**Теория**

Схема Блейкли (A. Blackley, 1979) основана на следующих геометрических фактах.Одна прямая на плоскости описывает бесконечное множество точек, но любые две непараллельные прямые задают единственную точку их пересечения. Любые две некомпланарные плоскости в трехмерном пространстве пересекаются по прямой, которая задает бесконечное множество точек, но любые три некомпланарные плоскости пересекаются в единственной точке. Эти наблюдения по аналогии можно продолжить и в пространствах больших размерностей. Если каждому из участников криптосистемы «выдать» по одному уравнению плоскости (или гиперплоскости в пространствах размерности больше 3), то определить единственную точку их пересечения можно будет опять -таки при достаточном числе этих уравнений. В схеме Блейкли увеличение числа участников сопровождается ростом размерности пространства, в котором решается задача, что усложняет решение системы уравнений.

**Практика по схеме (7,4). (5,3)**

1. **1. Выбор 5 взаимно простых чисел при условии, что: \*\*<S<\***

=7; \*\*=105.

=5;

=3; \*=34.

=2;

=17. M= \*\*\*\*=7\*5\*3\*2\*17=3570.

**Выбор** S из отношений 34<S<105, fie S=100.

**Формирование тени ≡S(mod mi).**

=100 mod 7=2;

=100 mod 5=0;

=100 mod 3=1;

=100 mod 2=0;

=100 mod 17=15.

**Каждый получает параметры (,, M).**

=(2, 7, 3570);

=(0, 5, 3570);

=(1, 3, 3570);

=(0, 2, 3570);

=(15, 17, 3570).

**Установка ключа:**

= = mod ().

===510, = mod 7=6.

===714, = mod 5=4.

===1190, = mod 3=2.

===1785, = mod 2=1.

===210, = mod 17=3.

=\*.

=2\*510\*6=6120;

=0;

=1\*1190\*2=2380;

=0;

=15\*210\*3=9450.

S= mod ().

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

S = (6120+2380+9450) mod (7\*3\*17)=

S = 17950 mod 357

S = 100.