Problem 6 - Solution

Since Alice wants to deal a one-byte secret, which could be regarded as a 8-bits binary string, therefore, the size of the message space would be

$$|M| = 2^8 = 256$$

Therefore, the smallest prime field should be at least as large as the message space. Since the smallest prime number that is larger or equal to 256 is 257, therefore, $\mathbb{F}_{257}$ would be used for the following analysis with Shamir secret sharing.

For k-out-of-n secret share, we have the following equation to compute each share:

$$f(x) = M + a_1 x + a_2 x^2 + ... + a_{k-1} x^{k-1} \pmod N$$

Given the problem setting, we know that $k = 2$ and $N = 257$, thus we use the following equation to compute or solve each share:

$$f(x) = M + a_1 x \pmod{257}$$

Now, we consider the case when $x = 1$ and $x = 2$:

$$f(1) = M + a_1 * 1 \pmod{257} = 209 \; [1]$$
$$f(2) = M + a_1 * 2 \pmod{257} = 34 \; [2]$$

Perform [2] - [1], we would get the following:

$$a_1 = 34 - 209 \pmod{257} = 82$$

Given that $a_1 = 82$, we could find the shared secret M as well as the player 3's share via the following computation:

$$M = 209 - 82 \pmod{257} = 127$$
$$f(3) = 127 + 82 * 3 \pmod{257} = 116$$

Therefore, the shared secret should be 127 = 0x7F, and player 3's share should be 116 = 0x74