Дополнительная задача 2
Богданов Александр Иванович, Б05-001

1. Как работает создаются ключи?

   Равновероятно заполняем векторы s и e элементами из диапазона $(-\frac{module}{2}+1; \frac{module}{2})$. Затем равновероятно заполним вектор a элементами из диапазона $(1, module)$. ase_vector посчитаем таким образом $ase\_vector = (a\_vector * s\_vector + e\_vector)\%module$.

2. Как работает происходит вычисление векторов, необходимых для проверки?

   Мы вычисляем по определенным формулам $c, z1, z2$. (В программе указаны)

3. Как работает проверка?

   Зная $c, z1, z2$, проверяется, что вектор w получились именно такими, которыми они должны быть.

4. Как работает взлом?

   Во - первых, вектора z_1 и z_2 не должны быть не нулевыми, они так задаются при создании пары, а во вторых вектора z_1, z_2, c должны удовлетворять соотношению: $(a\_vector * z1 + z2 - ase\_vector * c + message\_hash)\%module - c = 0$. Возьмем вектор c равный нулю, вектор $z1$ с элементами равными $module$ ($module$ не равен нулю), вектор $z2$ заполним такими элементами, которые в сумме с $message\_hash$ дают ноль, если какой - то элемент $message\_hash$ равен нулю, то соответствующему элементу добавим m, так как остаток m от деления на m равен нулю.