**Разделения секрета по Blakley (7,4) другой вариант(5,3)**

**1.Выбираем 7 простых чисел с условием: \*\*\*<S<\*\***

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

=11;

=3; \*\*=665.

=13;

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

=19;

=7.

Выбираем S, 665<S<858, пусть S=750.

**Формируем тени:**

**≡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.

**Каждая часть получает 3 параметра (,, M).**

=(0, 2, 570570);

=(2, 11, 570570);

=(0, 3, 570570);

=(9, 13, 570570);

=(0, 5, 570570);

=(9, 19, 570570);

=(1, 7, 570570).

**Востановление ключей:**

= = 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+275070+540540+326040 )mod (11\*13\*19\*7)=4565310 mod 19019=750.

Начиная со следующего наблюдения: две непараллельные линии в плоскости пересекаются в точке, три непараллельные плоскости пересекаются в точке, тогда любая n-мерная гиперплоскость пересекается в точке.

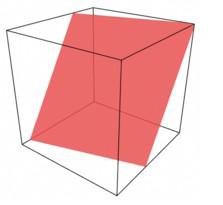
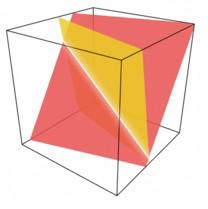
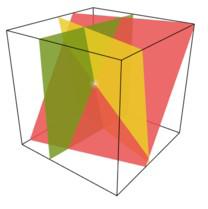
Секрет может быть в кодировании точки пересечения. Если секрет является кодировкой, в которой используются все координаты, даже если они случайные, то инсайдер (владелец одной или нескольких сторон) получает больше информации о секрете, потому что он знает, что быть в самолете. Если посторонний может получить больше информации о секрете, чем посторонний, то система больше не обладает свойством безопасности. Если используется только одна из координат n, то у инсайдера больше информации, чем у аутсайдера (например, секрет лежит на оси x для двумерной системы). Каждый участник получает достаточно информации для определения гиперпространства; секрет восстанавливается путем вычисления точки пересечения гиперплоскостей и последующего извлечения ее из существенной координаты.[](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)

Схема Блейкли в пространстве XYZ: каждая сторона представляет собой плоскость, и секрет заключается в точке пересечения плоскостей.