6. 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 12.07.2016, 11:00 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**.

Aufgabe 1 – Cipher Block Chaining (CBC) Mode (6 Punkte)
Im Folgenden betrachten wir eine Variante des CBC-Betriebsmodus (CBC'). Hierbei wird der Initialwert C_0 aus der Verschlüsselung einer Nonce (einmalig auftretender Wert) N generiert, d.h. $C_0 = E_K(N)$. Die Verschlüsselung einer Nachricht $M = M_1 \,||\, M_2 \,||\, \ldots \,||\, M_\ell$ mit $M_i \in \{0,1\}^n$ unter dem Modus CBC' sei also wie folgt definiert:

$$C_i = E_K(C_{i-1} \oplus M_i) \quad \text{mit } C_0 = E_K(N),\ 1 \le i \le \ell.$$

Es sei weiterhin bekannt, dass die verwendete Blockchiffre $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ einen Fixpunkt für einen bestimmten Wert X besitzt, d.h. es $\exists X : E_K(X) = X$. Zeigen oder widerlegen Sie, dass folgende Konstruktionen im RoR-CPA-Modell sicher sind. Begründen Sie ihre Antwort!

a) Es ist einem Angreifer erlaubt, den Wert der Nonce N frei zu wählen.

b) Der Wert N wird zufällig aus der Menge $\{0, \ldots, 2^n - 1\}$ gezogen.

c) Der Wert N wird zufällig aus der Menge $\{0, \ldots, 2^n - 1\}$ gezogen. Wir betrachten jetzt jedoch einen blockweise-adaptiven Angreifer. Solch ein Angreifer ist in der Lage, sich einen Klartextblock M_i verschlüsseln zu lassen und erhält den dazugehörigen Chiffretextblock C_i. Anschließend kann der Angreifer den Klartextblock M_{i+1} frei wählen und erhält den dazugehörigen Chiffretextblock C_{i+1}, usw.

Aufgabe 2 – CPA-CCA-Sicherheit (6 Punkte)
Im Folgenden sei jeweils ein Betriebsmodus und eine Sicherheitsdefinition gegeben. Beschreiben Sie für jedes der unten aufgeführten Szenarien einen effizienten Angreifer und geben Sie dessen Vorteil an.

a) ECB-Modus (Folie 210) im RoR-OTCPA-Modell.

b) Einfacher Counter-Modus (Folie 225) im RoR-CPA-Modell.

c) Beide Varianten des Counter-Modus (Folie 225 und 226) im RoR-CCA-Modell.

Aufgabe 3 – Message Authentication Codes (MACs) (6 Punkte)
Sei $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ eine sichere Blockchiffre und $K \twoheadleftarrow \{0,1\}^k$ ein zufällig gezogener Schlüssel. Zeigen oder widerlegen Sie für die folgenden Konstruktionen, dass diese im UF-CMA-Modell (Folie 236) sicher sind.

a) $\mathrm{AMAC}_K(M_1, \ldots, M_\ell) = \bigoplus_{i=1}^{\ell} E_K(M_i)$

b) $\mathrm{BMAC}_K(M_1, \ldots, M_\ell) = \bigoplus_{i=1}^{\ell} (E_K(i) \oplus M_i)$

c) $\mathrm{CMAC}_K(M_1, \ldots, M_\ell) = \bigoplus_{i=1}^{\ell} E_{K \oplus i}(M_i)$

Aufgabe 4 – CFB-MAC (3 Punkte)
Sei $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ eine sichere Blockchiffre, $K \twoheadleftarrow \{0,1\}^k$ ein zufällig gezogener Schlüssel und *const* eine öffentlich bekannnte Konstante. Der $\mathrm{MAC} : \{0,1\}^k \times (\{0,1\}^n)^* \to \{0,1\}^\tau$ sei für eine ℓ-Block-Nachricht $M = (M_1, \ldots, M_\ell)$ wie folgt definiert:

$$\begin{aligned} C_0 &= 0^n \\ C_i &= E_K(C_{i-1}) \oplus M_i, \ 1 \le i \le \ell \\ \mathrm{MAC}_K(M_1, \ldots, M_\ell) &= C_\ell \oplus const \end{aligned}$$

Zeigen oder widerlegen Sie, dass diese Konstruktion sicher im UF-CMA-Modell ist.

Aufgabe 5 – Effektive Schlüssellängen (2 Punkte)
Alice möchte über TLS sicher mit Bob kommunizieren. Sie bekommt die untenstehende Auswahl. Erläutern Sie kurz, welche Variante für Verschlüsselung und Schlüsselaustausch von diesen die höchste Sicherheit bietet.

- 3DES-CBC mit 4096-bit-Primzahl für den Diffie-Hellman-Schlüsselaustausch.
- AES-128-CBC mit 3072-bit-Primzahl für den Diffie-Hellman-Schlüsselaustausch.
- AES-256-ECB mit 2048-bit-Primzahl für den Diffie-Hellman-Schlüsselaustausch.
- AES-128-CBC mit Diffie-Hellman-Exportschlüsseln.

Aufgabe 6 – Programmieraufgabe (4 Punkte)
Piratin Alice hat einen Schatz versteckt. Damit Bob, aber nicht Eve, den Ort erfährt, verschlüsselt Alice eine Weltkarte auf der die Stelle markiert ist mit AES im Counter-Mode und schickt sie verschlüsselt an Bob. Dummerweise schickt Alice zunächst eine (verschlüsselte) Version der Karte ohne die Markierung und erst, als sie ihren Irrtum bemerkt, die richtige Version. Schusslig wie sie ist, nutzt sie beide Male den gleichen Initialwert IV (und natürlich den gleichen geheimen Schlüssel K). Sie finden beide Grafiken auf der Übungsseite.

Implementieren Sie ein Pythonskript, dass die Pfade zu zwei verschlüsselten `bmp`-Grafiken als Eingabe erwartet und ein Bild gleicher Größe erzeugt, das die Stelle sichtbar macht, an der Alice ihren Schatz versteckt hat. Um die Schatzsuche erfolgreich zu gestalten, ist zudem die zugrundeliegende Weltkarte auf der Webseite verfügbar.

Beispielaufruf:

```
$ ./recover-bmp.py <1st image path> <2nd image path> <output path>
```

Hinweis 1: Sie können z. B. die Python Image Library `PIL` nutzen.
Hinweis 2: Sie brauchen für die Aufgabe weder den IV noch den geheimen Schlüssel K.