IT Sicherheit Übung 1

Prof. Dr. Rüdiger Weis

Klassische Kryptanalyse

Aufgabe 1: Schlüssellängen (18 Punkte)

Untersuchen Sie die Angriffsdauer von Brute-Force-Angriffen für die Schlüssellängen von 40, 56, 64, 80, 112 und 128 Bit in folgenden Szenarien:

- Der Angreifer verfügt über ASICs, welche 2^{44} (Stand: April 2019) 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.
- Wie teuer ist gemessen an der aktuellen Bitcoin Miningrate ein Angriff mit der Komplexität 2^{64} beziehungsweise 2^{80}.

Aufgabe 2: Substitutionschiffren (42 Punkte)

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