrian Häfliger GYMINF Fachdidaktik, HS21

Aufgabenblatt 3

Diese Aufgaben sollen in 3-er Gruppen bearbeitet werden.

- Verteilen Sie die drei Rollen untereinander: Empfangende, sendende und angreifende Person.
- Die sendende Person möchte der empfangenden Person den Schlüssel 24715938 für eine asymmetrische Verschlüsselung zukommen lassen, so dass anschliessend die sendende und die empfangende Person symmetrisch verschlüsselte Nachrichten austauschen können. Ihr einziger Kommunikationskanal ist ein Chat, bei welchem auch die angreifende Person mitlesen kann. Alle drei haben das Programm RSA.py zur Verfügung. Wie gehen Sie vor?
- Wenn es gelungen ist, dass die sendende Person der empfangenden Person einen Schlüssel hat zukommen lassen können, mit welchem diese die Nachricht verschlüsseln und an die sendende Person zurückschicken konnte, ohne dass die angreifende Person diese lesen kann, haben Sie die Aufgabe erfolgreich gelöst. Tauschen Sie nun mindestens einmal die Rollen und spielen Sie den Ablauf erneut durch.
- Diskutieren Sie: Wie sicher ist dieses Verfahren? Wo bietet es Angriffsmöglichkeiten?