Базовые криптографические протоколы

Юрий Лифшиц *

Июль 2006г.

> "- Хорошо, дайте же сюда деньги.
> - На что же деньги?
> У меня вот они в руке!
> Как только напишете расписку, в ту же минуту их возьмете.
> - Да позвольте, как же мне писать расписку? Прежде нужно видеть деньги. Чичиков выпустил из рук бумажки Собакевичу, который, приблизившись к столу и накрывши их пальцами левой руки, другою написал на лоскутке бумаги, что задаток двадцать пять рублей государственными ассигнациями за проданные души получен сполна."
>
> *Н. В. Гоголь.* ***"Мертвые души"****, глава 5.*

1 Неформальная постановка разделения секрета

Задача. Есть комната управления секретной ракетой, президент, министр обороны и начальник космодрома. Нужно сделать замок (систему замков) таким образом, чтобы:

А Дверь может открыть каждый из трех

Решение: выдать каждому по ключу от замка

Б Дверь можно открыть только при согласии всех трех

Решение: сделать три разных замка

Б' Если речь идет не о ключах, а о пароле?

*Конспектировали лекцию Владислав Кудинов и Алексей Диевский.

Простое решение: просто дать каждому по паролю, а общий пароль получится, если ввести подряд три пароля, т.е.

$$p = \text{pas swo rd}$$

Хитрое решение: это когда общий пароль - это какая-нибудь функция от всех трех паролей, например:

$$p = ((p_1 + p_2 + p_3) \mod N)$$

Г А как сделать так, чтобы пароль могли восстановить любые два из трех? И вообще, возможно ли это?

Ответ: возможно. О том, как это сделать, как раз и рассказывается в этой статье.

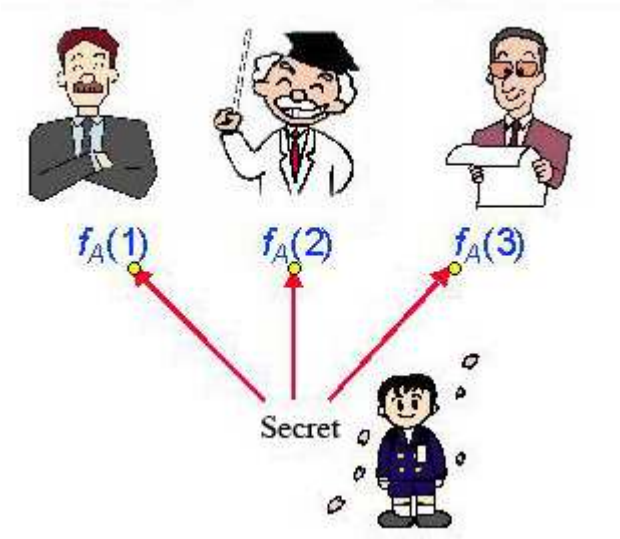
2 Две реализации разделения секрета

Криптографический протокол - это основное понятие теоретической криптографии. Под протоколом понимается распределенный алгоритм с двумя или более участниками. Протокол является криптографическим, если он решает по крайней мере одну из трех задач криптографии — обеспечение:

- *конфиденциальности*
- *целостности*
- *неотслеживаемости*

Определение криптографического протокола включает в себя различные компоненты: участников протокола, каналы связи между участниками, а также либо алгоритмы, используемые участниками, либо постановку той задачи, которую протокол призван решать.

2.0.1 Постановка задачи



Суть задачи очень проста - кто-то, назовем его Вася - знает несколько секретов, скажем 20 цифр банковского счета, на который он положил миллион долларов. И вот Вася решил оставить его в наследство своим шестерым детям, но он не хотел, чтобы дети ссорились из-за денег, в то же время не хотел никого выделять, поэтому сказал каждому по 20-значному числу, отличному от реального номера и очень похожего на случайное. А номер получался, если сложить все 6 чисел и взять первые 20 цифр получившегося числа. Таким образом, они смогут получить эти деньги тогда, когда все вместе придут в банк и скажут банкиру 6 кодов.

Формализация.

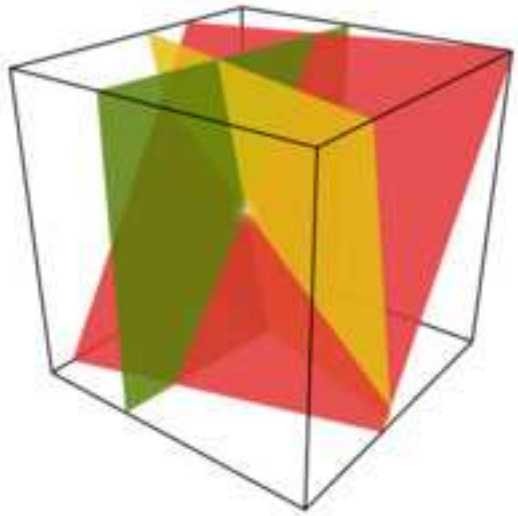
Теперь запишим формальные требования, которым должен удовлетворять протокол:

- Разделять секрет $m \in [1..N]$ между n участниками
- Любые t из них могут восстановить m
- Любые $t-1$ из них НИЧЕГО не могут узнать про m

2.0.2 Схема Блэкли

Одной из самых наглядных схем реализации протокола „Разделения секрета“ - является схема Блэкли, которую он придумал в 1979 году. Блэкли, т.к. видимо любил геометрию, когда ему понадобилось вдруг решить такую задачу, сразу вспомнил замечательное свойство плоскостей в пространстве - они пересекаются в **одной точке**, т.е. если мы дадим

каждому по плоскости, то все втроем они получат точку, а по отдельности бесконечное число точек(прямую), т.е. собственно говоря **ничего**.



Формализация.

Опишем, чуть более формально, схему "3 из n", т.е. если мы хотим, чтобы любые три участника, собравшись, могли узнать секрет, а 2 или меньше - нет.

Предпосылки:

- Все дело происходит в трехмерном пространстве
- Три плоскости общего положения(грубо говоря - плоскости должны попарно пересекаться) определяют точку.

Замечание 1. Компьютер не любит вещественные числа, поэтому мы рассматриваем 3-х мерное пространство над целыми числа по модуля p, т.е. $\mathbb{Z}_p^3$

Подготовительные шаги:

1. Выберем простое p
2. Секрет: $x_0 \in \mathbb{Z}_p$
3. Случайно выбираем $y_0, z_0 \in \mathbb{Z}_p$
4. Получили секретную точку $Q = (x_0, y_0, z_0)$

Раздача секрета:

1. Для каждого участника выбираем случайно $a, b \in \mathbb{Z}_p$
2. Вычисляем $c = z_0 - a \cdot x_0 - b \cdot y_0$
3. Получили плоскость: $z = a \cdot x + b \cdot y + c$

Задача 1. Придумать, как построить схему "t из n"?

2.0.3 Схема Шамира

В тоже время(1979 год), еще один ученый, явно в детстве больше любивший матан и алгебру, придумал другой способ решения поставленной задачи и реализовал протокол „Разделения секрета".
Основная идея (из матана) довольно проста и все необходимое мы знаем еще из школы:

- зная значения многочлена степени $t-1$ в t точках - можно восстановить его значения во всех остальных, это операция называется интерполяцией.
- зная только $t-1$ значения, невозможно предсказать остальные точки, что и обеспечивает второе необходимое свойство для данного протокола.

Теперь запишем эту идею формально.

Подготовительный шаг: раздающий выбирает простое p, которое больше всех возможных секретов.

Кодирование секрета:

- Выбираем $s_1 \dots s_{t-1} \overset{\text{ran}}{\in} \mathbb{Z}_p$ - секреты, которые ему необходимо раздать.
- Устанавливаем $s(x) \overset{def}{=} m + s_1 x + \dots + s_{t-1} x^{t-1}$

Замечание 2. Дальше все вычисления идут по модулю p, и поэтому все переменные всегда меньше p и „не раздуваются"

Раздача секрета: для каждого $i = 1, 2, \dots, n$ посылаем участнику i пару чисел $(i, s(i))$

Первый вопрос, который встает - а могут ли n человек, собравшись вместе, восстановить секрет и будет ли это восстановление единственным? Так давайте же поскорее на него и ответим.

Допустим собрались t человек, и они знают t точек на графике многочлена:

$$(x_1, s(x_1)), \dots, (x_t, s(x_t))$$

Выписываем систему уравнений:

$$\begin{pmatrix} 1 & x_1 & \dots & x_1^{t-1} \\ 1 & x_2 & \dots & x_2^{t-1} \\ \vdots & & \vdots & \vdots \\ 1 & x_t & \dots & x_t^{t-1} \end{pmatrix} \begin{pmatrix} m \\ s_1 \\ \vdots \\ s_{t-1} \end{pmatrix} = \begin{pmatrix} sx_1 \\ s(x_2) \\ \vdots \\ s(x_{t-1}) \end{pmatrix}$$

Факт, который нам известен из матана:

Эта система имеет единственное решение (а именно это мы и хотим) тогда и только тогда, когда определитель этой матрицы (она называется матрицей Вандермонда) не равен нулю. А человечеству известно (это еще один факт из матана), что если все $x_1, \dots, x_t$ различны, то определитель матрицы не ноль, т.е. система, имеет единственное решение.

Задача 2. чему равен определитель?

Теперь ответим на вопрос, как, собственно говоря, подсчитать секрет этим t бедалагам.
Секрет — это значение в нуле: $m = s(0)$

Вспомним формулу **интерполяции Лагранжа:**

$$s(x) = \sum_{i=1}^{t} s(x_i) \frac{\prod_{j\in[1..t]}^{j\neq i}(x_j - x)}{\prod_{j\in[1..t]}^{j\neq i}(x_j - x_i)}$$

Подставим вместо $x = 0$, получим **формула для ответа:**

$$m = \sum_{i=1}^{t} s(x_i) \frac{\prod_{j\in[1..t]}^{j\neq i} x_j}{\prod_{j\in[1..t]}^{j\neq i}(x_j - x_i)}$$

2.0.4 Анализ

Рассмотрим, какие есть у этого метода недостатки и достоинства.

Достоинства:

+ Размер данных не раздувается(см. **зам.2**)
+ При фиксированном t (количестве секретов) можно динамически добавлять новых участников
+ Один секрет можно шифровать много раз
+ Можно строить неравномерные структуры доступа

Недостатки:

– Одноразовость

– Возможность мошенничества со стороны раздающего

– Возможность мошенничества со стороны участников

– Необходимость сборки секрета перед его использованием

Задача 3. Задача на дом.

Вы хотите повесить несколько обычных замков и раздать ключи, чтобы было выполнено правило доступа “6 из 11”.

Какое минимальное число замков вам понадобится?

3 Византийские генералы - мотивация

Представим себе, что по небу летит самолет. На автопилоте. А теперь представим, что этот автопилот сломался. Ничего хорошего не произойдет, не так ли? Как бороться с такой ситуацией? Ясное дело, поставить еще один независимый автопилот. Но которого из них слушаться, когда они дают разные указания? Из двух автопилотов ни один не способен образовать большинство. Значит, надо поставить три автопилота! Даже если один из них сломается, остальных все равно будет больше, и они смогут принять правильное решение голосованием! Но кто будет проводить это голосование? Некий контрольный центр? Но если сломается он, то все усилия пойдут насмарку. Значит, автопилоты должны договориться между собой и сами прийти к правильному решению.

К сожалению, это невозможно. Вернее, это невозможно для трех автопилотов. А вот для четырех, из которых испортилось не более одного, необходимый протокол существует, и он будет предъявлен.

4 Византийское соглашение

4.1 Византийские генералы

В изначальной постановке задачи никаких автопилотов не было, а было n византийских отрядов, осаждающих вражеский город. Каждым отрядом командовал независимый генерал. Генералы могли общаться друг с другом по закрытому каналу, например, с помощью голубиной почты. Все вместе они общаться не могли, потому что отряды стояли далеко друг от друга, а радио и Интернет еще не изобрели. Все знали, что враг хитер и коварен, и вполне мог подкупить кого-нибудь из генералов; оставалось надеяться, что генералов-предателей не очень много. Тем временем осада затягивалась, пора было переходить к решительным действиям. Да вот беда - генералы не могли собраться вместе и выработать единый план. Если бы

не угроза предательства, все было бы просто - каждый генерал изложил бы остальным свой план с помощью голубей, а затем каждый выбрал бы наиболее популярный план и действовал бы согласно ему. Но так поступить нельзя - а ну как предатель скажет одному генералу, что пора наступать, а другому - что лучше отойти? Половина генералов рванется в бой, половина отступит, и получится черт знает что.

Таким образом, нужен был протокол, отвечающий двум требованиям:

1. Все честные генералы должны в итоге принять одно и то же решение.
2. Если предателей не очень много, то это решение должно оказаться правильным.

Сам протокол, по-видимому, должен состоять из двух фаз:

Фаза 1. Генералы обмениваются информацией.

Фаза 2. Генералы принимают решение на основе полученной информации.

Если мы в ходе первой фазы сделаем так, чтобы все генералы получили одинаковую сводку информации, то вторая фаза будет очень простой - выбрать наиболее популярный план из n предложенных. Таким образом, от первой фазы мы требуем два условия:

1А. Информация честных генералов должна дойти до остальных неискаженной.

1Б. От любого генерала все должны получить одинаковую информацию, даже если он попытается сообщить разную.

Далее мы для простоты будем считать, что каждый генерал делает бинарный выбор, например, выбирает между атакой и отступлением.

4.2 Командир и его заместители

Ясно, что изложенная выше задача разбивается на n одинаковых подзадач - каждый генерал должен передать свой выбор остальным. Эти подзадачи эквивалентны задаче о командире, который должен передать свой приказ $n-1$ заместителям, причем предателями могут быть как заместители, так и командир. От такого протокола мы опять потребуем два похожих свойства:

1. **Согласованность** Все честные заместители должны поступить одинаково.
2. **Исполнительность** Если вдобавок командир честен, то есть отдал всем одинаковый приказ, а среди заместителей не слишком много предателей, то все честные заместители должны поступить так, как приказал командир.

В этой схеме каждый может общаться с каждым. Докажем от противного, что для $n = 3$ и не более чем одного предателя требуемый протокол невозможен.

Первая ситуация. Пусть командир и первый заместитель - честны, а второй заместитель - предатель. Командир отдает приказ атаковать, однако второй заместитель, желая запутать первого, говорит ему, что командир приказал отступать. Наш предполагаемый протокол должен обладать исполнительностью, поэтому честный первый заместитель должен выполнить приказ командира, то есть пойти в атаку, игнорируя своего коллегу. Таким образом, выходит, что заместитель должен в любом случае слушаться командира.

Вторая ситуация. Пусть теперь предатель - командир. Он отдает первому заместителю приказ атаковать, а второму - отступать. Честные заместители честно сообщают друг другу эти приказы, но, согласно предыдущему выводу, игнорируют разночтения, так что первый заместитель идет в атаку, а второй отступает. Стоп! Мы потеряли согласованность.

Это и доказывает невозможность такого протокола.

4.3 Протокол для $n \geq 3m + 1$

В предыдущем пункте беда была в том, что предателей было *не менее одной трети*. Сейчас мы построим протокол, обладающий нужными свойствами, если предателей менее одной трети. Строить будем по индукции по числу m, где, как потом окажется, m - это максимальное число предателей, для которого протокол все еще работает. Напомним, что мы сейчас рассматриваем не задачу о генералах, а более простую задачу о командире и заместителях, причем с бинарным выбором приказа.

Протокол $BG(0)$.

1. Командир рассылает заместителям приказ.
2. Заместители поступают в соответствии с полученным от командира приказом.

Заметим вскользь, что для случая, когда предателей нет, протокол прекрасно работает.

Протокол $BG(m)$.

1. Командир рассылает заместителям приказ.
2. Каждый заместитель рассылает этот приказ своим коллегам, используя протокол $BG(m-1)$. На время рассылки рассылающий заместитель играет роль «командира» среди своих коллег.

3. Каждый заместитель из $n-1$ приказа (одного «своего» и $n-2$ полученных от коллег) выбирает наиболее часто встречающийся и поступает в соответствии с ним.

Тут необходимо сделать одну оговорку. К сожалению, может случиться так, что наиболее частого плана не будет (рассмотрите самостоятельно случай, когда командир-предатель приказывает одной паре честных заместителей атаковать, а другой - отступать, используя протокол $BG(1)$). Поэтому мы будем считать, что заранее оговорен «план по умолчанию», которому все следуют в случае «ничьей».

Лемма. Для любых натуральных чисел k, m протокол $BG(m)$ обладает исполнительностью, если $n \geq 2k + m + 1$, а предателей не больше k.

Доказательство. Индукция по m.

База: $m = 0$**.** В самом деле, все честные заместители поступят в соответствии с полученным правильным приказом.

Переход: $m - 1 \mapsto m$**.** Всякий честный заместитель, получив приказ, рассылает его коллегам по $BG(m-1)$. При этом участников этой рассылки $n - 1$ (все, кроме командира), то есть не менее $2k + m$, а предателей среди них по прежнему не более k. По предположению индукции, в этом случае $BG(m-1)$ обладает исполнительностью, а стало быть, честные заместители правильно передадут коллегам правильный приказ командира. В этом случае у каждого заместителя окажется не менее $k + m + 1$ правильных копий приказа (не более чем k предательских копий окажутся неправильными), а это в любом случае больше половины. Таким образом, каждый честный заместитель выполнит правильный приказ.

Доказательство завершено.

Теперь докажем основную теорему.

Теорема о корректности $BG(m)$**.** Для любого натурального m протокол $BG(m)$ обладает согласованностью и исполнительностью, если $n \geq 3m + 1$, а предателей не более m.

Доказательство. Исполнительность следует из леммы при $k = m$. Согласованность будем доказывать по индукции по m.

База: $m = 0$**.** Раз предателей нет вовсе, то все получат одинаковый приказ и выполнят его.

Переход: $m-1 \mapsto m$**.** Если командир честен, то согласованность следует из исполнительности (все правильные приказы одинаковы), а исполнительность уже доказана. Пусть теперь командир предатель. Заместителей не менее $3m$, а предателей среди них - не более $m-1$, поэтому по предположению индукции протокол $BG(m-1)$ среди заместителей обладает согласованностью. Поэтому копия приказа, пересланная каждым из заместителей коллегам, будет принята всеми одинаково. Это означает, что все честные заместители получат одно и то же представление о приказах, полученных другими заместителями. Это, в свою очередь, означает, что у честных заместителей будет совпадать «сводка приказов». Но в этом случае они все примут одинаковое решение.

Доказательство завершено.

Как мы видим, построенный нами протокол работает и отвечает всем требованиям при соблюдении приведенных выше условий (менее трети предателей). Можно доказать, что для случая, когда предателей не менее трети, протокол такого вида невозможен. Это доказательство сводится к уже рассмотренному случаю «один из трех».

Как легко видеть, протокол довольно громоздок. Можно доказать, что при фиксированном m число сообщений в протоколе $BG(m)$ асимптотически равно n^{m+1} (в случае командира и заместителей) или n^{m+2} (в случае генералов) при большом n.

В конце конспекта приведено два примера для $n = 4$, $m = 1$.

5 Пример работы византийского протокола

Пусть $n = 4$, $m = 1$. Может быть два принципиально различных случая: когда предатель - командир и когда предатель - один из заместителей.

Командир. Желая ослабить наступление, командир приказывает двум заместителям атаковать, а третьему - отступать. Согласно протоколу $BG(1)$, заместители рассылают друг другу копии приказа, используя протокол $BG(0)$, то есть, посылают их прямым текстом. В итоге первый заместитель получает следующую сводку:

Командир	Атаковать!
Второй зам.	Командир приказал атаковать!
Третий зам.	Командир приказал отступать!

Согласно $BG(1)$, первому заместителю следует атаковать. Аналогичная ситуация складывается у второго заместителя. А вот сводка для третьего:

Командир	Отступать!
Первый зам.	Командир приказал атаковать!
Второй зам.	Командир приказал атаковать!

Таким образом, третий заместитель тоже будет атаковать, несмотря на преступный приказ командира, и тем самым обеспечит согласованность.

Заместитель. Пусть предателем является третий заместитель. Желая запутать остальных, он говорит, что командир приказал ему отступать, когда на самом деле приказ был атаковать. В таком случае первый заместитель получает следующую сводку:

Командир	Атаковать!
Второй зам.	Командир приказал атаковать!
Третий зам.	Командир приказал отступать!

Сводка второго заместителя будет выглядеть так же. Как мы видим, гнусному предателю не удалось запутать доблестных воинов, которые смело пойдут в атаку.

Было бы интереснее, конечно, привести протокол $BG(2)$, но он, как известно, работает при $n \geq 7$, так что в нем участвует не менее 156 сообщений.