Institut für Kryptographie und Sicherheit
Jun.-Prof. Dr. D. Hofheinz

Stammvorlesung Sicherheit im Sommersemester 2014

Übungsblatt 1

Aufgabe 1. Gegeben ist der folgende Chiffretext. Ermitteln Sie den dazugehörigen Klartext. (Hinweise: Als Verschlüsselungsmechanismus wurde das Vigenère-Verfahren benutzt. Den Chiffretext finden Sie auch als Textdatei zum Herunterladen auf der Webseite zur Vorlesung.)

```
MZMTELFMPLWUFEWXTZPCJDQPBVUKSIEEQDIMIIDRLQNTPWFBZNYNTTQLMAFAGQADDYXOPLIDIWYXFIN
ISZBSCZUOPLIDMNGTTMCCEDTTCVMBEYGWACCPUMOMRWVZUPQLRCSRBSCTXITLXQFEGSDCDCSRICCGAO
YGDMJWCAAZOYWMSPWOMATQOUAXCXTWOFEPVZQYOPOCTQVOCROQPQOMATQOUELQXTMQGVEBEMTGJWGWT
IYYGOWFLXANEFIMBEYGWJFRMFQDAPQICRLMBEFIDMHCVQWEFIDAHFSIMCCEIICCSRQEGRQQRFXQMYDM
RBJDSGZNFEDTPQFMJMYKQELQKAIOCHUVEMFDMLIMZOEFIHQRCRQZPAMBPPPATMYHSTVSYPXJCMGWBSU
EUBPQWGJXGXFMOYRQENGTTMCRSFPPHSGZYYPANEFIEWNGIFGZDXTMLPXEESCRNIMZESMDFSIMORLMBE
FAMQECWOQAFIDELQIEAPLXUIWJCVCDREZWEFIDZPAVQIEGSZWQRLQDTEIZMCCGUXSCVFPHYMFMDALMT
WCRSMOZENJLEIFWMPIMSSGWOQAFIDMYASPMORAUKPUMFPVCCEWQBMRNPPIZBWCRSBSZENJLEIECNAIQ
LPBMZLPAVKXEGRSIDYQBTPULUKSRYDVPBSGBEMFQBSCTAMXRLQDTQMAVZDWUVMWEXNCCHFMYLCEWYCR
OZJNXQLLAGAZOGRSBZRLQSPWAAZOCQUTJRLQNTPWFVLKIANECRZGDMREETDINIMZESMYCZQZPVTXITL
IPBSCQQBSMHTMFQIPAESHUMDMJNIMZESMDLSFMDPIHMLJXTIEFITIOSWQLEFIYMEFSPTLRIDXFZPUAS
CHNGVYWUAVGEZLDSKSMDRXTIEFITIOZIQVFQMZOEFIYMEFSPIDCEDTJYWQQRFXQMYDSGZEWWUF
```

Aufgabe 2. Das Wiederverwenden eines Schlüssels K im One-Time-Pad-Verfahren birgt Angriffsmöglichkeiten. Schreiben Sie ein Programm (beispielsweise ein Python-Skript), das zwei im WAVE-Format kodierte Dateien M_1, M_2 mithilfe des One-Time-Pad-Verfahrens verschlüsselt und dabei denselben Schlüssel K verwendet. Was passiert, wenn Sie die beiden Chiffrate XOR-verknüpfen? (Hinweis: Falls Sie eine XOR-verknüpfte Datei in einem Mediaplayer abspielen möchten, benötigen Sie einen korrekten WAVE-Dateiformat-Header. Wie könnte dieser aussehen, wenn Sie die ursprünglichen im WAVE-Format gespeicherten Klartexte nicht kennen?)

Aufgabe 3. Wir wissen, dass die Blockchiffre $(\mathsf{E}, \mathsf{D}) : \{0,1\}^8 \times \{0,1\}^4 \to \{0,1\}^4$ bei Eingabe eines festen Schlüssels K_0 eine Eingabe M wie folgt auf eine Ausgabe $C := \mathsf{E}(K_0, M)$ abbildet:

M	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
C	0111	1111	1110	0001	1101	0101	1010	0011	1000	0010	1001	0100	1011	0000	1100	0110

Verschlüsseln Sie die Klartexte $M_1 =$ 0100 1011 0100 0001 und $M_2 =$ 0100 1101 0100 0001 unter K_0 in den Betriebsmodi Electronic Code Book (ECB), Cipher Block Chaining (CBC) und Counter Mode (CTR). Worauf sollte bei der Wahl eines Initialisierungsvektors IV in den einzelnen Modi, falls vonnöten, geachtet werden? (Beispielsweise: Falls E ununterscheidbar von einer Zufallsfunktion ist, wie sollte IV im CBC-Modus oder CTR-Modus gewählt werden, um passive Sicherheit zu gewährleisten?)