kaspersky.academy

Лекция 8.

Протоколы

Онлайн-курс по математике в информационной безопасности

kaspersky.academy

Лекция 8. Протоколы

Привет!

Что ж, мы рассмотрели много симметричных шифров и теперь самое время поговорить о **протоколах**.

Мы выработаем ключи, используя **незащищенные каналы связи**, но сделаем это настолько ловко, чтобы на самом деле их не передавать. Звучит интригующе? Давайте разбираться!

Наш план на эту лекцию:

Поехали!

Возвращаемся в Вестерос: протокол Диффи-Хеллмана

Санса Старк и **лорд Варис** живут на разных концах Вестероса. И хотят переписываться друг с другом да еще отправлять свои письма с помощью воронов – по незащищенному каналу связи и безо всякой возможности обменяться ключами!

Многого хотят?

Ну, во всяком случае, математики **Диффи и Хеллман** решили эту проблему и придумали правила, следуя которым люди теперь могут вырабатывать секретные ключи. Когда мы говорим «следовать правилам», мы имеем в виду **протокол** «делай раз, делай два, делай три», то есть некоторую последовательность действий.

Рисунок 1. Уитфилд Диффи (слева) и Мартин Хеллман (справа) - создатели протокола Диффи-Хеллмана

Протокол – это договоренность участников о том, что они будут делать. Например, следуя криптографическому протоколу, они могут выработать общий секретный ключ для шифрования своих сообщений.

Вернемся к Сансе с Варисом. Напомним их задачу – организовать передачу данных по незащищенному каналу связи.

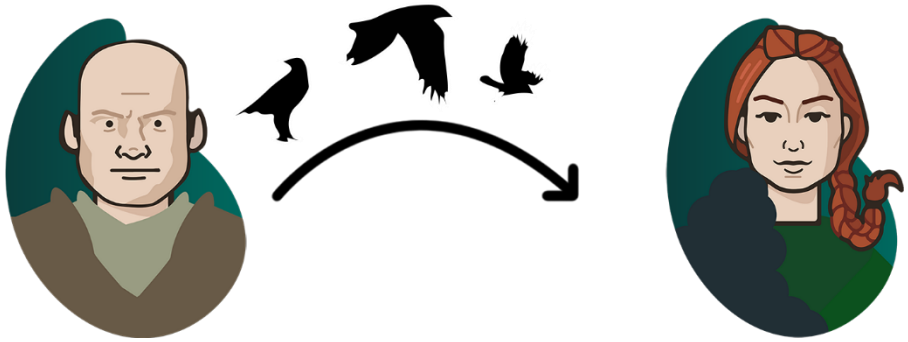


Рисунок 2. У Сансы и лорда Вариса в распоряжении только незащищенный канал связи.

В этом случае **Квиберн** может перехватить их переписку… И узнать их секреты:

Рисунок 3. Квиберн перехватывает послание Вариса по незащищенному каналу связи

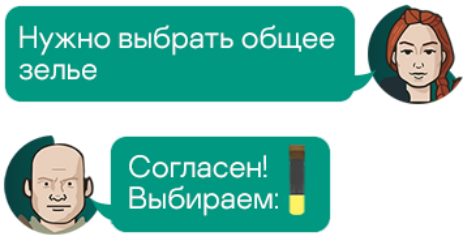
Что делать?

Допустим, у Сансы есть своя алхимическая лаборатория в Винтерфелле, а у лорда Вариса – своя. Но, знаете, все алхимические лаборатории Вестероса выглядели примерно одинаково, и все зелья, которые были у Сансы, были и у Вариса.

Санса и Варис договорились, будут следовать протоколу Диффи-Хеллмана. Давайте сначала просто понаблюдаем, что они делают – а потом разберемся в логике их действий.

Шаг 1:

Санса и Варис выбирают **общее открытое зелье** – любой человек может узнать, что это за зелье.

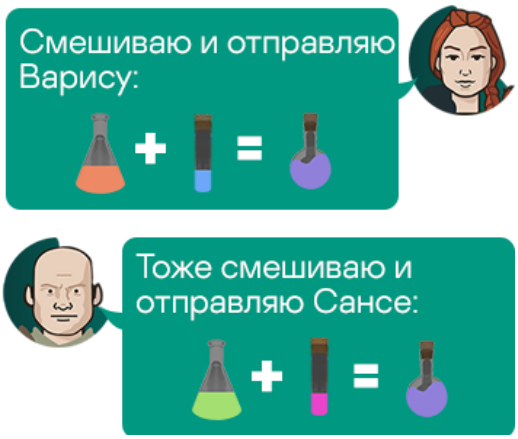


Шаг 2:

Санса выбирает **свое секретное зелье,** и Варис выбирает свое секретное зелье.

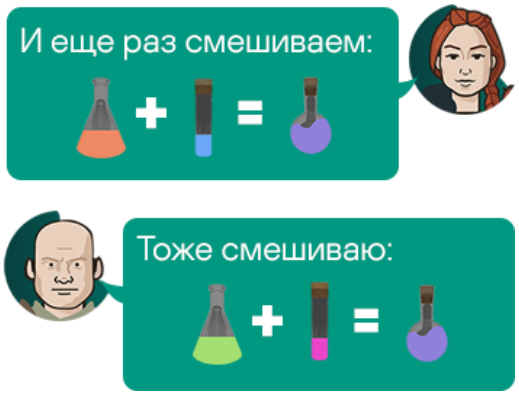
Шаг 3:

Санса перемешивает **свое секретное зелье с общим открытым зельем** и отправляет смесь Варису. Варис поступает так же и отправляет свою смесь Сансе.



Шаг 4:

После того как Санса получила смесь Вариса, она добавляет в эту смесь **свое секретное зелье.** А Варис – добавляет свое зелье в смесь Сансы.



Так что же сделали Санса и лорд Варис? По **незащищенному каналу связи** передавались следующие зелья: общее открытое зелье, смесь Сансы и смесь Вариса. А **общее секретное зелье** Вариса и Сансы состоит из секрета Сансы, секрета Вариса и открытого общего зелья.

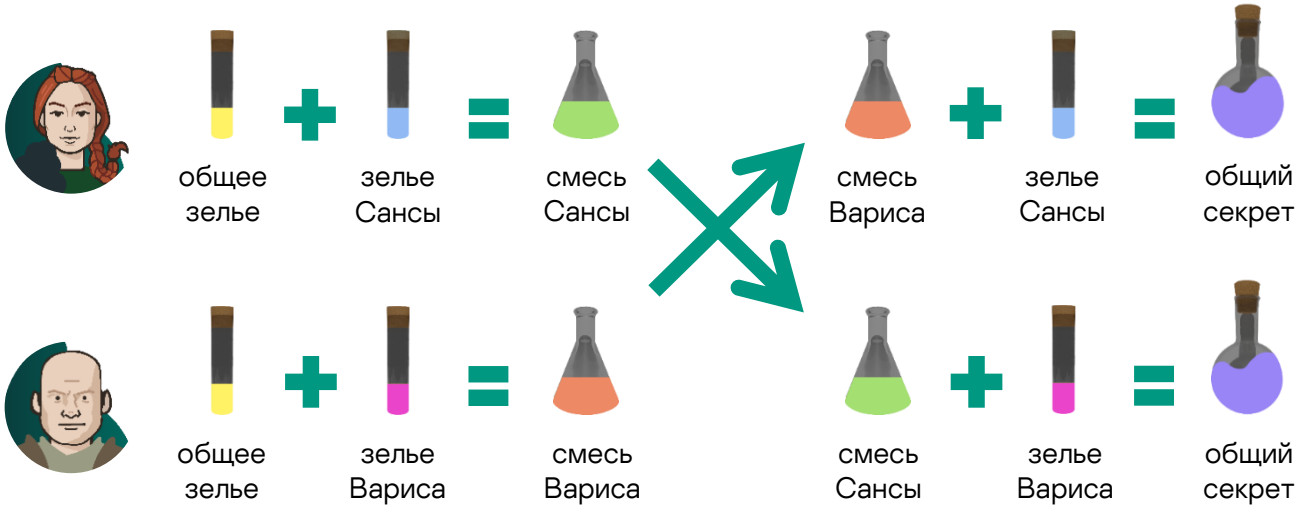


Рисунок 4. Протокол Сансы и Лорда Вариса

Сейчас вы увидели **протокол Диффи-Хеллмана** в действии. Несколько важных выводов:

1. Это **общее секретное зелье** Вариса и Сансы и будет их **ключом**, которое они смогут использовать для шифрования своих секретов.
2. При этом ни Санса, ни Варис не выдали **свои секретные зелья,** которые выбирали вначале.
3. Даже при перехвате **общего секретного зелья** понять, что именно использовалось для смеси, **практически невозможно** – нам легко смешать зелья, но разделить их обратно в действительности нереально.

Как работает протокол Диффи-Хеллмана?

Давайте рассмотрим протокол с точки зрения математики. Возьмем выражение:

$$g^x \bmod p$$

Это преобразование и будет являться смешиванием зелий.

Числа g и p – это общее открытое зелье Сансы и Вариса, их **открытый ключ,** то есть числа, не являющиеся секретными. x – приватный, или **закрытый ключ** каждого из участников.

Число p – простое, а g – первообразный корень по модулю этого простого числа. Если вы вдруг не помните, что это такое, загляните в лекцию по арифметике :)

Рассмотрим на примере: Санса с Варисом решили взять $p = 23$, $g = 5$.

Санса и Варис выбирают свои секретные зелья – это число x. В качестве x можно выбрать любое число, но у нас их два – для Сансы и для Вариса – поэтому возьмем переменные a и b. Санса выбрала число $a = 2$, а Варис взял себе число $b = 3$. Дальше каждый из них вычисляет выражение:

$$g^x \bmod p$$

и отправляет своему собеседнику число, которое получилось (смесь зелий). Пусть A – смесь зелий Сансы, а B – смесь зелий Вариса. Тогда:

$$A = g^a \bmod p = 5^2 \bmod 23 = 2$$

– это значение Санса отправит Варису

$$B = g^b \bmod p = 5^3 \bmod 23 = 10$$

– это значение Варис отправит Сансе

Теперь давайте проведем ревизию зелий и посмотрим, что появилось в лаборатории Сансы и Вариса.

Итак, вот что есть у Сансы:

- общее открытое зелье (5, 23)
- смесь Сансы ($A = 2$)
- смесь Вариса ($B = 10$)
- секретное зелье Сансы ($a = 2$)

А вот что есть у Вариса:

- общее открытое зелье (5, 23)
- смесь Сансы ($A = 2$)
- смесь Вариса ($B = 10$)
- секретное зелье Вариса ($b = 3$)

Как вы видите, секретные зелья Вариса и Сансы никак не передавались и остались только у них.

Теперь Санса и Варис вычисляют секретный ключ. Санса вычисляет значение:

$$B^a \bmod p = 10^2 \bmod 23 = 8,$$

А Варис:

$$A^b \bmod p = 2^3 \bmod 23 = 8$$

Как видите, ключ получился одинаковым. Проверим, что $B^a \bmod p$ и $A^b \bmod p$ – это действительно один и тот же общий секретный ключ.

Что делает Варис:

$$A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p$$

Что делает Санса:

$$B^a \bmod p = (g^b \bmod p)^a \bmod p = g^{ab} \bmod p$$

И то, что получается у Вариса и Сансы, – это одно и то же число! Теперь мы понимаем, как работает протокол Диффи-Хеллмана.

Задача дискретного логарифмирования

...или: «Почему взломать ключ в протоколе Диффи-Хеллмана сложно?» Давайте разбираться.

Варис и Санса помнят, что числа g и p нельзя выбирать любыми. Для выражения $g^x \bmod p$ результат зависит от выбранных чисел. **g должно быть первообразным корнем по модулю p** – это означает, что при возведении числа g в степень можно будет получить *все* остатки от деления по модулю p: 0, 1, 2, 3, ..., $p-1$

Если g не будет первообразным корнем по модулю p, то разных остатков мы получим меньше. Допустим, Санса и Варис возьмут модуль равным 7: $p = 7$, а $g = 2$. Тогда мы получим такие остатки от деления: 1, 2, 4.

$$2^1 \bmod 7 = 2 = \bmod 7 = 2$$
$$2^2 \bmod 7 = 4 \bmod 7 = 4$$
$$2^3 \bmod 7 = 8 \bmod 7 = 1$$
$$2^4 \bmod 7 = 16 \bmod 7 = 2$$
$$2^5 \bmod 7 = 32 \bmod 7 = 4$$
$$2^6 \bmod 7 = 64 \bmod 7 = 1$$

Санса и Варис смогут получить только три различных числа в качестве своего **общего секретного ключа.**

А Варис с Сансой уже знают, что чем меньше перебирать, тем быстрее взламывается шифр. И чтобы Квиберн помучился и подольше поперебирал бы возможные ключи, Санса и Варис возьмут **первообразный корень.**

Допустим, они решили взять число $g = 3$:

$$3^1 \bmod 7 = 3 \bmod 7 = 3$$
$$3^2 \bmod 7 = 9 \bmod 7 = 2$$
$$3^3 \bmod 7 = 27 \bmod 7 = 6$$
$$3^4 \bmod 7 = 81 \bmod 7 = 4$$
$$3^5 \bmod 7 = 243 \bmod 7 = 5$$
$$3^6 \bmod 7 = 729 \bmod 7 = 1$$

В этом случае количество возможных секретных ключей будет вдвое больше, значит, Квиберну придется перебирать дольше.

Что нужно знать Квиберну, чтобы все же взломать ключ? Ему нужно знать хотя бы один из приватных ключей – или ключ Сансы, или ключ Вариса. Значит, в выражении

$$y = g^x \bmod p$$

ему придется искать x.

$$x = \log_g y \bmod p$$

Квиберн ищет степень числа и хочет логарифмировать y. И ни современные ученые, ни современники Квиберна – никто пока не знает алгоритмов, которые могли бы это делать лучше, чем **алгоритм полного перебора.**

Это сложная задача. Представьте, что в записи числа p количество цифр – 10^{100}. Это сто один знак в числе! Перебирать придется до тех пор, пока не вылупятся новые драконы.

Атака «Человек посередине»

Практически отчаявшийся **Квиберн** решил подойти к проблеме взлома с другой стороны.

Если Квиберн может не только перехватывать сообщения Сансы и Вариса, но также и отправлять свои письма, **он сможет атаковать протокол Диффи-Хеллмана.**

Квиберн перехватит письмо Сансы и вместо ее послания отправит Варису свое. Значит, Варис подумает, что он общается с Сансой, а Санса решит, что ей пишет Варис.

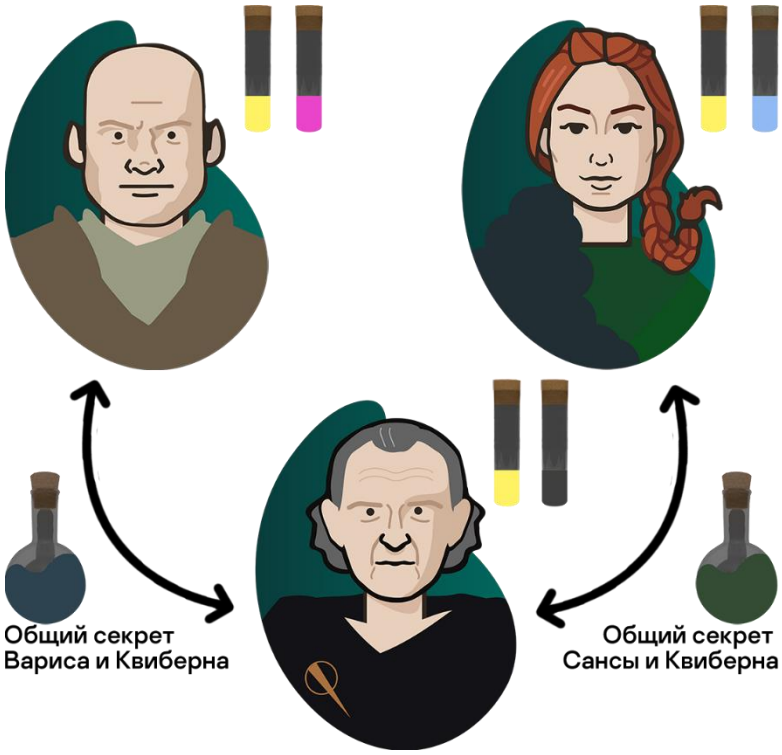


Рисунок 5. Атака "Человек посередине"

Тем временем Квиберн будет находиться где-то между Королевской гаванью и Винтерфеллом и общаться одновременно и с Сансой, и с Варисом, вырабатывая **общие секретные ключи** с каждым из них – это два разных общих секретных ключа: ключи «Санса-Квиберн» и «Квиберн-Варис». А Общего секретного ключа «Санса-Варис» теперь вообще не существует.

Квиберн вклинивается в переписку и теперь может читать как сообщения Сансы, так и сообщения Вариса.

Краткий вывод, или Рассказ о том, что может пойти не так

Протокол Диффи-Хеллмана наконец-то позволил человечеству **не искать защищенные каналы связи** для передачи ключей. И это отличные новости!

А плохая новость в том, что если злоумышленник может не только читать сообщения из канала связи, а еще и активно участвовать в переписке, то **протокол Диффи-Хеллмана нас не спасет.** А теперь – всем решать задачки!