Institut für Theoretische Informatik
Prof. Dr. Dennis Hofheinz
Übungsleiter: Thomas Agrikola

Stammvorlesung Sicherheit im Sommersemester 2017

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
```

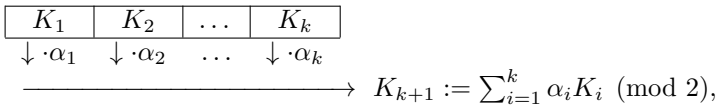
Aufgabe 2. Wir wissen, dass die Blockchiffre $(\mathsf{E}, \mathsf{D})\colon \{0,1\}^8 \times \{0,1\}^4 \to \{0,1\}^4$ bei Eingabe eines festen Schlüssels K_0 eine Eingabe M wie folgt auf eine Ausgabe $C := \mathsf{E}(K_0, M)$ abbildet:

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

Verschlüsseln Sie die Klartexte $M_1 = \texttt{0100 0111 0100 0001}$ und $M_2 = \texttt{0100 1101 0100 0001}$ unter K_0 in den Betriebsmodi Electronic Code Book (ECB), Cipher Block Chaining (CBC), und Counter Mode (CTR). Wählen Sie, falls nötig, einen geeigneten Initialisierungsvektor. Worauf sollte bei der Wahl eines Initialisierungsvektors IV in den einzelnen Modi, 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?)

Aufgabe 3. Aus der Vorlesung ist bekannt, dass One-Time-Pad-Chiffrate verformbar sind. (Ein Chiffrat $C := M \oplus K$, mit Klartext M und Schlüssel K, können wir verformen, indem wir $C' := C \oplus X$, für ein beliebiges X, berechnen. Bei der Entschlüsselung wird daraus $M' := D(K, C') = C' \oplus K = (C \oplus X) \oplus K = M \oplus X$.) Das im HEX-Format gegebene Chiffrat "`DF C0 71 42 8A 90 17 0E 14 12`" verschlüsselt das Wort "COMPLEXIFY". Verformen Sie dieses, sodass bei der Entschlüsselung der Klartext "DOKTORMETA" entsteht. (Hinweis: Die Buchstaben sind im ASCII-Format kodiert.)

Aufgabe 4. Aus der Vorlesung sind Linear-Feedback Shift Registers (LFSRs) als Beispiel für Pseudozufallsgeneratoren für Stromchiffren bekannt. Ihr Zustand besteht aus k Bits $K_1, \ldots, K_k$. Bei einem Zustandsupdate wird ein neues Bit K_{k+1} wie folgt berechnet:



wobei $\alpha_1, \ldots, \alpha_k \in \{0,1\}$ geheim sind. Das erste Bit des jeweils aktuellen Zustands $c_1 := K_1$ wird ausgegeben, der aktualisierte Zustand ist $K_2, \ldots, K_{k+1}$.

Geben Sie einen Angriff auf dieses Verfahren an. **Genauer:** Geben Sie eine Möglichkeit an, gegeben eine Sequenz von $\mathbf{O}(k)$ Ausgabe-Bits des Zufallsgenerators, mindestens ein weiteres Ausgabe-Bit vorherzusagen. (Das sollte bei einem guten Zufallsgenerator nicht funktionieren.) Wie viele Ausgabe-Bits müssen wir betrachten, damit ein solcher Angriff immer gelingt?