Präsenzübung 1

1. Grundlagen

a) Das Kerckhoffs'sche Prinzip spielt in der modernen Kryptographie eine zentrale Rolle. Geben Sie es mit Ihren eigenen Worten wider.

b) Die Wissenschaft der Kryptologie lässt sich in die Untergebiete Kryptographie und Kryptanalyse gliedern. Beschreiben Sie beide kurz mit Ihren eigenen Worten.

c) Skizzieren Sie die klassische Ausgangssituation zweier Kommunikationspartner Alice und Bob, die über einen unsicheren Kanal miteinander kommunizieren. Erklären Sie anhand dessen, warum die Kommunikationspartner kryptographische Algorithmen einsetzen müssen.

d) Ordnen Sie die folgenden Variablen, welche in der Kryptographie sehr wichtig sind, ihren jeweiligen Definitionen zu: $e(.)$, $d(.)$, x, y, k, $\#k$.

- Schlüssel
- Verschlüsselung
- Schlüsselraum (Menge aller möglichen Schlüssel)
- Chiffrat
- Entschlüsselung
- Klartext

2. Brute-Force-Angriff auf AES & Moores Law

AES ist die momentan am häufigsten eingesetzte symmetrische Chiffre. In dieser Aufgabe wird die Langzeitsicherheit von AES mit 128-Bit-Schlüsseln[1] betrachtet. Die Annahme ist, dass der beste bekannte Angriff die vollständige Schlüsselsuche (auch: Brute-Force-Angriff) ist, bei dem systematisch alle möglichen Schlüssel durchgetestet werden.
Hinweis: Falls Sie keinen Taschenrechner haben schätzen Sie ihr Ergebnisse mithilfe der Potenzgesetze und der Annahme $10^3 \approx 2^{10}$ ab.

a) Wie viele verschiedene 128-Bit-Schlüssel gibt es?
Tipp: Geben Sie die Anzahl als Zweierpotenz an.

b) Wir nehmen an, dass der Angreifer spezielle Hardware, sogenannte ASICs (Application Specific Integrated Circuits), hat, die für AES-Schlüsseltests optimiert sind. Ein ASIC kann $7 \cdot 10^8$ Schlüssel pro Sekunde überprüfen und der Angreifer verfügt über ein Budget von einer Million Euro. Ein einzelnes ASIC kostet 40€ und es wird ein Overhead (Mehraufwand) von 100%

[1] Eine 128-Bit-Zahl besteht aus 128 aufeinanderfolgenden Nullen und Einsen

für die Integration der ASICs angenommen (Bau des Computers, Stromversorgung, Kühlung usw.).

Wie viele ASICs kann man mit dem gegebenen Budget parallel betreiben? Wie lange dauert eine vollständige Schlüsselsuche im Durchschnitt? Setzen Sie diese Zeit in Relation zu dem Alter des Universums, welches 10^{10} Jahre beträgt.

c) Wir schätzen nun die Entwicklung der Rechenleistung zukünftiger Computer ab. Die Zukunft vorherzusagen ist bekannterweise nicht einfach, aber wir orientieren uns an dem **Mooreschen Gesetz**. Diesem zufolge verdoppelt sich die Rechenleistung alle 18 Monate, wobei die Kosten für Computer konstant bleiben. Nach wie vielen Jahren kann eine Maschine zur vollständigen Schlüsselsuche von AES-128 für eine Million Euro realisiert werden, mit der die *durchschnittliche* Suchzeit 24 h beträgt? Wir ignorieren bei dieser Abschätzung die Geldinflation.

3. Für zuhause: Moodle-Registrierung

Sämtliche Kursinhalte und -materialien, Ankündigungen, sowie die Aufzeichnungen der Vorlesungen sind über unseren Moodlekurs abrufbar. Außerdem erfolgt die Abgabe der Hausaufgaben elektronisch.
Bitte registrieren Sie sich daher unter `https://moodle.ruhr-uni-bochum.de` für den Kurs *Einführung in die Kryptographie (141022-WiSe19/19)*. Das Passwort lautet *krypto1819*.