Prof. Dr. Rüdiger Weis

Sicherheit in Verteilten Systemen

Übungsblatt 1: Kryptanalyse Klassischer Cipher

Aufgabe 1 Substitutionschiffren (42 Punkte)

Schreiben Sie ein Python Programm, um einen gegebenen Ciphertext, welcher mit einer buchstabenweise arbeitenden Substitutionchiffre verschlüsselt wurde, automatisch zu entschlüsseln.

Verwenden Sie hierzu eine Statistik für die einzelnen Buchstaben und ein Wörterbuchabgleich zur Ermittlung des Schlüssels.

Nehmen Sie vereinfachend an, dass der Klartext lediglich aus ASCII Kleinbuchstaben und Leerzeichen besteht.

Aufgabe 2 (18 Punkte) Schlüssellängen

Untersuchen Sie die Angriffsdauer von Brute-Force-Angriffen für die Schlüssellängen von 40, 56, 64, 112 und 128 Bit in folgenden Szenarien:

- Der Angreifer verfügt über ASICs, welche $5 \cdot 10^8$ Schlüssel pro Sekunde überprüfen kann und über einen Etat von 1 Mio Euro verfügt. Die Kosten pro ASIC belaufen sich auf 50 Euro und wir nehmen weiter 50 Euro pro Einheit für die Integration an.
  - Wie viele Einheiten können mit dem zur Verfügung stehenden Etat parallel betrieben werden?
  - Wie lange dauert die durchschnittliche, die minimale und die maximale Schlüsselsuchzeit?
- In wievielen Jahren könnte mit einem Etat von 1 Mrd Euro unter der Annahme der Weitergeltung von Moore's Law eine Schlüsselsuchmaschine gebaut werden, welche eine durchschnittliche Suchzeit von 24 Stunden benötigt?