CS 5311 Assignment 2

Due on Thursday, Feb. 14, 2013

Each student is required to do this assignment **individually** and to hand in a hard copy of your solution on due date. Computer typeset for the solution is preferred. Hand written is also acceptable, but request to write clearly. If you use computer to solve some questions, you don't need to include the computer program, but just put the answer (results) in your solution.

Put your Name, Student Number, Course Number (CS 5311) on your answer sheet.

Assignments which are not met the above requirements will not be marked. The score of the assignment will depend on:

Specification and documentation: 10 %

Correctness: 90 %

Late assignments will be penalized and will not be accepted after 3 days.

Problem 1.

In the Shamir's threshold scheme, the dealer chooses a polynomial $A(x)$ in $\mathbb{Z}_p$ and give $y_i = A(x_i)$ to user $P_i, 1 \le i \le w$, where $t < w$ and

$$A(x) = K + \sum_{j=1}^{t-1} a_j x^j \bmod p.$$

Let

$$A'(x) = \sum_{j=1}^{t} \left(y_{i_j} \prod_{1 \le k \le t, k \ne j} \frac{x - x_{i_k}}{x_{i_j} - x_{i_k}} \right) \bmod p.$$

Prove:

1. $A'(x_{i_j}) = y_{i_j}$.
2. $A'(x) = A(x)$.
3. $$K = \sum_{j=1}^{t} \left(y_{i_j} \prod_{1 \le k \le t, k \ne j} \frac{x_{i_k}}{x_{i_k} - x_{i_j}} \right) \bmod p.$$

Problem 2.

Write a computer program to implement addition $(+)$ and multiplication $(\cdot)$ in $\mathbb{F}_{2^8}$ with irreducible polynomial $x^8 + x^4 + x^3 + x + 1$. Then compute the following

1. $(11011010) + (01101010)$
2. $(00110101) \cdot (00010101)$

3. $(00001100) \cdot ((10101010) + (01011010))$

The notation of elements in $\mathbb{F}_{2^8}$ are from the lecture notes. Do not include your source code for this problem, but record the outputs. Also write down your algorithm for the multiplication.

Problem 3.

Suppose we have a (c, r, b)-ramp scheme constructed from an r-$(q, b+r-c, 1)$-OA, where $1 < c < r-2$. Prove the following:

1. Each $r-c$ tuple from $\mathbb{F}_q(GF(q))$ appears q^c times at the last $r-c$ columns of the OA.
2. Suppose $c+1$ users try to attack the ramp scheme. They used the first c shares together with any $r-c$ tuple at the last $r-c$ columns of OA to determine a unique row. Then they check if the $c+1$ share at this row is correct. If it is not, then they know that the $r-c$ tuple is not the key. Do you think they can find out the key using this method? Why?
3. Explain why a ramp scheme is not a perfect secret sharing scheme.

Problem 4.

Prove the following: Suppose that p is a prime. Let t, n, w be positive integers such that $p^n > (t-1)\binom{w}{2}$. Then there is a $(2^{\mathcal{U}}, w)$-OTBES for a set $\mathcal{U}$ of p^{nt} users, having message set $\mathbb{F}_{p^{2n+1}}$ such that each user needs to store at most $p^n + (t-1)(p^{nt}-1)$ values in $\mathbb{F}_{p^{2n+1}}$. The broadcast contains p^{2n} values in $\mathbb{F}_{p^{2n+1}}$.