*Индивидуальная работа (Разделение секрета “Shamir”)(7,4)*

*(5,3)*

Пусть, секрет равен S = 71. Разделим его на 7 частей.

Возьмем три простых числа и сформируем полином: a1 = 19 a2 = 11 a3 = 5

Полученный полином: f(x) = 19x3 + 11x2 + 5x + 71

Формируем тени: Formam umbrele:

f(1) = 19\*13 + 11\*12 + 5\*1 + 71 = 106

f(2) = 19\*23 + 11\*22 + 5\*2 + 71 = 277

f(3) = 19\*33 + 11\*32 + 5\*3 + 71 = 698

f(4) = 19\*43 + 11\*42 + 5\*4 + 71 = 1483

f(5) = 19\*53 + 11\*52 + 5\*5 + 71 = 2746

f(6) = 19\*63 + 11\*62 + 5\*6 + 71 = 4601

f(7) = 19\*73 + 11\*72 + 5\*7 + 71 = 7162

Полученные тени: (1, 106)(2, 277)(3, 698)(4, 1483)(5, 2746)(6, 4601)(7, 7162)

Далее выберем четыре из вышеприведенных теней: (2, 277)(3, 698)(4, 1483)(5, 2746)

Формируем секрет S, используя интерполяционный полином Лагранжа: L(x) = \sum_{j=0}^n y_j l_j(x), где l_j(x)=\prod_{i=0, j\neq i}^{n} \frac{x-x_i}{x_j-x_i} = \frac{x-x_0}{x_j-x_0} \cdots \frac{x-x_{j-1}}{x_j-x_{j-1}} \frac{x-x_{j+1}}{x_j-x_{j+1}} \cdots \frac{x-x_{n}}{x_j-x_{n}}\,\! :

l0 = = = (x3 – 12x2 + 47x - 60)

l1 = = = (x3 – 11x2 + 38x - 40)

l2 = = = (x3 – 10x2 + 31x - 30)

l3 = = = (x3 – 9x2 + 26x - 24)

L(x) = \sum_{j=0}^n y_j l_j(x)

(x3 – 12x2 + 47x - 60) + (x3 – 11x2 + 38x - 40) (x3 – 10x2 + 31x - 30) +

+ (x3 – 9x2 + 26x - 24) = x3( ) +

+ x2( ) +

+ x( ) + ( ) =

= 19x3 + 11x2 + 5x + 71