**Împărțirea secretelor. Schema lui Shamir**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | J | K | L | M |
| 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 |

Fie că trebuie expediat un mesaj secret: MAR

M - 22

A - 10

R - 27

chema lui Shamir se bazează pe interpolarea polinomială

1. Fie *S* – secretul; *S*=**221027**;
2. Alegem aleator *k* coieficienți: a1, a2, ..., ak;

***k=*5; a1=2; a2=7; a3=13; a4=4; a5=9;** - valori secrete

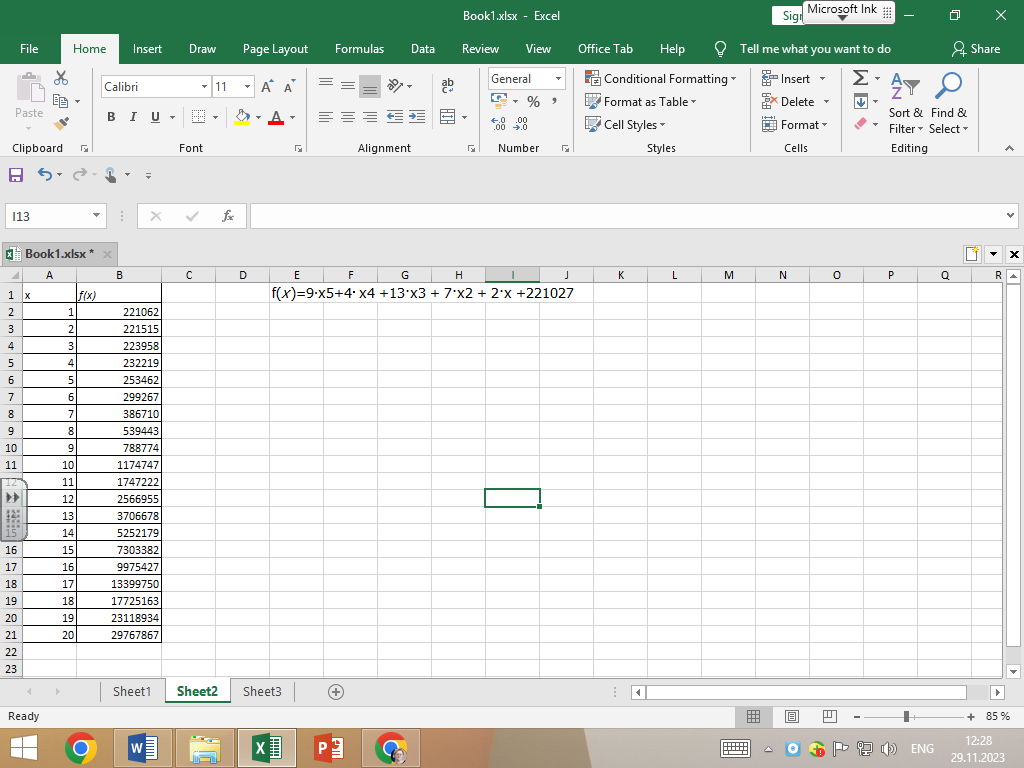
1. Construim polinomul: *f*(*x*)= ak·*xk* +ak-1·*xk*-1 + ... + a1·*x*+a0

**a0=S;**

*f*(*x*)= 9∙x5+4⋅*x*4+13·*x*3 + 7·*x*2+ 2·*x*+**221027 -** secret

1. Se alege un număr *n*=20, n - numărul de umbre (curieri)

Definim umbrele, adică formez perechile (*i*, *f*(*i*)):



Umbrele se repartizează ca perechi: **(1,221062), (2,221515), …, (20, 29767867).**

Pentru restabilirea secretului avem nevoie de *k*+1 umbre.

Deoarece *k*=5, atunci avem nevoie de 6 umbre pentru restabilirea secretului.

Pentru restabilirea polinomului vom aplica polinomul de interpolare Lagrange:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | X0 | X1 | X2 | X3 | X4 | X5 |
| i,x | 2 | 4 | 7 | 11 | 12 | 15 |
| f(i),y | 221515 | 232219 | 386710 | 1747222 | 2566955 | 7303382 |
|  | y0 | y1 | y2 | y3 | Y4 | Y5 |

...+ ...+

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | y0 | y1 | | y2 | | y3 | | y4 | | y5 | |
| numarator | -55440 | -27720 | | -15840 | | -10080 | | -9240 | | -7392 | |
| numitor | -11700 | 3696 | | -2400 | | 1008 | | -1200 | | 13728 | |
|  |  |  | |  | |  | |  | |  | |
|  |  |  | |  | |  | |  | |  | |
|  | -12280791600 | -6437110680 | | -6125486400 | | -17611997760 | | -23718664200 | | -53986599744 | |
|  |  |  | |  | |  | |  | |  | |
|  | 1049640,308 | -1741642,5 | | 2552286 | | -17472220 | | 19765553,5 | | -3932590,308 | |
|  |  | |  | |  | |  | |  | |  | |
| Secretul | 221027 | |  | |  | |  | |  | |  | |
|  |  | |  | |  | |  | |  | |  | |
| Formule: |  | |  | |  | |  | |  | |  | |
| B25 | =-C17\*D17\*E17\*F17\*G17' | | | |  | |  | |  | |  | |
| B26 | =(B17-C17)\*(B17-D17)\*(B17-E17)\*(B17-F17)\*(B17-G17)' | | | | | | | |  | |  | |
| B29 | =B25\*B18' | |  | |  | |  | |  | |  | |
| B31 | =B29/B26' | |  | |  | |  | |  | |  | |
| B34 | =SUM(B31:G31)' | |  | |  | |  | |  | |  | |
|  |  | |  | |  | |  | |  | |  | |

Secretul restabilit este: **221027**

**Restabiulirea secretului:**

Pentru a obține secretul inițial se împarte numărul în secvențe de 2 cifre de la dreapta spre stânga

**22 10 27 (împărțim numărul în numere de două cifre)**

**22 – M, 10 – A, 27 – R**

Sarcina 8.

1. Secretul lui Shamir, pentru k=5
2. Secretul **PRIM**
3. Program
4. De verificat rezultatele de la pl1 și de afișat screenshot.