Modern Cryptology (236506) – Exercise no. 6


5 bonus points will be given to printed (or exceptionally clear and organized) submissions.

1. This question deals with the Fiat-Shamir protocol.

Assume that after the prover sends $X = R^2 \pmod{n}$ to the verifier, the least significant bit of $R$ is flipped in the prover’s memory.

How can the verifier use this error to get the secret $S$?

2. When Peggy wants to prove her identity to Vic, the following steps are repeated $t$ times:

- Peggy chooses two large prime numbers $p$ and $q$, and publishes $n = pq$ and some $x \in QNR(n)$. Peggy is going to prove that she knows the factorization of $n$ by being able to find efficiently whether some given $z$ is in $QR(n)$ or $QNR(n)$.
  
  (a) Vic chooses $v \in Z_n^*$ randomly and computes $y \equiv v^2 \pmod{n}$, chooses bit $i \in \{0, 1\}$ randomly, and sends $z \equiv x^i y \pmod{n}$ to Peggy.
  
  (b) If $z \in QR(n)$ then Peggy defines $j = 0$, otherwise, $j = 1$, and sends $j$ back to Vic.
  
  (c) Vic checks whether $i = j$.

- Vic accepts the proof if the check succeeded in all $t$ times.

(a) Show how Oscar (a cheater) can use the protocol to receive information he can not compute by himself.

(b) Here is a simulator to this protocol:

i. $T$ is the transcript of the conversation, and in the beginning we initialize $T = (x, n)$

ii. Do $t$ times:

A. Choose $i, y, v$ and $z$ like Vic.

B. Concatenate $(z, i)$ to $T$

Show that the output distribution of the simulator is equal to the distribution of a real communication with Peggy.

(c) Is this a ZK protocol?

If you answer yes, explain how is it that Oscar can use this protocol to gain information that he cannot compute by himself. If you answer no, explain what is wrong with the simulator, as it has the same distribution of outputs as in the protocol.

3. Researchers suggested to strengthen DES by switching entry 13 in the first row of $S_1$ with entry 14 in the second row of $S_1$: 

Show that this proposal weakens DES considerably.

(a) Suggest a high probability iterative characteristic.

(b) Show how to use the characteristic to attack the cipher.

Describe the attack and give an estimate to the amount of data required.

4. (a) Compute the probability of the following 3-round characteristic:

\[
\Omega_P = 00\ 78\ 00\ 2C\ 00\ 00\ 00_x
\]

\[
\begin{align*}
A' &= 00\ 00\ 00\ 00_x \\
F &\quad a' = 00\ 00\ 00\ 00_x \\
B' &= 8C\ 00\ 00\ 00_x \\
&= P(00\ 11\ 00\ 08_x) \\
F &\quad b' = 00\ 78\ 00\ 2C_x \\
C' &= 00\ 00\ 08\ 30_x \\
&= P(04\ 00\ 00\ 05_x) \\
F &\quad c' = 8C\ 00\ 00\ 00_x \\
\Omega_T &= 00\ 78\ 08\ 1C\ 8C\ 00\ 00\ 00_x
\end{align*}
\]

(b) Consider DES reduced to four rounds, and assume that the two pairs \( P_1, P_1^* \) \((P_1 \oplus P_1^* = \Omega_P)\), \( P_2, P_2^* \) \((P_2 \oplus P_2^* = \Omega_P)\) are right pairs with respect to the characteristic of question 4a. Recover at least 14 bits of information on the subkey of the fourth round (it is possible to find 28 bits of information from the following data, but you are required to find 14), given:
<table>
<thead>
<tr>
<th>$P_1$</th>
<th>$= 46\ 03\ 1E\ 01\ 88\ D3\ C2\ 73_x$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P_1^*$</td>
<td>$= 46\ 7B\ 1E\ 2D\ 88\ D3\ C2\ 73_x$</td>
</tr>
<tr>
<td>$T_1$</td>
<td>$= 02\ 55\ 6F\ 8D\ 0E\ DD\ D8\ 90_x$</td>
</tr>
<tr>
<td>$T_1^*$</td>
<td>$= 39\ 21\ 67\ E9\ 0E\ A5\ D0\ 8C_x$</td>
</tr>
<tr>
<td>$T_1'$</td>
<td>$= 3B\ 74\ 08\ 64\ 00\ 78\ 08\ 1C_x$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$P_2$</th>
<th>$= F8\ 3B\ CB\ 26\ 76\ 11\ 03\ 58_x$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P_2^*$</td>
<td>$= F8\ 43\ CB\ 0A\ 76\ 11\ 03\ 58_x$</td>
</tr>
<tr>
<td>$T_2$</td>
<td>$= 4A\ 1D\ 6B\ 75\ 22\ E2\ 49\ 11_x$</td>
</tr>
<tr>
<td>$T_2^*$</td>
<td>$= 43\ 1A\ 47\ 79\ 22\ 9A\ 41\ 0D_x$</td>
</tr>
<tr>
<td>$T_2'$</td>
<td>$= 09\ 07\ 2C\ 0C\ 00\ 78\ 08\ 1C_x$</td>
</tr>
</tbody>
</table>

$P^{-1}[3B\ 74\ 08\ 64_x] = 00\ 2A\ DA\ 5D_x$

$P^{-1}[09\ 07\ 2C\ 0C_x] = 00\ 60\ C5\ 2B_x$

$P^{-1}[B7\ 74\ 08\ 64_x] = 00\ 3B\ DA\ 55_x$

$P^{-1}[85\ 07\ 2C\ 0C_x] = 00\ 71\ C5\ 23_x$

Explain your answer. (You can find an online version of the difference distribution tables and list of pairs on the course homepage, also note that we gave a few hopefully useful values of $P^{-1}$)