kaspersky.academy

Лекция 6.

Шифр RSA

Онлайн-курс по математике в информационной безопасности

kaspersky.academy

Лекция 6. Шифр RSA

Привет!

До этой лекции мы с вами рассматривали **симметричные шифры**, в которых ключи зашифрования и расшифрования совпадают. Но вы уже знаете самую большую сложность использования таких шифров – у вас в запасе должен быть целый дракон, чтобы доставлять ключи по защищенному каналу :) Не знаю, как у вас, но у трех крутых математиков в прошлом веке своего дракона не было, и пришлось что-то придумывать.

Давайте обо всем по порядку.

Наш план на эту лекцию:

Поехали!

О шифре RSA

Вернемся к трем математикам. Эти парни – **Рональд Ривест, Ади Шамир и Леонард Адлеман,** а потому и шифр, который они придумали, называется **RSA** – по первым буквам их фамилий (Rivest, Shamir, Adleman),

Рисунок 1. Слева направо: Ади Шамир, Рональд Ривест, Леонард Адлеман

Но ребята могли не скромничать, добавляя в название только первые буквы, потому что шифр и правда классный – **он решает проблему передачи ключей по незащищенному каналу с воронами.**

Вообще-то, изобретение RSA не абсолютное ноу-хау, потому что еще до RSA был придуман протокол Диффи – Хеллмана. А Ривест, Шамир и Адлеман нашли ему практическое применение.

Кстати, Вестерос там или не Вестерос, а все-таки и у нас свои «вороны» есть – все протоколы передачи данных, которые используются в интернете. И если мы драконов не изобретем, то нам хотя бы придется одеть в броню воронов – мы будем шифровать все данные, которые передаются по сети.

И так как к каждому серверу, с которым вы устанавливаете соединение, вы лично не подойдете и ключ не передадите, будем использовать **асимметричное шифрование** и **протоколы выработки ключей**. Теперь можно сидеть дома на диване и не бояться, что сообщения передаются несекретно.

Итак, **RSA – наш первый пример асимметричного шифра** – ключ зашифрования и ключ расшифрования для этого алгоритма будут различными.

Вспоминаем асимметричное шифрование

Давайте прежде всего вспомним, что такое асимметричное шифрование в идеологическом смысле.

Как вы помните из вводной лекции, **Варис** очень хочет рассказать **Сансе** важный секрет про Джона Сноу. Но Дейнерис не спит и следит за ним. Поэтому Варис просит Сансу сделать такой сундук, который закрывался бы методом захлопывания (опустил крышку – и считай, закрыл), а открывался бы с помощью огромного тяжелого ключа.

Шаг 1. Санса делает такой сундук и отправляет Варису – в открытом виде, конечно же, иначе зачем Варису сундук, который он открыть не сможет? А еще она делает ключ, но ключ оставляет себе. Когда Варис кладет письмо в сундук и захлопывает его, никто, даже сам Варис, это письмо теперь не сможет достать.

Шаг 2. Сундук отправляется обратно к Сансе, а она открывает его своим ключом. В нашей истории сундук – это **открытый ключ Сансы Старк**, который может получить любой желающий. Даже Дейнерис.

А тяжелый железный ключ – это **приватный ключ Сансы Старк.** Варис шифрует, или скрывает, свое сообщение с помощью публичного ключа – он кладет письмо в сундук и захлопывает крышку.

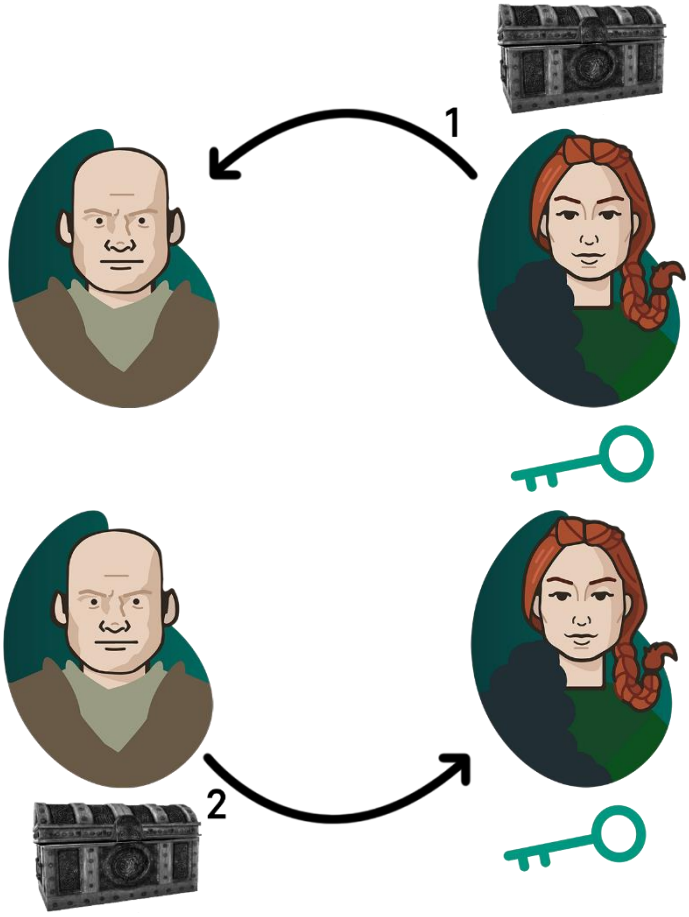

Рисунок 2. Работа ассиметричного шифра

Санса открывает сундук своим приватным ключом, который она никому никогда не отдавала. И ключ этот сторожили злые псы в Винтерфелле.

Я надеюсь, теперь вы понимаете, насколько все серьезно. А сейчас пришло время добавить математики!

RSA с точки зрения математики: что делает Санса?

Что же делает Санса Старк холодными зимними вечерами в Винтерфеле?

1. **Сначала Санса генерирует открытый (публичный ключ).** Она хочет взять два простых числа. Пусть это будет $p = 11$ и $q = 5$. Санса вычисляет n – произведение чисел p и q:

$$n = p \cdot q = 11 \cdot 5 = 55$$

Санса вычисляет функцию Эйлера:

$$\varphi = (p - 1) \cdot (q - 1) = 4 \cdot 10 = 40$$

Санса выбирает число e, которое подходит под описание:

- оно должно быть меньше φ
- оно должно быть взаимно простым с φ

Остаются варианты: 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39.

Санса решила выбрать $e = 3$. Это число называется **открытой экспонентой.**

Теперь пара чисел (e, n) **– это открытый ключ Сансы.** Она отправляет его Варису, чтобы он смог зашифровать свое сообщение.

2. **Наконец, Санса генерирует закрытый (приватный ключ),** чтобы повесить его на стену в псарне и близко не подпускать никого.

Ей нужно вычислить число d, обратное e по модулю φ. Вы, конечно, помните, что взаимно простые числа – это такие, у которых остаток от деления по модулю φ произведения $d \cdot e$ должен быть равен 1. Вот так:

$$(d \cdot e) \bmod \varphi = 1$$

Санса уже устала писать формулы при свете свечи, но остался последний шаг. Она вычисляет:

$$(d \cdot 3) \bmod 40 = 1$$

d может быть равно 27:

$$(3 \cdot 27) \bmod 40 = 1$$

Пара (d,n) – **это приватный ключ,** и Санса наконец может пойти и выпить немного чая...

RSA с точки зрения математики: что делает Варис?

Что тем временем делает Варис в Королевской гавани?

Пусть **сообщение Вариса** $P = 29$. 29 – это код сообщения «Джон Сноу – наследник Вестероса». А еще Варис получил **открытый ключ Сансы:**

$$(e,n) = (3,55)$$

Варис возводит сообщение P в степень e по модулю n и получает зашифрованное сообщение E.

$$E = P^e \bmod n$$

Зашифрованное сообщение Вариса теперь выглядит так:

$$29^3 \bmod 55 = 24$$

Условный код 55 означает «Некоторые дети терпеть не могут молоко». Полученное **зашифрованное сообщение** $E = 24$ Варис отправляет Сансе.

Нужно только помнить, что сообщение $P = 29$ не должно быть больше модуля $n = 55$, потому что остатки от деления на n всегда будут меньше P и сообщение Вариса невозможно будет расшифровать.

Как Санса узнает секрет Вариса?

Санса получила послание Вариса: у нее есть секретное зашифрованное сообщение Вариса $E = 24$ и **свой закрытый ключ** $(d, n) = (27,55)$.

Мы знаем, что открытый ключ *(e, n)* не может расшифровать сообщение. А закрытый ключ Сансы стерегут ее псы, поэтому она идет за ним. И теперь Санса берет в руки **закрытый ключ** и начинает открывать сундук.

Санса тоже будет возводить сообщение в степень, но вместо *e* она использует *d*.

$$P = E^d \bmod n$$

Санса возводит *E* в степень *d*:

$$24^{27} \bmod 55 = 29$$

– **и Санса получает сообщение Вариса**. О боже! Значит, Джон – наследник Вестероса?.. Что же делать?..

Взлом шифра RSA

Почему Варис и Санса верят, что Дейнерис не сможет раскрыть их секреты?

Маленький спойлер: **RSA – достаточно стойкий шифр,** а стойкость его основана на вычислительной сложности разложения числа на простые множители.

Представьте: случилось самое страшное и Дейнерис перехватила сообщение Вариса – а значит Дейнерис знает открытый ключ Сансы Старк *(e,n).* А что ей нужно знать, чтобы расшифровать сообщение? Правильно, закрытый ключ Сансы *(d,n)*!

Дейнерис знает математику и этот закрытый ключ может посчитать по формуле:

$$(d \cdot e) \bmod \varphi = 1$$

Но после того как Дейнерис написала формулу, она поняла, что не знает φ. А вот если бы она знала φ...

И вот теперь мы добрались до **задачи разложения чисел на простые множители.** Если Дейнерис найдет числа *p*, *q* – такие, что $p \cdot q = n$, она сможет узнать φ:

$$\varphi = (p - 1) \cdot (q - 1)$$

Но пока человечеству не известны суперэффективные способы разложения чисел на множители. Единственное, что у нас есть, – это метод брутфорс-атаки, или **полный перебор.**

А если эта задача кажется вам простой, вы всегда можете попробовать разложить на множители число ниже:

$$n = 27\,697\,011\,211\,241$$

Спойлер:

$$27\,697\,011\,211\,241 = 5\,262\,823 \cdot 5\,262\,767$$

Кстати, сами создатели RSA ради эксперимента опубликовали число n, у которого в записи было 129 знаков с предложением взломать их шифр. В итоге **их сообщение все-таки взломали** – спустя 15 лет после публикации! И для этого энтузиасты использовали большие вычислительные мощности.

Немного про будущее RSA

Сейчас физики, инженеры и математики работают над созданием квантовых компьютеров. Эти компьютеры будут делать все то же самое, что и современные компьютеры, плюс еще кое-что: они смогут раскладывать числа на простые множители быстрее, чем с помощью полного перебора. И если это случится, вся идея RSA сгорит в пламени дракона.

Но, надеемся, этого не случится прямо завтра, поэтому давайте пока учиться использовать RSA. Пора перейти к задачкам!