Problems from the Book:

Chapter 10

1. To approach this problem, one should use a (2, 4) threshold scheme. If we use a Shamir (2, 4) scheme, the polynomial is of the form:

   \[ s(x) = 5 + a_1 x \pmod{p}. \]

Let us take \( p = 7 \) and choose the polynomial \( s(x) = 5 + x \pmod{7} \) (there are many other possible choices for polynomials). Then the secret value is \( s(0) = 5 \), and we may choose the shares \( (1, 6), (2, 0), (3, 1), \) and \( (4, 2) \).

3. The polynomial is

   \[ 8(x - 3)(x - 5) \quad (1 - 3)(1 - 5) + 10(x - 1)(x - 5) \quad (3 - 1)(3 - 5) + 11(x - 1)(x - 3) \quad (5 - 1)(5 - 3) \]

The secret is the constant term, obtained by letting \( x = 0 \):

   \[ \frac{8 \cdot 15}{8} + \frac{10 \cdot 5}{4} + \frac{11 \cdot 3}{8} = \frac{53}{8} \equiv 2 \pmod{17} \]

8. The slopes of the lines \( AB \) and \( AD \) are equal to \( 3/2 \) and \(-1/3 \), which are congruent mod 11. Therefore \( A, B, D \) lie on a line. \( C \) is not on this line, so \( C \) is the foreign agent. The line through \( A \) and \( B \) is \( y \equiv 8 + 7x \), so the secret is 8.

9. Split the launch code into three equal components using a 3 party secret splitting scheme. One component will be given to each of \( A, B, \) and \( C \). For the component that belongs to Government \( A \), use a \((3, 10)\) secret sharing scheme to give shares to the delegates of Government \( A \). Similarly, use a \((4, 10)\) secret sharing scheme to give shares of the component for Government \( B \) to \( B \)'s delegates. Finally, use a \((2, 10)\) scheme to share government \( C \)'s component amongst \( C \)'s delegates.

Chapter 10 Computer

3. We form the interpolating polynomial for different combinations of two users, and then compare the results. The answer that occurs most often is the correct answer.

\[
\begin{align*}
\text{>> p} &= 984583; \\
\text{>> x} &= [38 \quad 3876 \quad 23112 \quad 432]; \\
\text{>> s} &= [358910 \quad 9612 \quad 28774 \quad 178067]; \\
\text{>> interpoly(x([1 2]),s([1 2]),p)} \\
\text{ans} &= \\
\quad 69918 \quad 318526 \\
\text{>> interpoly(x([1 3]),s([1 3]),p)} \\
\text{ans} &= \\
\quad 21502 \quad 941642 \\
\text{>> interpoly(x([1 4]),s([1 4]),p)} \\
\text{ans} &= \\
\quad 21502 \quad 941642 \\
\text{>> interpoly(x([3 4]),s([3 4]),p)} \\
\text{ans} &= \\
\quad 21502 \quad 941642 \\
\end{align*}
\]

From these, it is clear that share 2 is the incorrect share.

Supplemental Problem

See the notes (Powerpoint slides) for the derivation of \( a(t) \). Instead of doing \( a(T) = 1/2 \), simply manipulate \( a(1) = 1/3 \) to solve for the constant term and then substitute back in.