**Partajarea secretă Blakley (7,4) (5,3)**

1. **Alegem 7 numere reciproc prime cu conditia că: \*\*\*<S<\*\***

=2; \*\*\*=858.

=11;

=3; \*\*=665.

=13;

=5; M= \*\*\*\*\*\*=2\*11\*3\*13\*5\*19\*7=570570.

=19;

=7.

Alegem S din relatia 665<S<858, fie S=750. secretul

**Formam urmele ≡S(mod mi).**

=750 mod 2=0;

=750 mod 11=2;

=750 mod 3=0;

=750 mod 13=9;

=750 mod 5=0;

=750 mod 19=9;

=750 mod 7=1.

**Fiecare persoana primeste prametrii (,, M).**

=(0, 2, 570570);

=(2, 11, 570570);

=(0, 3, 570570);

=(9, 13, 570570);

=(0, 5, 570570);

=(9, 19, 570570);

=(1, 7, 570570).

**Restabilira cheii:**

= = mod ().

===285285, = mod2=1.

===51870, = mod11=9.

===190190, = mod3=2.

===43890, = mod13=7.

===114114, = mod5=4.

===30030, = mod19=2.

===81510, = mod7=4.

=\*.

=0;

=2\*51870\*9=933660;

=0;

=9\*43890\*7=2765070;

=0;

=9\*30030\*2=540540;

=1\*81510\*4=326040.

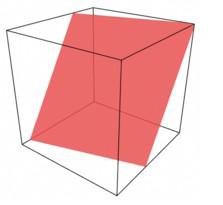
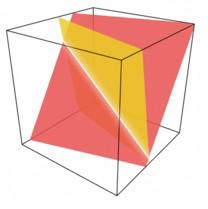
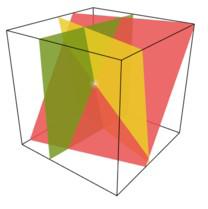
S= mod ().

S=++ )mod (\*\*\*)=

=(933660+2765070+540540+326040 )mod (11\*13\*19\*7)=4565310 mod 19019=750.

Pornind de la următoare observaţie: Două linii neparalele dintr-un plan se intersectează într-un punct, trei plane neparalele se intersectează într-un punct, atunci oricare *n* hiperplane de dimensiune *n* se vor intersectează într-un punct.

Secretul poate fi o codificare a unei coordonate a punctului de intersecţie. În cazul în care secretul este o codificare în care s-a folosit toate coordonatele, chiar dacă ele sunt aleatoare, atunci un insider (cineva care are în posesia sa una sau mai multe părţi) dobândeşte mai multe informaţii cu privire la secretul deoarece el ştie că trebuie să se afle în plan. Dacă o persoană din interior poate obţine mai multe informaţii despre secret decât un outsider, atunci sistemul nu mai are proprietatea de securitate. În cazul în care doar unul dintre cele *n* coordonate este folosită, atunci insiderul nu are mai mult informaţii decât un outsider (de exemplu, *că secretul se află pe axa x-pentru un sistem de 2-dimensional*). Fiecare participant primeşte destule informaţii pentru a defini un hiperspaţiu ; secretul este recuperat prin calcularea punctului de intersecţie a hiperplanelor şi apoi extragerea din coordonata esenţială.

[](http://profs.info.uaic.ro/~alaiba/mw/index.php?title=Fi%C5%9Fier:Art6Dragan.JPG)[](http://profs.info.uaic.ro/~alaiba/mw/index.php?title=Fi%C5%9Fier:Art7Dragan.JPG)[](http://profs.info.uaic.ro/~alaiba/mw/index.php?title=Fi%C5%9Fier:Art8Dragan.JPG)

Schema lui Blakley în spaţiul XYZ: fiecare parte este un plan, iar secretul este punctul aflat la intersecţia planelor.