CS 758

Assignment 3

due by Noon on Monday, November 11, 2013

General Instructions

- Assignments must be handed in by the designated time. I prefer an electronic copy (.pdf file) submitted by email, but I will also accept a hard copy that is dropped off in class or at my office. Due to the large number of students in the class, no extensions will be given.
- You are permitted to discuss assignment questions *informally* with a partner. However, when you hand in the assignments you must indicate who you had discussions with, and all solutions must be written up separately. No "copied" solutions or computer code are allowed; copied assignments are considered to be plagiarism and are subject to severe penalties.
- It is recommended that you attempt to solve every question on your own. If you do use an external information source (a book or a research paper, for example), give an appropriate citation.
- Computational questions can be done using any desired programming tools, languages or calculators. Maple is **strongly recommended** as the easiest way to do the questions. Please include all source code, and sufficient output so I can verify the main steps in the computations.
- I am available to provide extra help or hints if you get stuck on a question.

Questions

1. Suppose that the *Blom KPS* is implemented with security parameter k. Suppose that a coalition of k bad users, say $\mathrm{W}_1, \ldots, \mathrm{W}_k$, pool their secret information. Additionally, assume that a key $K_{\mathrm{U},\mathrm{V}}$ is exposed, where U and V are two other users.

   (a) Describe how the coalition can determine the polynomial $g_{\mathrm{U}}(x)$ by polynomial interpolation, using known values of $g_{\mathrm{U}}(x)$ at $k+1$ points.

   (b) Having computed $g_{\mathrm{U}}(x)$, describe how the coalition can compute the bivariate polynomial $f(x, y)$ by bivariate polynomial interpolation.

   (c) Illustrate the preceding two steps, by determining the polynomial $f(x, y)$ in the sample implementation of the *Blom KPS* where $k = 2$, $p = 1000003$, and $r_i = 11i$ $(1 \leq i \leq 4)$, supposing that

$$\begin{aligned} g_1(x) &= 292596 * x^2 + 502725 * x + 205896, \\ g_2(x) &= 379195 * x^2 + 870136 * x + 427928, \quad \text{and} \\ K_{3,4} &= 756408. \end{aligned}$$

(d) Compute $g_3(x)$ and $g_4(x)$.

2. We describe a secret-key based three-party session key distribution scheme. In this scheme, K_{Alice} is a secret key shared by Alice and the TA, and K_{Bob} is a secret key shared by Bob and the TA.

Step 1. Alice chooses a random number, r_A. Alice sends ID(Alice), ID(Bob) and

$$y_A = e_{K_{\text{Alice}}}(\text{ID(Alice)} \parallel \text{ID(Bob)} \parallel r_A)$$

to Bob.

Step 2. Bob chooses a random number, r_B. Bob sends ID(Alice), ID(Bob), y_A and

$$y_B = e_{K_{\text{Bob}}}(\text{ID(Alice)} \parallel \text{ID(Bob)} \parallel r_B)$$

to the TA.

Step 3. The TA decrypts y_A using the key K_{Alice} and it decrypts y_B using the key K_{Bob}, thus obtaining r_A and r_B. It chooses a random session key, K, and computes

$$z_A = e_{K_{\text{Alice}}}(r_A \parallel K)$$

and

$$z_B = e_{K_{\text{Bob}}}(r_B \parallel K).$$

z_A is sent to Alice and z_B is sent to Bob.

Step 4. Alice decrypts z_A using the key K_{Alice}, obtaining K; and Bob decrypts z_B using the key K_{Bob}, obtaining K.

(a) State all consistency checks that should be performed by Alice, Bob and the TA during a session of the protocol.

(b) The protocol is vulnerable to an attack if the TA does not perform the necessary consistency checks you described in part (a). Suppose that Oscar replaces ID(Bob) by ID(Oscar), and he also replaces y_B by

$$y_O = e_{K_{\text{Oscar}}}(\text{ID(Alice)} \parallel \text{ID(Bob)} \parallel r'_B)$$

in step 2, where r'_B is random. Describe the possible consequences of this attack if the TA does not carry out its consistency checks properly.

(c) In this protocol, encryption is being done to ensure both confidentiality and data integrity. Indicate which pieces of data require encryption for the purposes of confidentiality, and which ones only need to be authenticated. Rewrite the protocol, using MACs for authentication in the appropriate places.

3. Discuss whether the property of perfect forward secrecy is achieved in *MTI/A0* for a session key that was established between U and V in the following two cases:

   (a) one LL-key a_{U} is revealed.

   (b) both LL-keys a_{U} and a_{V} are revealed.

4. (a) Suppose that the following are the nine shares in a $(5, 10)$-*Shamir Threshold Scheme* implemented in $\mathbb{Z}_{100000007}$:

i	x_i	y_i
1	1001	41884014
2	1002	90967621
3	1003	95742366
4	1004	29847132
5	1005	51923901
6	1006	35767422
7	1007	19576738
8	1008	7452181
9	1009	67898370
10	1010	84572698

   Exactly one of these shares is defective (i.e., incorrect). Your task is to determine which share is defective, and then figure out its correct value, as well as the value of the secret. The "primitive operations" in your algorithm are polynomial interpolations and polynomial evaluations. Try to minimize the number of polynomial interpolations you perform.

   (b) Suppose that a (t, w)-*Shamir Threshold Scheme* has exactly one defective share, and suppose that $w - t \geq 2$. Describe how it is possible to determine which share is defective using at most $\lceil \frac{w}{w-t} \rceil$ polynomial interpolations. Why is this problem impossible to solve if $w - t = 1$?

   (c) Suppose that a (t, w)-*Shamir Threshold Scheme* has exactly τ defective shares, and suppose that $w \geq (\tau + 1)t$. Describe how it is possible to determine which shares are defective using at most $\tau + 1$ polynomial interpolations.