Cryptography, winter 2006
Prof. Dr. Werner Schindler, Dipl.-Inf. Daniel Loebenberger

3. Exercise sheet (22.11.2006)
Hand in solutions to the homework exercises on Wednesday, December 13th, in the tutorial/the lecture.

Exercise 3.1 (Repetition: Elementary stochastics).

On a conference on Internet security are 15\% of the people cryptographers. 90\% of the cryptographers drink coffee. In total 25\% of the participants of the conference drink coffee. In the morning you see a person drinking coffee. What is the probability that this person is a cryptographer?

Exercise 3.2 (Modes of Operation).

Recall that $S_n$ is the set of all bit permutations of the set $\{0,1\}^n$. Let $\pi \in S_n$. Consider the following block cipher $\eta_\pi : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$, $(x_0, \ldots, x_{n-1}) \mapsto (x_{\pi(0)}, \ldots, x_{\pi(n-1)})$.

Decrypt the ciphertext 101010101010 using ECB mode, CBC mode and OFB mode. Use the cipher defined above with block length 3 and key

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

The initialization vector is 000. For the OFB mode, use $r = 2$.

Exercise 3.3 (Perfect secrecy: The Two Time Pad).

Show that the one-time pad is no longer unconditionally secure (perfect secrecy) if a key is used two (or more) times.

Exercise 3.4 (Homework: Forging the IV). (7 points)

Consider the following ASCII table

```
<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
</tbody>
</table>
```
Assume you intercepted a message \((m, IV)\), \(m \in \{0,1\}^*\), IV \(\in \{0,1\}^{64}\) where the plaintext was encoded according to the above ASCII table and encrypted with the CBC mode of a block cipher with block length 64 bit and initialization vector IV=0xAAAAAAAAAAAAAAAA yielding \(m\). Assume further you know that the plaintext of the message starts with the phrase DEAR SIR. Find an initialization vector IV’ such that the decrypted message will start with DEAR MAM.

**Exercise 3.5** (Homework: Perfect Secrecy). (5 points)

Prove that the Caesar cipher is not unconditionally secure.

**Exercise 3.6** (Homework: Modes of Operation). (8 points)

Decrypt the ciphertext 111111111111 using ECB mode and CBC mode. Use the cipher defined in Exercise 3.2 with block length 3 and key

\[
\begin{pmatrix}
1 & 2 & 3 \\
2 & 3 & 1
\end{pmatrix}
\]