3. Übungsblatt
Kryptographie und Mediensicherheit (SoSe 2018)

Bauhaus-Universität Weimar, Professur für Mediensicherheit (Prof. Lucks)
Betreuer: Eik List
URL: `http://www.uni-weimar.de/de/medien/professuren/mediensicherheit/teaching`
Abgabe: 15.05.2018, 11:00 Uhr vor Beginn der Übung oder an `eik.list(at)uni-weimar.de`.
LaTeX-Template: template.tex

Hinweis: Denken Sie daran, stets nachvollziehbare Lösungswege anzugeben. Für Lösungen, deren Herkunft nicht nachvollziehbar ist, werden 0 Punkte vergeben. Schreiben Sie mindestens eine Matrikelnummer in den Dateinamen Ihrer Abgaben.

Hinweis: Die ersten beiden Aufgaben für dieses 3. Aufgabenblatt finden Sie als Aufgaben 5 und 6 im unteren Teil des 2. Aufgabenblatts.

Aktualisierung: 12.05.: Die Anzahl der gegebenen Klartext-Chiffretext- Paare in Aufgabe 1 wurde auf drei erhöht.

Aufgabe 1 – Data Encryption Standard (DES) (4 Punkte)

Sie haben folgenden Varianten des DES gegeben (Vorlesung: Folien 135/136):

(1) 2DES mit zwei unabhängigen 56-bit Schlüsseln $K_1 \neq K_2$.

(2) Three-Key 3DES mit drei unabhängigen 56-bit Schlüsseln K_1, K_2, K_3.

Beschreiben Sie für die Varianten einen Angriff, der mit Hilfe dreier abgehörter Klartext-Chiffretext-Paare und signifikant weniger als 2^{112} DES-Operationen für Variante (1), bzw. signifikant weniger als 2^{168} DES-Operationen für Variante (2), den korrekten Schlüssel findet. Geben Sie zudem den benötigten Zeit- und Speicheraufwand an.

Bonus (+1): Beschreiben Sie den Angriff in Aufgabenteil (2) mit nur zwei gegebenen Klartext-Chiffretext-Paaren.

Aufgabe 2 – Mini-DES (Programmieraufgabe) (5 Punkte)

Mini-DES ist eine verkleinerte Variante des DES: Es verschlüsselt 32-bit-Inputs unter einem 16-bit-Schlüssel der in jeder von 16 Feistelrunden verwendet wird. Die Details der Blockchiffre spielen in der Folge keine Rolle. Sie finden eine Python-Implementierung auf der Übungswebseite. Mini-2DES verwendet zwei Iterationen von Mini-DES unter zwei unabhängigen Schlüsseln K_1 und K_2:

$$C_i = \text{Mini-2DES}_{K_1,K_2}(P_i) \stackrel{\text{def}}{=} \text{Mini-DES}_{K_2}(\text{Mini-DES}_{K_1}(P_i)).$$

Die folgenden zwei Klartext-Chiffretextpaare wurden unter einem geheimen (K_1, K_2) mit Mini-2DES wie oben beschrieben verschlüsselt:

i	P_i	C_i
1	`abcdef01`	`d18c096d`
2	`11223344`	`31f0989e`

Implementieren Sie ein Programm in Python 3, welches mit signifikant weniger als 2^{32} Aufrufen der Blockchiffre den geheimen Schlüssel (K_1, K_2) rekonstruiert mit welchem die oben stehenden Klartext-Chiffretextpaare verschlüsselt wurden. Das naive Austesten aller Schlüssel ist für diese Aufgabe **kein** gültiger Ansatz. Schicken Sie die Lösungen als Anhang einer E-Mail

`mini_2des_<MatrNr>.py`

an `eik.list(at)uni-weimar.de` mit dem Betreff `[Krypto SS18] Beleg 3` bis zum 15. Mai 2018, 11:00 Uhr. Es reicht dabei eine Matrikelnummer aus der Gruppe anzugeben.