Modern Cryptology (236506) – Exercise no. 6

Submission in singles until 21/06/2018.

5 bonus points will be given to two sided, printed submissions.

1. (a) Find the modular square roots of 8 modulo 23, using the algorithm we saw in class. Describe your calculations.
(b) Find the modular square roots of 5 modulo 29, using the algorithm we saw in class. Describe your calculations.

2. Let \( p \) be a large prime number and \( g \) a generator of \( \mathbb{Z}_p^* \).
Peggy picks at random a secret value \( x \in \mathbb{Z}_{p-1} \) and calculates \( Y = g^x \mod p \).
(a) Suggest a Zero-Knowledge protocol for the DLOG problem. I.e., a protocol that will let Peggy prove that she knows \( x \), the DLOG of \( Y \) modulo \( p \).
(b) Prove that your protocol is an interactive proof for the DLOG problem.
(c) Prove that your protocol is Zero-Knowledge.
(d) Is your protocol perfect Zero-Knowledge, or computational Zero-Knowledge? Explain.

3. Let \( G = (V, E) \) be a graph. Hamiltonian cycle for a graph is a cycle in the graph that visits each vertex exactly once. Finding a Hamiltonian cycle for a graph is known to be a NP-complete problem.

Peggy wants to prove to Victor that she knows a Hamiltonian cycle for a given graph \( G \), without revealing the cycle. So she went to wikipedia, where she found the following protocol:

**Protocol 1**
Repeat \( t \) times:

1. Peggy chooses a random permutation \( \pi \) on \( V \), and sends to Victor \( G_1 = \pi(G) = (\pi(V), \pi(E)) \).
2. Victor chooses a random \( i \in \{1, 2\} \) and sends it to Peggy.
3. If \( i = 1 \), Peggy sends \( \pi \) to Victor.
   If \( i = 2 \), Peggy reveals a Hamiltonian cycle in \( G_1 \).
4. Victor checks Peggy’s answer.

(a) Show that this protocol is an interactive proof for the Hamiltonian cycle problem. In particular, show how Peggy calculates her answer at 3., and how Victor checks her answer at 4.
(b) Show that this protocol is not Perfect Zero-Knowledge, assuming \( P \neq NP \).

Victor suggested changing the protocol by using a commitment scheme:

**Protocol 2**

Repeat \( t \) times:

1. Peggy chooses a random permutation \( \pi \) on \( V \), and computes \( G_1 = \pi(G) = (\pi(V), \pi(E)) \).
2. For each of the \( \frac{|V|(|V|-1)}{2} \) possible edges on \( G_1 \) Peggy computes a different commitment, and sends the commitments to Victor. I.e., for each pair of vertices \( (u_1, u_2) \in \pi(V) \), she sends commitment on 1 if \( (u_1, u_2) \in \pi(E) \), and commitment on 0 otherwise.
3. Victor chooses a random \( i \in \{1, 2\} \) and sends it to Peggy.
4. If \( i = 1 \), Peggy sends \( \pi \) to Victor, and reveals all the commitments on the graph.
   If \( i = 2 \), Peggy reveals commitments on \( |V| \) edges that form a Hamiltonian cycle in \( G_1 \).
5. Victor checks Peggy’s answer.

(c) What kind of commitment should we use (with perfect secrecy or perfect binding)? Explain.

(d) Is this protocol Zero-Knowledge? If your answer is yes, prove it, and determine if the protocol is Perfect Zero-Knowledge or Computational Zero-Knowledge. Otherwise, explain what Victor can learn from the protocol. You don’t have to show that the protocol is an interactive proof.

---

Researchers suggested to strengthen DES by switching entry 13 in the first row of \( S_1 \) with entry 14 in the second row of \( S_1 \):

\[
\begin{array}{cccccccccccccccc}
14 & 4 & \boxed{13} & 1 & 2 & 15 & 11 & 8 & 3 & 10 & 6 & 12 & 5 & 9 & 0 & 7 \\
0 & 15 & 7 & 4 & \boxed{14} & 2 & 13 & 1 & 10 & 6 & 12 & 11 & 9 & 5 & 3 & 8 \\
4 & 1 & 14 & 8 & \boxed{13} & 6 & 2 & 11 & 15 & 12 & 9 & 7 & 3 & 10 & 5 & 0 \\
15 & 12 & 8 & 2 & 4 & 9 & 1 & 7 & 5 & 11 & 3 & 14 & 10 & 0 & 6 & 13 \\
\end{array}
\]

i.e., the new \( S_1 \) is:

\[
\begin{array}{cccccccccccccccc}
14 & 4 & 14 & 1 & 2 & 15 & 11 & 8 & 3 & 10 & 6 & 12 & 5 & 9 & 0 & 7 \\
0 & 15 & 7 & 4 & 13 & 2 & 13 & 1 & 10 & 6 & 12 & 11 & 9 & 5 & 3 & 8 \\
4 & 1 & 14 & 8 & 13 & 6 & 2 & 11 & 15 & 12 & 9 & 7 & 3 & 10 & 5 & 0 \\
15 & 12 & 8 & 2 & 4 & 9 & 1 & 7 & 5 & 11 & 3 & 14 & 10 & 0 & 6 & 13 \\
\end{array}
\]

Show that this proposal weakens DES considerably: describe the best characteristic you can find, and explain how it is possible to use it to attack the full 16-round DES. What is the probability of the characteristic? What is the complexity of the attack?