Aufgaben zu Kapitel 2
Kryptographie (WS 14/15)

Institut: HS Schmalkalden
Dozent: Prof. Dr. Christian Forler
Url: `https://studip.fh-schmalkalden.de`
Email: `c.forler(at)hs-sm.de`

Aufgabe 1 (2+2 Punkte) Funktionen
Wie viele Funktionen $f : \{0,1\}^n \to \{0,1\}^n$ gibt es, wenn

a) f eine beliebige Funktion sein darf?

b) f eine beliebige Permutation sein darf?

Aufgabe 2 (2+2 Punkte) Random Enterprise Inc.
Die Firma `Random Enterprise Inc.` hat eine echte Zufallsfunktion $f : \{0,1\}^{64} \to \{0,1\}^{64}$ in Auftrag gegeben. Für jedes $x \in \{0,1\}^{64}$ wird $y = f(x)$ wirklich rein zufällig per 64-fachen Münzwurf - mit einer fairen Münze - bestimmt. Nun soll diese teuer erkaufte Zufallsfunktion natürlich auch irgendwo gespeichert werden. Die Geschäftsführung entscheidet sich dazu die Funktion verteilt auf mehreren Blu-ray Discs zu sichern, und diese dann in $50m^3$ großen Räumen zu lagern.

a) Schätzen Sie ab, wie viele Räume zur Lagerung benötigt werden. Gehen Sie vereinfacht davon aus, dass eine Blu-ray Disc 128 GB fasst und etwa das Volumen $(120 \times 120 \times 1,4)\text{mm}^3$ hat.

b) Nach einer Budgeterhöhung kann sich `Random Enterprise Inc.` sogar eine Zufallsfunktion $f : \{0,1\}^{128} \to \{0,1\}^{128}$ leisten. Wie viele Räume werden nun benötigt? Vergleichen Sie das vereinnahmte Volumen mit dem Volumen der Erde (ca. $1,083 \cdot 10^{21} m^3$)

Aufgabe 3 (2+2+2 Punkte) Drei Runden Feistel-Netzwerk (P_3)
Seien P_3^1, P_3^2 und P_3^3 drei Blockchiffre die wie der P_3 aus einem 3-Runden Feistelnetzwerk (siehe Vorlesung Kapitel 2.1, Folie 48) besteht.

a) Die einzelnen Rundenfunktion des P_3^1 sind wie folgt definiert:

- f_1 ist die Identität (d.h. $f_1(x) = x$).
- f_2 und f_3 sind zwei unabhängige Zufallsfuktionen.

Fertigen Sie eine Skizze des P_3^1 an und konstruieren Sie einen effizienten **einseitigen** (CPA) P_3^1-Angreifer.

b) Die einzelnen Rundenfunktion des P_3^2 sind wie folgt definiert:

- f_2 ist die Identität (d.h. $f_2(x) = x$).

- f_1 und f_3 sind zwei unabhängige Zufallsfuktionen.

Fertigen Sie eine Skizze des P_3^2 an und konstruieren Sie einen effizienten **einseitigen** (CPA) P_3^2-Angreifer.

c) Die einzelnen Rundenfunktion des P_3^3 sind wie folgt definiert:

- f_3 ist die Identität (d.h. $f_3(x) = x$).
- f_1 und f_2 sind zwei unabhängige Zufallsfuktionen.

Fertigen Sie eine Skizze des P_3^3 an und konstruieren Sie einen effizienten **einseitigen** (CPA) P_3^3-Angreifer.

d) In der Vorlesung haben wir gezeigt, dass der P_3 sicher gegen einseitige Angreifer ist. Weshalb gilt dies nicht für P_3^1, P_3^2 und P_3^3?

Aufgabe 4 (3+3+3 Punkte) Luby-Rackoff
In der Vorlesung wurde der Luby-Rackoff-Generator $P_3 : \{0,1\}^{2m} \to \{0,1\}^{2m}$ vorgestellt (Kapitel 3.1, Folie 62). Finden Sie einen effizienten Chosen-Plaintext Angreifer falls,

a) die einzelnen Rundenfunktion des P_3' wie folgt definiert sind

$$f_i(x) = \mathbf{K}_i \oplus x.$$

Bei $\mathbf{K}_1, \mathbf{K}_2$ und $\mathbf{K}_3$ handelt es sich um drei unabhängige zufällige gezogene und geheime Schlüssel.

b) zwei Blöcke $R, R' \in \{0,1\}^m$ mit $f_1(R) = f_1(R')$ bekannt sind.

c) die Funktion f_2 die Komplement-Eigenschaft $f_2(x) = \overline{f_2(\overline{x})}$ hat. Dabei bezeichnet $\overline{x}$ das bitweise Inverse von x (Beispiel: $\overline{00110} = 11001$).

Geben Sie auch die Anzahl der jeweils erforderlichen Einseitigen-Anfragen (CPA-Anfragen) an, die der Angreifer benötigt, sowie den Vorteil, den er erzielt.

Aufgabe 5 (4 Punkte) Post Whitening
Sei E eine sichere n-bit Blockchiffre und $\mathbf{K}_1, \mathbf{K}_2 \xleftarrow{\$} \{0,1\}^n$. Eine Nachricht $M \in \{0,1\}^n$ wird wie folgt verschlüsselt.

$$C := E_{\mathbf{K}_1}(M) \oplus \mathbf{K}_2.$$

Geben Sie einen Angreifer mit signifikanter Erfolgswahrscheinlichkeit an, der mit $\ll 2^{2n}$ Verschlüsselungsoperationen die beiden Schlüssel $\mathbf{K}_1$ und $\mathbf{K}_2$ berechnet.

Nebenbedingung: Dem Angreifer steht leider nur stark begrenzter Speicherplatz zur Verfügung, da seine Cloud auf Grund eines erneuten Stromausfalls nicht zur Verfügung steht. Daher muss der Angriff mit linearem Speicherverbrauch ($O(n)$) auskommen.