Homework #3

Due Date: 03/2/2017, Thursday

Problem 1 *(20 points total)*

Consider the design of a Bloom filter with $k = 4$ hash functions for a set of 1 million entries. It is required that the probability of false positive be less than or equal to 10^{-2}. What is the minimum number of bits required in the Bloom filter? Show steps of your derivation.

Problem 2 *(20 points total)*

Consider the design of a systematic erasure code for $k = 4$ and $n = 7$ using $GF(2^3)$. Show elements (in binary representation) of the first three rows of the Vandermonde matrix.

Problem 3 *(10 points total)*

Consider a key tree that is full and balanced with height h, degree d for n users. Show that the total number of keys is approximately $\frac{d}{d-1}n$.

Note: h is defined to be the number of edges from the root node to a leaf node (u-node) in the key tree.

Problem 4 *(20 points total)*

There is a unique polynomial $f(x)$ of degree 3 such that $f(1) = 6, f(2) = 0, f(3) = 10,$ and $f(4) = 4$. The coefficients of $f(x)$ are in $GF(11)$. Derive the polynomial. In particular, what is the shared secret?

Hint: You probably will find the following information useful.

The prime field $GF(11) = \{0, 1, 2, \ldots, 10\}$. *For* $a \in GF(11)$, *there exists a unique* $b \in GF(11)$ *such that* $a + b = 0$ *modulo* 11. b *is called the addition inverse of* a *and is denoted as* $-a$. *For* $a \in GF(11)$ *and* $a \neq 0$, *there exists a unique* $b \in GF(11)$ *such*

that $a \cdot b = 1$ *modulo* 11. *b is called the multiplication inverse of a and is denoted as* a^{-1}. *See Table 1 for multiplication inverses of all elements in* $GF(11)$.

a	1	2	3	4	5	6	7	8	9	10
a^{-1}	1	6	4	3	9	2	8	7	5	10

Table 1: Multiplication inverses of $GF(11)$.

Problem 5 *(20 points total)*

Discuss the pros and cons of the Iolus approach versus the key tree approach for providing confidential group communications. In particular, in terms of the total processing cost for encrypting and decrypting keys by server/agents, describe the condition(s) under which the Iolus approach performs better than the key tree approach. (Limit your writing to 350 words. Please type your answer.)