**Теория**

Схема Шамира (A. Shamir, 1979) основана на хорошо известном математическом факте, который заключается в том, что через любые t точек на плоскости можно провести бесконечное множество кривых, описываемых многочленом t -го порядка,

но через любые t+1 различные точки можно провести только единственную кривую, описываемую многочленом

t-го порядка. Так, через любую точку на плоскости проходит бесконечное множество прямых линий, но через две различные точки –

только единственная. Через любые две точки можно провести бесконечное множество парабол, но через любые три различные точки – только одну и т.д. Таким

образом, если каждому из участников криптосистемы «выдать» по одной точке, то восстановить кривую можно будет только при достаточном количестве участников.

**Практика**

**секрет** S=23, разделяем секрет на 7 частей и будем реабилитировать по 4 частям .

1. Берем 3 случайных числа (обязательно простые) и формируем полином: = 5, =2, =3

Полученный полином имеет вид: f(x)=5+2+3x+23.

1. Формируем тени:

f(1)=5+2+3+23=33

f(2)=5\*+2\*+3\*+23=77

f(3)= 5\*+2\*+3\*3+23=185

f(4)= 5\*+2\*+3\*4+23=387

f(5)= 5\*+2\*+3\*5+23=713

f(6)= 5\*+2\*+3\*6+23=1193

f(7)= 5\*+2\*+3\*7+23=1857

получили следующие тени:

(1,33);(2,77);(3,185);(4,387);(5,713);(6,1193);(7,1857).

Выбираем тени по которым будем реабилитировать секрет: (2,77);(3,185);(4,387);(5,713).

Для реабилитация секрета S используется интерполирование с помощью полинома Lagrange:

L(x)=\*=\* ;

= = = - (-12+47x-60)

= = = (-11+38x-40)

= = = - (-10+31x-30)

= = = (-9+26x-24)

L(x)=\*=

= - -12+47x-60) + (-11+38x-40) - (-10+31x-30) + (-9+26x-24) =

(-+ - + ) + ( + - )+

+ x(-+ – + ) + ( + - ) = () + () +

+ x( ) + (770 – 3700 +5805 – 2852) =

= 5+2+3x+23

S=23