IV054 Coding, Cryptography and Cryptographic Protocols

2009 – Exercises IX. (last)

1. Let us consider the Okamoto identificaton scheme with $p = 15643$, $q = 79$, $\alpha_1 = 216$, $\alpha_2 = 2712$. Alice has chosen $a_1 = 32$, $a_2 = 68$, $k_1 = 24$, $k_2 = 71$. Bob's challenge is $r = 888$. Show in detail how verification works. (Omit the part of the scheme related to signature of TA).

2. Alice and Bob use the Fiat-Shamir identification scheme. For some reason, Bob needs to convince Charles that he communicated with Alice recently. Therefore, he shows Charles what he claims to be a transcript of a recent execution of the Fiat-Shamir scheme in which he accepted Alice's identity. Should Charles get convinced after seeing the transcript? Explain your reasoning.

3. Consider the Shamir's threshold scheme. Let $n = 5$ and $k = 3$. Reconstruct the secret if $p = 11$ and participants P_1, P_2 and P_4 have the shares $(1, 8)$, $(2, 10)$ and $(4, 4)$, respectively.

4. Let p be a large prime and G a subgroup of $\mathbb{Z}_p$ which contains q elements. Let $g \neq h$ be two generators of G. All these values are public. Consider the following commitment scheme which enables Alice to commit herself to a number $x \in \{0, 1, \ldots, q-1\}$:

   - To commit to $x \in \{0, 1, \ldots, q-1\}$, Alice randomly chooses $r \in \{0, 1, \ldots, q-1\}$, computes $b = g^x h^r \pmod p$ and sends b to Bob.
   - To open her commitment, Alice sends to Bob the numbers x, r. Bob verifies whether $b = g^x h^r \pmod p$.

   Assuming that the discrete logarithm problem is intractable, show that the commitment scheme is both hiding and binding.

5. Consider the Shamir's (n, k) treshold scheme with large p. What is the maximum number of cheating shareholders (depending on n and k) so that the secret can still be recovered?
   How many computations of the secret needs to be made to discover one cheating shareholder in case of $(13, 3)$ scheme.

6. Consider the following bit commitment protocol that uses a pseudorandom generator G that generates $3n$ bits from n-bit seed. Alice wants to commit herself to a bit b.

   - Bob chooses a random sequence R of $3n$ bits and sends it to Alice.
   - Alice chooses n-bit vector S and computes $G(S)$.
   - If $b = 0$ Alice sends $G(S)$ to Bob, if $b = 1$ she sends $G(S) \oplus R$.
   - To open her commitment, Alice sends S to Bob who checks whether he got $G(S)$ or $G(S) \oplus R$.

   Decide whether this protocol is correct, hiding and biding. Explain yor reasoning.

7. Consider the Schnorr identification scheme. What happens if Alice uses the same random number k in two different executions of the scheme?

8. Propose a zero-knowledge proof for a graph problem called dominating set, i.e. suggest a protocol which allows Peggy to convince Victor that she knows a solution to the dominating set problem for a given graph G without revealing this solution to Victor.

   Show that your protocol is complete, sound and zero-knowledge.

   (A *dominating set* D of $G = (V, E)$ is a subset of V such that every vertex in $V - D$ is adjacent to at least one vertex in D).

9. A certain military office consists of one general, two colonels and five desk clerks. They have control of a powerful missile, but they do not want to launch it unless the general decides to launch it, or the two colonels decide to launch it or the five desk clerks decide to launch it or one colonel and three clerks decide in favor of launching. Describe how you would do it with a secret sharing scheme.

10. Twelve students of IV054 were discussing the interesting lecture. After a while one of them said: "Friends, I wonder what is our average number of points from exercises." They want to respect each other's privacy. How are they going to solve this problem?

11. *(Bonus)* You have found the following announcement. You presume that the NSA tries to test your hawk-eye.