CS 758

Assignment 2

due by 1:00 PM on Thursday, July 7, 2016

General Instructions

- Assignments must be handed in by the designated time. Please hand in a *hard copy*. 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 copying of solutions or computer code is 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 $K_{\mathrm{U,V}}$ 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 $r_i = 101i$ $(1 \le i \le 4)$, supposing that

   $$\begin{aligned} g_1(x) &= 947286603 * x^2 + 744382840 * x + 241614105, \\ g_2(x) &= 762250336 * x^2 + 429596023 * x + 880853905, \quad \text{and} \\ K_{3,4} &= 211567571. \end{aligned}$$

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

2. 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.

3. Consider a sensor network KPS constructed from a TD$(3, 50, 83)$ (this KPS can support up to 83^3 nodes!). The identifier for a node A_c is a triple $c = (c_0, c_1, c_2) \in (\mathbb{Z}_{83})^3$ which corresponds to the polynomial $c_0 + c_1 x + c_2 x^2$.

   Write a simple program to solve quadratic equations in $\mathbb{Z}_{83}$, using the formula to extract square roots that is given on slide 64. Then use your program to determine all the common keys held by the following pairs of nodes A_c and A_d:

   (a) $c = (2, 58, 33)$, $d = (16, 23, 14)$.

   (b) $c = (56, 16, 38)$, $d = (11, 9, 7)$.

   (c) $c = (4, 80, 2)$, $d = (36, 2, 75)$.

4. (a) Suppose that the following are the nine shares in a $(4, 12)$-*Shamir Threshold Scheme* implemented in $\mathbb{Z}_{123456791}$:

i	x_i	y_i
1	1001	37831051
2	2002	89199733
3	3003	4632249
4	4004	88998204
5	5005	29883260
6	6006	8700231
7	7007	83405158
8	8008	65040476
9	9009	11562218
10	10010	104383204
11	11011	31089090
12	12012	96549487

   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 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.