$$m_q = 1394^{2011} mod\ 59 = 1394^{2011\ mod\ 58} mod\ 59 = 1394^{39} mod\ 59 = 30$$

$$\begin{cases} x = 30 (mod\ 59) \\ x = 36 (mod\ 53) \end{cases}$$

$$M_0 = 59 \cdot 53 = 3127,$$

$$M_1 = 53,\ M_2 = 59.$$

$$\begin{cases} 53y_1 = 30 (mod\ 59) \\ 59y_2 = 36 (mod\ 53) \end{cases}$$

$$59y_2 = 36 (mod\ 53) = 6y_2 = 36 (mod\ 53)$$

$$\begin{cases} y_1 = 54 \\ y_2 = 6 \end{cases} x = M_1 y_1 + M_2 y_2\ (mod M_0) = 3216 (mod\ 3127) = 89 (mod\ 3127)$$

Вот мы и получили наше исходное сообщение, используя при расшифровке китайскую теорему об остатках.

ЛИТЕРАТУРА

1. Википедия, свободная энциклопедия (https://www.wikipedia.org)

2. Чистяков Н.В. Аддитивные цепочки // 68-я научно-техническая конференция учащихся, студентов и магистрантов, 17-22 апреля, Минск: сборник научных работ : в 4 ч. Ч. 4 / - Минск: БГТУ, 2017. с. 272-275

УДК 004.056.55 - 003.26

Студ. Е.М.Лашкевич, Д.А.Ковалевич
Науч. рук. доц. И.К.Асмыкович
(кафедра высшей математики, БГТУ)

ВЕКТОРНАЯ СХЕМА РАЗДЕЛЕНИЯ СЕКРЕТА

Векторная схема разделения секрета или же схема Блэкли (англ. Blakley's scheme) — схема разделения секрета между сторонами, основанная на использовании точек многомерного пространства. Предложена Джорджем Блэкли в 1979 году. Схема Блэкли позволяет создать (t, n)-пороговое разделение секрета для любых t, n.

Идея

Разделяемым секретом в схеме Блэкли является одна из координат точки в m-мерном пространстве. Долями секрета, раздаваемые сторонам, являются уравнения (m − 1)-мерных гиперплоскостей. Для восстановления точки необходимо знать m уравнений гиперплоскостей. Менее, чем m сторон не смогут восстановить секрет, так как

множеством пересечения m − 1 плоскостей является прямая, и секрет не может быть восстановлен.

Пример схемы Блэкли в трех измерениях (рис. 1): каждая доля секрета — это плоскость, а секрет — это одна из координат точки пересечения плоскостей. Двух плоскостей недостаточно для определения точки пересечения.

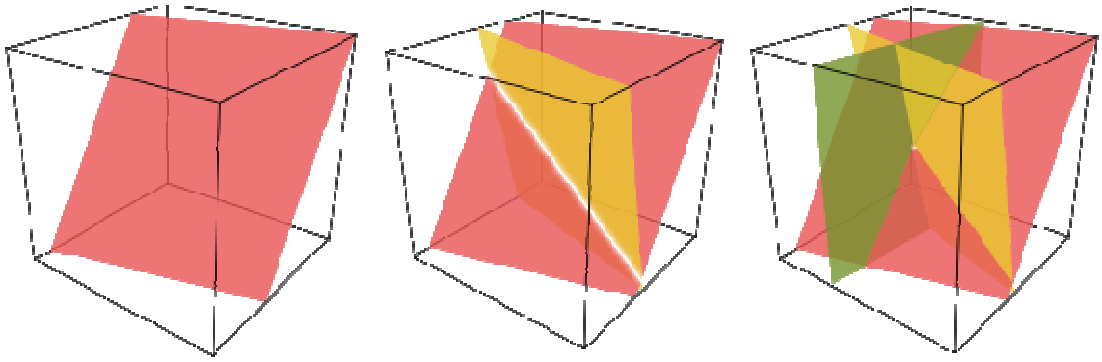

Рисунок 1 – Пример схемы Блэкли

Нужно отметить, что геометрическое описание и иллюстрации приведены для понимания главной идеи схемы. Однако сам процесс разделения секрета происходит в конечных полях с использованием аналогичного, но иного математического аппарата.

Описание

Генерация точки

Пусть нужно реализовать(k, n) пороговую схему, то есть секрет M разделить между n сторонами так, чтобы любые k из них могли восстановить секрет. Для этого выбирается большое простое число p > M, по модулю которого будет строиться поле $GF(p)$. Случайным образом дилер выбирает числа $b_2, \dots, b_k \in GF(p)$. Тем самым задается точка $(M, b_2, \dots, b_k)$в k-мерном пространстве, первая координата которой является секретом.

Раздача секрета

Для каждой стороны $P_i, i = (1, \dots, n)$P i , i = (1 , … , n) {\displaystyle P_{i},i=(1,\dots ,n)} случайным образом выбираются коэффициенты a 1 i , a 2 i , … , a k i {\displaystyle a_{1i},a_{2i},\dots ,a_{ki}} $a_{1i}, a_{2i}, \dots, a_{ki}$, равномерно распределенные в поле *G F (p) {\displaystyle GF(p)} GF(p).* Так как уравнение плоскостиимеет вид $a_{1i} \cdot x_1 + a_{2i} \cdot x_2 +, \dots, a_{ki} \cdot x_i + d_i = 0$a 1 i ⋅ x 1 + a 2 i ⋅ x 2 + ⋯ + a k i ⋅ x k + d i = 0 {\displaystyle a_{1i}\cdot x_{1}+a_{2i}\cdot x_{2}+\dots +a_{ki}\cdot x_{k}+d_{i}=0}, для каждой стороны необходимо вычислить коэффициенты d i {\displaystyle d_{i}} d_i:

$$d_1 = -(a_{11} \cdot M + a_{21} \cdot b_2 + \cdots + a_{k1} \cdot b_k) \bmod p$$
$$d_2 = -(a_{12} \cdot M + a_{22} \cdot b_2 + \cdots + a_{k2} \cdot b_k) \bmod p$$
$$\cdots$$
$$d_i = -(a_{1i} \cdot M + a_{2i} \cdot b_2 + \cdots + a_{ki} \cdot b_k) \bmod p$$
$$\cdots$$
$$d_n = -(a_{1n} \cdot M + a_{2n} \cdot b_2 + \cdots + a_{kn} \cdot b_k) \bmod p$$

При этом необходимо следить, чтобы любые *k {\displaystyle k} k* уравнений были линейно независимы. В качестве долей секрета сторонам раздают набор коэффициентов, задающих уравнение гиперплоскости.

Восстановление секрета

Для восстановления секрета любым *k {\displaystyle k} k* сторонам необходимо собраться вместе и из имеющихся долей секрета составить уравнения для отыскания точки пересечения гиперплоскостей:

$$\begin{cases} (a_{11} \cdot x_1 + a_{21} \cdot x_2 + \cdots a_{k1} \cdot x_k + d_1) \bmod p = 0 \\ (a_{12} \cdot x_1 + a_{22} \cdot x_2 + \cdots a_{k2} \cdot x_k + d_2) \bmod p = 0 \\ \cdots \\ (a_{1k} \cdot x_1 + a_{2k} \cdot x_2 + \cdots a_{kk} \cdot x_k + d_k) \bmod p = 0 \end{cases}$$

Решение системы дает точку в *k {\displaystyle k} k*-мерном пространстве, первая координата которой и есть разделяемый секрет. Систему можно решать любым известным способом, например, методом Гаусса, но при этом необходимо проводить вычисления в поле $GF(p)$.

Если число участников встречи будет меньше, чем kk {\displaystyle k} , например, $k-1$, то результатом решения системы уравнений, составленной из имеющегося набора коэффициентов, будет прямая в

-мерном пространстве. Тем самым множество допустимых значений секрета, удовлетворяющих полученной системе, в точности совпадает с полным числом элементов поля $GF(p)$, и секрет равновероятно может принимать любое значение из этого поля. Таким образом, участники, собравшись вместе, не получат никакой новой информации о разделенном секрете.

ЛИТЕРАТУРА

1. Электронный источник: http://cryptowiki.net
2. Электронный источник: https://ru.wikipedia.org