

# Homework 15

Try out Shamir secret sharing

1. Create a polynomial with the secret being the constant term  $a_0$ , the other  $a$  values ( $a_1 \dots a_4$ ) can be chosen at random  
The polynomial will be of the form  
$$y(x) = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$$
2. Calculate the  $y$  values for five  $x$  values by applying the polynomial, these are the shares.
3. Reconstruct the polynomial using those points and an online interpolation calculator such as <https://planetcalc.com/8680/>