Лекция N 1 курса Базовые протоколы “Современные задачи криптографии”

Юрий Лифшиц *

20 Сентября 2005г.

“- 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 Введение

Для начала рассмотрим, в чем, собственно говоря, проблемы и какие могут быть задачи. Неформально опишем такие задачи, как:

- Контроль над ракетой (разделение секрета)
- Электронная ставка
- Развод по телефону

Обсудим, как они обычно решаются в бытовой жизни и подумаем, можно ли принципиально решать поставленные задачи, когда речь идет не о реальном общении, а об электронном общении.
Затем дадим формальную постановку задачам, т.е. опишем соответствующие протоколы, и реализуем их.

*Законспектировал лекцию **Кудинов Владислав**

План лекции:

1. Неформальные постановки
   - Контроль над ракетой
   - Электронная ставка
   - Развод по телефону
2. Реализации протоколов
   - Схема Блэкли
   - Схема Шамира
   - Привязка к биту I
   - Привязка к биту II
   - Подбрасывание монетки по телефону
3. Родственные задачи и подведение итогов

2 Неформальные постановки

2.1 Разделение 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?

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.

2.2 Электронная ставка

Задача. Алиса - очень азартная девушка и не может жить без риска, поэтому хочет сделать ставку у букмейкера Боба, но при этом хочет чтобы еч не обманул,но и Боб не хочет быть в дураках, т.е. необходимо выполнение следующих свойств:

- **Секретность:** Боб не сможет узнать, на кого поставила Алиса
- **Связанность:** Алиса не может изменить свою ставку

Жизненное решение: отдать ставку в запечатанном конверте:

Наша задача: конверт - это хорошо, но нам нужна электронная версия этого протокола.

Возможно ли это?

Ответ: конечно, иначе вас бы и не спрашивали. И о том, как это сделать, как раз и рассказывается в этой статье.

2.3 Развод по телефону

Задача. Это еще одна очень интересная, а главная насущная для многих задача, суть ее в следующем: Алиса разводится с Бобом, и им нежно полюбовно поделить имущество и детей. Оба претендуют как на BMW, так и на детей, и никто не хочет уступать. Что делать?

Человеческое решение: первое, что приходит в голову - это, конечно, подбросить монетку.

Но, что делать, если дошло до того, что Алиса и Боб уже видеть друг друга не могут и общаются только по телефону(ICQ).

Тут встает резонный **вопрос:** возможно ли электронное подбрасывание монетки?

И как всегда, **ответ** - ДА.

2.4 Море протоколов

На самом деле, каждый день нам приходиться использовать огромное количество протоколов, о которых мы даже не задумываемся, которые мы реализуем каждый по-своему бытовыми способами. Но, в связи с бурным переходом на электронное общение, все эти протоколы появляются и в электронном пространстве. Вот только часть из них, которые мы собираемся осветить в данном курсе лекций и на семинарах, и в частности, в данной статье.

Протоколы:

- Одновременное подписание договора
- Одновременный обмен секретами
- Цифровая подпись
- Коллективное принятие решений
- Раздача карт по телефону
- Анонимность сообщений
- Электронные выборы
- Электронные деньги

3 Реализации протоколов

3.1 Криптографический протокол

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*

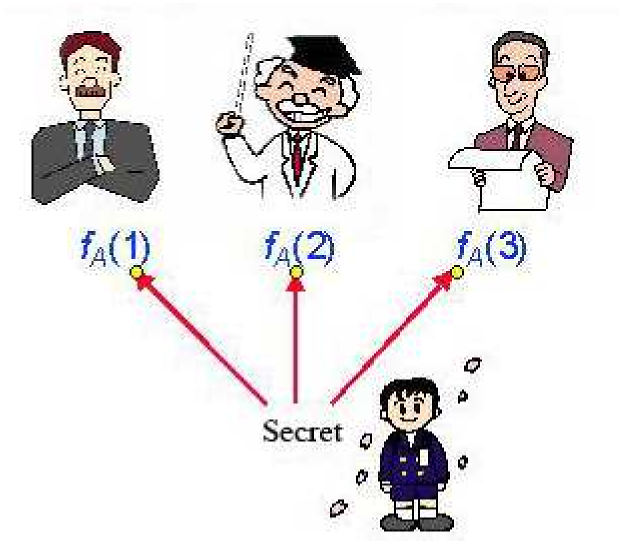
- *неотслеживаемости*

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.

Cryptography.Ru

3.2 Разделение секрета

3.2.1 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.

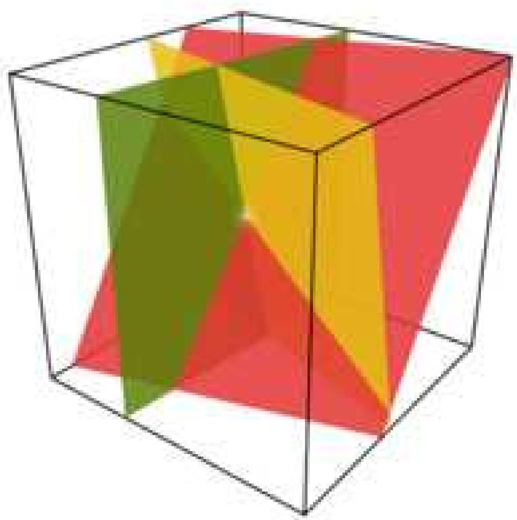
Теперь запишим формальные требования, которым должен удовлетворять протокол:

- 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

3.2.2 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"?

3.2.3 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 $i = 1, 2, \ldots, n$ 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:

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

Выписываем систему уравнений:

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

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 $x_1, \ldots, x_t$ 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:**

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

3.2.4 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:

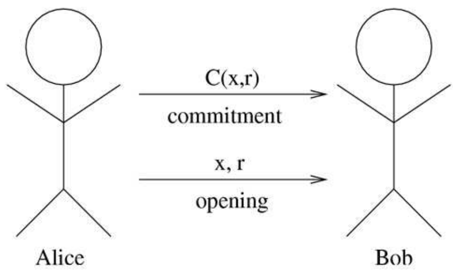
– Одноразовость
– Возможность мошенничества со стороны раздающего
– Возможность мошенничества со стороны участников
– Необходимость сборки секрета перед его использованием

3.3 Привязка к биту I

3.3.1 Диффи и Хеллман

В 1976 году Диффи и Хеллман совершили революцию в криптографии и создали целое новое направление в криптографии. По большому счету они придумали алгоритм с открытым ключом, хотя до конца его и не реализовали. До этого идеалогия была следующая: чтобы защитить строчку длины l, нужен ключ такой же длины l, т.е. для защиты гигабайта нужен гигабайтный ключ. Причем раньше, когда кто-то придумывал алгоритм - ему надо было доказывать, что его алгоритм действительно хороший, либо математически, либо временем.
Диффи и Хеллман предложили использовать уже существующие задачи, которые никто не умеет быстро решать(например, разложение чисел на множители(дискретный логарифм)), т.е. любой алгоритм, быстро взламывающий криптосистему X, можно переделать в алгоритм быстро решающий задачу P (про которую никто не верит, что ее можно легко решить). Это и называется вычислительной стойкостью алгоритма.

3.3.2 Постановка задачи.



Надеюсь, вы еше не забыли задачу о „ставке“, когда Алиса хочет сделать ставку у Боба, так чтобы он не узнал, какую она сделала ставку, а она не могла изменить ставку. Сейчас мы приведем несколько алгоритмов, как решать эту задачу. Общий принцип состоит в следующем: Алиса посылает Бобу $C(x, r)$, а потом, когда это понадобится, Алиса посылает Бобу x и r и Боб может убедиться, что Алиса действительно не жульничала.
Т.е $C(x, r)$ - известная функция от 2 аргументов. Боб не знает, ни r, ни x.

Замечание 3. Для простоты будем считать, что $x \in 0, 1$

Подумаем, когда кто может жульничать:

1. Боб может догадаться, какой бит(x) ему послали.
2. Алиса может схитрить, когда открывает x и r, она может так подобрать r, чтобы сказать, что она послала выигрышный x'

Для того, чтобы оценить насколько и как алгоритм защищен от подобных проделок, вводятся следующие понятия:

1. **Секретность** - это то, насколько протокол защищен от жульничества со стороны Боба.
   - **Безусловная секретность** распределения $C(0, r)$ и $C(1, r)$ совпадают, т.е. „0-множество“ и „1-множество“ - совпадают - это означает, что если существует 10 различных r, т.ч. $a = C(0, r)$, для кого-то $a \Rightarrow$ существует 10 различных r, т.ч. $a = C(1, r)$, для этого же a.
   - **Вычислительная секретность:** распределения $C(0, r)$ и $C(1, r)$ трудноразличимы, т.е. не существует алгоритма, который по $C(x, r)$ скажет x с вероятностью отличной от $\frac{1}{2}$.
2. - **Безусловная связанность:** бит b однозначно определен через $C(b, r)$, т.е. „0-множество“ и „1-множество“ - не пересекаются - это означает, что если существует r, т.ч. $a = C(0, r)$, для кого-то $a \Rightarrow$ не существует r, т.ч. $a = C(1, r)$, для этого же a.

- **Вычислительная связанность:** вычислительно трудно подобрать пару r_0, r_1, т.ч. $C(0, r_0) = C(1, r_1)$

3.3.3 Односторонняя перестановка

Для формального описания алгоритма нам придется для начала ввести одно определение:

Определение 1. Биективная функция $F : \{0,1\}^n \to \{0,1\}^n$ называется односторонней перестановкой, если:

1) Функция F вычислима за полиномиальное время
2) Не существует полиномиального алгоритма, который верно вычисляет F^{-1} *с хорошей вероятностью*

2') Существует предикат $h : \{0,1\}^n \to \{0,1\}$, т.ч. по $F(x)$ *трудно* вычислить $h(x)$

Замечание 4. Хорошая вероятность: $F(m)$ называется пренебрежимо малой, если: $\forall p(n) \quad \exists n_0 \forall n > n_0 F(n) < \frac{1}{p(n)}$

Замечание 5. Можно переделать F, т.ч. из 1) и 2) $\Rightarrow$ 2')

3.3.4 Привязка к биту I

Подготовительный шаг: фиксируем одностороннюю перестановку F и предикат h.

Привязка: Алиса выбирает случайное r, посылает Бобу $C(b, r) = (F(r), b \oplus h(r))$

Открытие секрета: Алиса посылает r, Боб вычисляет $F(r)$ и сравнивает с тем, что Алиса послала до этого, затем вычисляет $h(r)$ и т.к. $h(r) \oplus b \oplus h(r) = b$ узнает b.

Свойства схемы:

- Безусловная связанность.

  $C(b_1, r_1) = C(b_2, r_2) \Rightarrow F(r_1) = F(r_2) \Rightarrow h(r_1) = h(r_2)(1)$

  $C(b_1, r_1) = C(b_2, r_2) \Rightarrow b_1 \oplus h(r_1) = b_2 \oplus (r_2)(2)$

  $(1)\&(2) \Rightarrow b1 = b2$

- Вычислительная секретность, т.к. по свойству односторонней перестановки - зная только $F(r)$ *трудно* вычислить $h(r)$.

3.3.5 Привязка к биту II

Приведем еще один алгоритм для реализации данного протокола, который обладает безусловной связанностью и вычислительной секретностью, а наоборот - вычислительной связанностью и безусловной секретностью.

Подготовительный шаг: Фиксируем простое p и первообразный корень g

Замечание 6. g - первообразный корень p, если $g^1, g^2, g^{\cdot} \ldots, g^p$ - множество всех остатков, т.е. числа $1, 2, \ldots, p$ в каком-то порядке

Привязка в два шага:

- Боб выбирает случайное q
- Боб посылает Алисе $y = g^q$
- Алиса выбирает случайное r
- Алиса посылает Бобу $C(b, r) = y^b g^r$

Замечание 7. Все действия происходят по модулю p

Открытие секрета: Алиса посылает Бобу r

Свойства схемы:

- Вычислительная связанность
- Безусловная секретность

Задача 3. Проверить эти свойства.

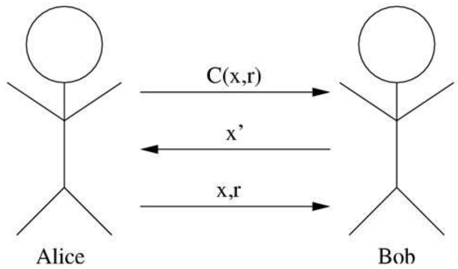
Пример 1. $p = 7, g = 3$

1. Боб выбирает $q = 4$
2. Боб посылает Алисе $y = 4$
3. Алиса выбирает r
4. Алиса посылает Бобу либо 3^r, либо $4 * 3^r$, например, получиться 5, Боб не может догадаться какой бит ему послали, потому что $5 = 4^0 * 3^5, 5 = 4^1 * 3^1$, т.е. это может быть как 0, так и 1.
5. Алисе очень трудно жулить, потому что ей придется находить q, т.е. научиться решать задачу о дискретном логарифме.

Задача 4. Могут ли одновременно достигаться и безусловная связанность и безусловная секретность?

3.4 Подбрасывание монетки по телефону

3.4.1 Подбрасывание монетки



Шаги:

1. Алиса подкидывает монетку и в связанном состоянии
2. посылает результат x Бобу
3. Боб посылает догадку x' Алисе
4. Алиса открывает x

С помощью привязки к биту делается очень легко.

4 Родственные задачи

- Визуальная криптография: чтобы увидеть картину необходимо наложить друг на друга ровно n черно-белых бумажек, иначе получается абра-кадабра.
- Проверяемое разделение секрета
- Пороговая криптография

Задача 5. 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?

5 Итоги

Если не запомните ничего другого:

- Схемы разделения секрета "t из n" могут быть основаны на интерполяции многочленов или пересечении гиперплоскостей.

- Привязка к биту может быть безусловно связанной и вычислительно секретной или наоборот
- Подбрасывание монетки делается с помощью привязки к биту