Sharim Secret Sharing

Aragon Andrade Angel Ivan

El Sharim Secret Scharing es un algoritmo que funciona en base a funciones matemáticas, consiste en encriptar datos a simple vista, esto lo hace mediante el ingreso de un polinomio y dicho dato que se quiera guardar.

Por ejemplo si queremos convertir 1234 a un polinomio de grado 3, debemos generar un polinomio aleatorio y adjuntarle la contraseña, así mismo debemos generar una determinada cantidad de coordenadas que nos servirán para decodificar la contraseña:

```
Polinomio generado:
```

$$64\,x^2 + 10\,x + 1234$$

```
Coordenadas generadas:
        1       1308
        2       1510
        3       1840
        4       2298
        5       2884
        6       3598
```

Posteriormente para desencriptar dichas coordenadas usaremos la interpolación de **Lagrange** que en palabras simples lo que hacer es evaluar las coordenas obtenidas respecto al grado del polinomio con el fin de obtener la función original en donde tenemos contenido la contraseña

```
Contraseña recuperada: 64    74  1308  1244  1234
```

Para k=4 y n=10

Polinomio generado:

$$96\,x^3 + 49\,x^2 + 81\,x + 1234$$

Coordenadas generadas:

1	1460
2	2360
3	4510
4	8486
5	14864
6	24220
7	37130
8	54170
9	75916
10	102944

Contraseña recuperada: 96 145 226 1460 1364 1315 1234