2. Exercise sheet

Hand in solutions until Monday, 14 November 2011, 23:59:59h.

If you find any errors in the sheets, do not hesitate to write an email to the mailing list 11ws-ac@lists.bit.uni-bonn.de.

Exercise 2.1 (Birthday Paradox.). (12 points)

We again turn to the birthday problem, which is the content of the following theorem.

Theorem. Consider an urn containing $N$ numbered, distinct balls. Randomly drawing balls and putting each one back right away, on average it takes $O(\sqrt{N})$ rounds until one ball is drawn for the second time.

Prove the theorem as follows:

(i) Show: For $x \in \mathbb{R}$ holds $1 - x \leq e^{-x}$. Hint: Taylor expansion. If you do not remember it, look it up.

(ii) Let $B_i$ be the number on the $i$th ball. Show that for any $i$ we have

$$\text{prob}(B_i \notin \{B_1, \ldots, B_{i-1}\} | \#\{B_1, \ldots, B_{i-1}\} = i - 1) = 1 - \frac{i - 1}{N}.$$ 

(iii) Denote by the random variable $S$ the number of rounds until one of the balls is drawn for the second time. Then

$$\text{prob}(S \geq j) = \prod_{i=0}^{j-1} \text{prob}(B_i \notin \{B_1, \ldots, B_{i-1}\} | \#\{B_1, \ldots, B_{i-1}\} = i - 1).$$

Show: $\text{prob}(S \geq j) \leq e^{-(j-2)^2/2N}$.

(iv) For the expected number of rounds we can compute

$$E(s) = \sum_{j \geq 1} j \cdot \text{prob}(S = j) = \sum_{j \geq 1} \text{prob}(S \geq j).$$

Show that this is less or equal than $2 + \sqrt{\pi} \sqrt{N}$. Hint: You may use without a proof that $\int_0^\infty e^{-x^2} dx = \sqrt{\pi}/2$. 

Exercise 2.2 (More on the Chien et al. RFID protocol). (5 points)

In the lecture we have encountered two attacks that show that the Chien et al. RFID protocol is insecure. Here we are going to explore yet another attack against the protocol: Database-auto-desynchronization. Assume that you are running the system with $T$ different tags. Show that a collision in the value $M$ for two different tags may desynchronize the database with one of the colliding tags.

Exercise 2.3 (A DES S-Box). (12+5 points)

The fifth DES S-Box is defined as follows:

<table>
<thead>
<tr>
<th>Outer bits</th>
<th>Middle four bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>0010 1100 0100 0001 0111 1010 1011 0110</td>
</tr>
<tr>
<td>01</td>
<td>1110 1011 0010 1100 0100 0111 1101 0001</td>
</tr>
<tr>
<td>10</td>
<td>0100 0010 0001 1011 1010 1101 0111 1000</td>
</tr>
<tr>
<td>11</td>
<td>1011 1000 1100 0111 0001 1110 0010 1101</td>
</tr>
<tr>
<td>00</td>
<td>1000 1001 1010 1011 1100 1101 1110 1111</td>
</tr>
<tr>
<td>01</td>
<td>0101 0000 1111 1010 0011 1001 1010 0110</td>
</tr>
<tr>
<td>10</td>
<td>1111 1001 1100 0111 0001 1110 0010 1101</td>
</tr>
<tr>
<td>11</td>
<td>0110 1111 0000 1001 1010 0100 0101 0011</td>
</tr>
</tbody>
</table>

We will now analyze some of the properties of this S-Box. The computations necessary are far beyond what you could do manually. Please employ a reasonable programming language of your choice. Hand in the suitably formatted result as well as the source code.

(i) Compute a table of input/output differences $\Delta P/\Delta S$ that has as entries the number of 6-bit input pairs $(P, P')$ with $S(P) \oplus S(P') = \Delta S$.

(ii) Verify experimentally that changing a single input bit induces a change in at least two output bits.

(iii) Verify one further S-box property presented in the lecture. Do not verify the property involving three S-Boxes.