4. Übungsblatt
Kryptographie und Mediensicherheit (SoSe 2016)

Bauhaus-Universität Weimar, Professur für Mediensicherheit
Prof. Dr. Stefan Lucks, Jakob Wenzel
URL: `http://www.uni-weimar.de/de/medien/professuren/mediensicherheit/teaching`

Abgabe: Bis zum 06.06.2016, 13:30 Uhr zu Beginn der Übung oder per E-Mail an `jakob.wenzel(at)uni-weimar.de`.
Lösungen sind bevorzugt in LaTeX zu verfassen. Ein Template finden Sie auf der Übungsseite der Veranstaltung. **Denken Sie daran, stets nachvollziehbare Lösungswege mit anzugeben. Für Lösungen, deren Herkunft nicht nachvollziehbar ist, werden 0 Punkte vergeben**.

Definition 1 (Differentielle Charakteristik)**.** *Sei $F : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ eine Funktion. Eine differentielle Charakteristik über r Runden einer Funktion F_{K_i} ist ein Vektor von Differenzen $\Delta_i \in \{0,1\}^n$, für $0 \leq i \leq r$: $\Delta_0 \xrightarrow{F_{K_1}} \Delta_1 \xrightarrow{F_{K_2}} \Delta_2 \xrightarrow{F_{K_3}} \cdots \xrightarrow{F_{K_r}} \Delta_r$. Eine iterative Charakteristik ist eine Charakteristik $\Delta \to \Delta$. Unter der Annahme, dass E eine Markov-Chiffre ist und alle Rundenschlüssel K_i unabhängig und gleichverteilt sind, können wir die Wahrscheinlichkeit jeder Charakteristik $\Delta_0 \xrightarrow{F^r} \Delta_r$ wie folgt berechnen:*

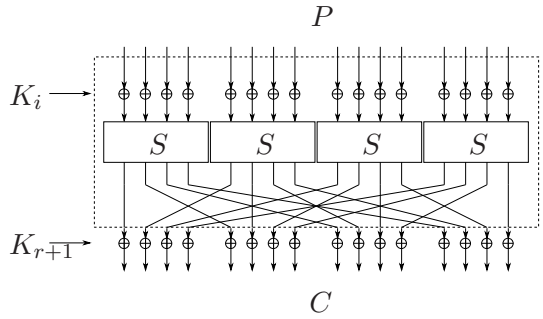
$$\Pr\left[\Delta_0 \xrightarrow{F^r \circ \ldots \circ F^1} \Delta_r\right] = \prod_{i=1}^{r} \Pr\left[\Delta_{i-1} \xrightarrow{F_{K_i}} \Delta_i\right].$$

Aufgabe 1 – Differentielle Kryptanalyse (6 Punkte)
Sei $F : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ eine Funktion. Es seien $\alpha, \beta, \gamma \in \{0,1\}^n$ bekannte gegebene Differenzen. Wir nehmen an, für alle Eingaben $X \in \{0,1\}^n$ und alle Schlüssel $K \in \{0,1\}^k$ gelten folgende Differentiale über F mit diesen Wahrscheinlichkeiten:

$$\Pr\left[\alpha \xrightarrow{F} \beta\right] = \frac{1}{4} \qquad \Pr\left[\alpha \xrightarrow{F} \gamma\right] = \frac{1}{2} \qquad \Pr\left[\beta \xrightarrow{F} \gamma\right] = \frac{1}{8} \qquad \Pr\left[\gamma \xrightarrow{F} \beta\right] = \frac{1}{4}.$$

Konstruieren Sie je eine differentielle Charakteristik auf die Luby-Rackoff-Chiffren mit 3, 4 bzw. 5 Runden (mit F als Rundenfunktion) mit Wahrscheinlichkeiten $\geq 1/4$, $\geq 1/16$ bzw. $\geq 1/64$ unter der Annahme, dass die Konstruktionen Markov-Chiffren und die Rundenschlüssel unabhängig und gleichverteilt sind.

Aufgabe 2 – Substitutions-Permutations-Netzwerke (5 Punkte)
Gegeben sei eine 16-Bit-Chiffre $E : \{0,1\}^k \times \{0,1\}^{16} \to \{0,1\}^{16}$. E besitzt r Runden, von denen jede aus dem XOR mit einem Rundenschlüssel K_i, einem S-Box-Layer und einer Transposition besteht (siehe Abbildung). Nach der letzten Runde findet ein XOR mit einem finalen Rundenschlüssel K_{r+1} statt, bevor der Chiffretext C ausgegeben wird.



1 Runde

x	0	1	2	3	4	5	6	7
$S(x)$	9	4	F	A	E	1	6	C
x	8	9	A	B	C	D	E	F
$S(x)$	0	7	3	8	2	B	5	D

a) Ermitteln Sie für die gegebene S-box $S : \{0,1\}^4 \to \{0,1\}^4$ die Wahrscheinlichkeiten aller 1-Bit-Differentiale $\Pr\left[\alpha \xrightarrow{S} \beta\right]$ für $\alpha, \beta \in \{1000, 0100, 0010, 0001\}$.
(Hier würde sich ein kleines Python-Skript lohnen oder Sie lösen zunächst Aufgabe 5.)

b) Nutzen Sie Ihre Erkenntnisse aus a) um eine iterative Charakteristik $\Delta \to \Delta$ über **vier Runden** zu finden und geben Sie die Wahrscheinlichkeit Ihrer Charakteristik (unter den üblichen Annahmen) an.

Aufgabe 3 – RSA I (5 Punkte)
Gegeben sind die beiden Primzahlen $p = 73$ und $q = 67$. Führen Sie die folgenden Rechenoperationen von Hand aus:

a) Berechen Sie n und $\varphi(n)$.

b) Sei der öffentliche RSA-Exponent $e = 163$. Berechnen Sie den geheimen RSA-Exponenten d. Warum ist $e = 11$ nicht sinnvoll?

c) Verschlüsseln Sie den Wert $M = 15$ (unter Verwendung des Square-and-Multiply-Algorithmus) und führen Sie als Probe die entsprechende Entschlüsselung aus.

Aufgabe 4 – RSA II (Faktorisierung von $\varphi(n)$) (4 + Bonus(2) Punkte)
Seien p und q zwei hinreichend große RSA-Primzahlen mit $p \neq q$.

a) Zeigen Sie, wie man $n = p \cdot q$ faktorisieren kann, wenn $\varphi(n) = (p-1) \cdot (q-1)$ bekannt ist. *(Hinweis: Die Berechnung der Quadratwurzel ist in $\mathbb{Z}_n$ ein mathematisch hartes Problem. In $\mathbb{Z}$ und $\mathbb{N}$ hingegen existieren allerdings Algorithmen, die eine Quadratwurzel effizient berechnen können.)*

b) **(Bonus)** Schreiben Sie ein Programm (in Python), welches einen RSA-Modulus n und einen Werte $\varphi(n)$ übergeben bekommt und unter Verwendung von $\varphi(n)$ den Werte n faktorisiert. Ihr Programm soll am Ende die beiden Primfaktoren p und q ausgeben.

Beispiel:

```
# factorize.py -n 51959 -phi 51504
(p,q) = 223, 233
```

Aufgabe 5 – Difference Distribution Table (Programmieraufgabe) (4 Punkte)
Seien Δ_{in} und Δ_{out} Input- und Output-Differenzen für die gilt:

$$\Delta_{in} = x \oplus x' \longrightarrow \Delta_{out} = y \oplus y'$$

tritt mit einer bestimmten Wahrscheinlichkeit $\Pr[\Delta_{in} \rightarrow \Delta_{out}]$ auf, wobei x und x' die Inputs einer S-Box S und y und y' die dazugehörigen Outputs sind mit $y = S(x)$ und $y' = S(x')$.

Schreiben Sie ein Programm in Python, dass eine beliebige S-Box S entgegennehmen kann und eine Häufigkeitstabelle für beliebige Input- und Output-Differenzen erzeugt (Difference Distribution Table, DDT). Aus dieser Tabelle soll zu entnehmen sein, wie hoch die Wahrscheinlichkeit für jedes Paar $(\Delta_{in}, \Delta_{out})$ ist. Die betrachtete S-Box soll dabei als Inhalt einer Datei (Pfad, Kommandozeilenparameter) übergeben werden. Dabei steht jener Wert x_i an i-ter Stelle in der Datei, für den gilt: $S(i) = x_i$.

Beispiel: Sei eine 3-zu-2-Bit S-Box definiert wie folgt:

```
Inhalt s-box.txt: 0, 2, 1, 3, 0, 2, 0, 1

# ddt_12345.py s-box.txt
in\out 00 01 10 11
000     8  0  0  0
001     0  2  6  0
010     2  4  0  2
011     0  2  2  4
100     4  2  2  0
101     2  0  4  2
110     2  4  0  2
111     0  2  2  4
```

Schicken Sie die Lösung als Anhang einer E-Mail

`ddt_<MatrNr>.py`

an `jakob.wenzel(at)uni-weimar.de` mit dem Betreff `[Krypto SS16] Beleg 4` bis zum 06. Juni 2016, 13:30 Uhr. Es reicht dabei eine Matrikelnummer aus der Gruppe anzugeben. Die vollständigen Namen und Matrikelnummern sollen als Kommentar im Python-Skript stehen.