Kryptologie: Übungsblatt 3, Besprechung ab dem 7.5.2018, 10:15, H20

32.) Wir haben es mit einer Sprache zu tun, in der es nur die 3 Buchstaben A, B, C gibt, und diese treten mit den Wahrscheinlichkeiten 0.7, 0.2 und 0.1 auf. Das Folgende ist ein Vigenère-verschlüsselter Text in dieser Sprache (wobei nun modulo 3 statt modulo 26 gerechnet wird):

A B C B A B B B A C

Wir wissen, dass die verwendete Schlüssellänge 1, 2 oder 3 ist. Zeige, dass die Schlüssellänge höchstwahrscheinlich 2 ist und bestimme den plausibelsten Schlüssel und Klartext.

33.) Die Verschlüsselungsfunktionen f_i bei DES brauchen (erstaunlicherweise) nicht injektiv zu sein. Nehmen wir den extremen Fall an, dass f_i (egal bei welcher Eingabe und bei welchem Teilschlüssel k_i) immer konstant auf den Nullvektor abbildet. Betrachte nun eine solche Verschlüsselungsstufe $(L_{i-1}, R_{i-1}) \mapsto (L_i, R_i)$ bei DES. Wie hängen L_i und R_i von L_{i-1} und R_{i-1} ab?
Man überzeuge sich davon, dass auch in diesem Fall, und ganz allgemein, die Abbildung $(L_{i-1}, R_{i-1}) \mapsto (L_i, R_i)$ immer injektiv, sogar bijektiv, ist.

34.) Die Zufallsvariable X kann endliche viele Werte x annehmen, ebenso kann Y endlich viele Werte y annehmen. Außerdem seien X und Y unabhängig, d.h. für alle x, y gilt $P(X = x, Y = y) = P(X = x) \cdot P(Y = y)$.
Man beweise: $H(X, Y) = H(X) + H(Y)$.

35.) Man beweise: $H(Y \mid X) = 0$, falls $Y = f(X)$.

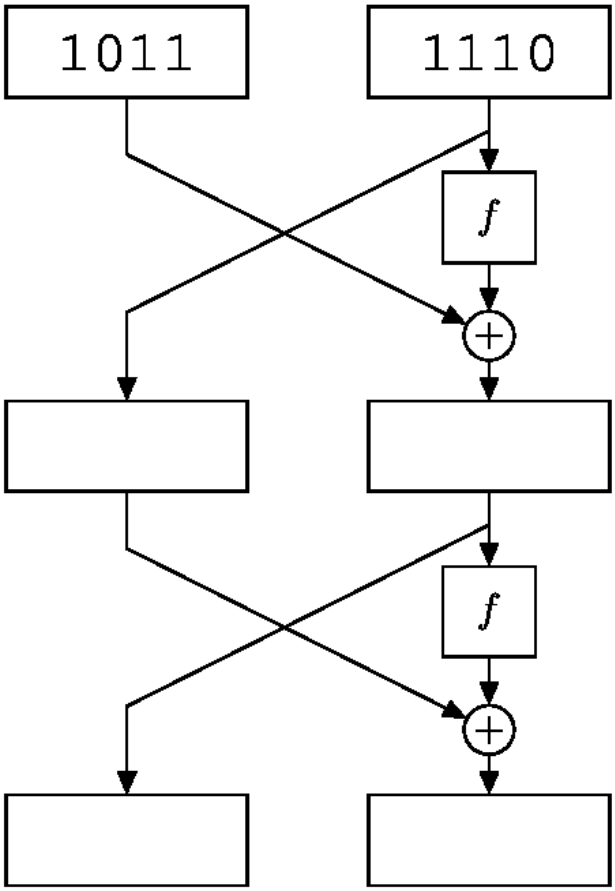
36.) Betrachte ein Schieberegister mit 4 Flip-Flops, dessen Rückkopplungsschaltung den Ausgang des 4. Flip-Flop und des 2. Flip-Flop mitels XOR zum Eingang des ersten Flip-Flop zurückführt (das ist dasselbe Schieberegister wie bei Aufgabe 24). Das zugeordnete Rückkopplungspolynom bei diesem Schieberegister ist somit $1 + x^2 + x^4$. Wenn sich das Rückkopplungspolynom in Polynome kleineren Grades faktorisieren lässt, dann erreicht das Schieberegister nicht die volle Periodenlänge. Zeige, dass dies bei diesem Rückkopplungspolynom der Fall ist.

37.) Ein Pseudozufallszahlengenerator arbeitet mit der Rekursion:

$$z_{i+1} = (z_i)^2 \bmod n$$

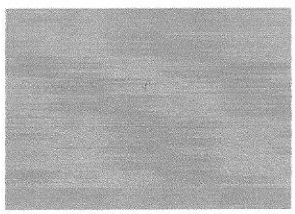
um Pseudozufallszahlen im Intervall $\{1, \ldots, n-1\}$ herzustellen.
a) Wenn n Primzahl ist, wieviele Zahlen kann eine solche Zahlenfolge höchstens durchlaufen, bis sich eine Zahl wiederholt, die schon einmal aufgetreten ist?
b) Dieselbe Frage, wenn $n = p \cdot q$ gilt, für zwei verschiedene Primzahlen (so wie beim Blum-Blum-Shub-Generator)?

38.) Gegeben sei das folgende Feistel-Netzwerk und f vertausche die Bits gemäß der Permutation $(1\,4\,3\,2)$ (d.h. das Bit an Position 1 wird zu Position 4 verschoben usw.). Fügen Sie die sich ergebenden (Zwischen-)Ergebnisse in die vier leeren Kästchen ein.

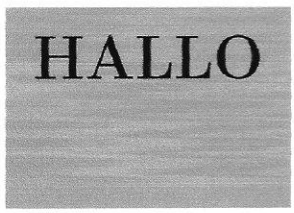


39.)

Gegeben seien drei Folien F_1, F_2 und F_M für visuelle Kryptographie. Einzeln erscheine jede Folie aus größerem Abstand gleichmäßig grau (linkes Bild). Legt man die Folien F_1 und F_M übereinander, so sei das Wort HALLO schwarz auf grau lesbar (mittleres Bild). Legt man die Folien F_2 und F_M übereinander, so sei das Wort WELT grau auf schwarz lesbar (rechtes Bild).



F_1 (ebenso: F_2, F_M)



F_1 auf F_M

F_2 auf F_M

Was passiert, wenn man die Folien F_1 und F_2 übereinanderlegt?

HALLO ist ...
- ○ nicht lesbar.
- ○ lesbar (schwarz auf grau).
- ○ lesbar (grau auf schwarz).

WELT ist ...
- ○ nicht lesbar.
- ○ lesbar (schwarz auf grau).
- ○ lesbar (grau auf schwarz).