kaspersky.academy

Лекция 0.

Введение в криптографию

Онлайн-курс по математике в информационной безопасности

kaspersky.academy

Лекция 0. Введение в криптографию

Всем привет!

Не устали решать задачки по математике? Хорошие новости – мы наконец добрались до последнего, завершающего модуля по криптографии, и тут мы посмотрим с вами, как математика применяется в реальной жизни.

Наш план на эту лекцию:

Поехали!

Что такое криптография?

Слово «криптография» звучит круто. Но на самом деле **криптография** – это только одна из ветвей криптологии – большой науки о зашифровании и расшифровывании данных.

А еще есть **криптоанализ** – наука, которая исследует шифры на уязвимость и стойкость к атакам - проще говоря, криптоаналитики пытаются взломать шифры. Это не всегда плохие ребята, кстати. Криптографы хотят быть уверенными в стойкости своих шифров – а пока не попробуешь поломать, не проверишь!

Основные понятия в криптографии

А мы с вами отправимся в удивительный мир «Игры Престолов». Тут Дейнерис хочет написать письмо Джону Сноу. А отправлять это письмо она будет с **воронами** – это самый модный способ переписки в Вестеросе.

Давайте будем говорить, что сообщения отправляются по каналу связи. Этот канал связи – вороны – будет **незащищенным**: можно легко перехватить ворона и отобрать у него письмо.

Но у Дейнерис есть план Б! У нее есть **драконы**! Уж на дракона точно никто не рискнет напасть. Вот этот канал связи уже будет защищенным, до него не добраться.

Незащищённый канал связи: злоумышленник может читать сообщения, которые передаются по каналу

Защищённый канал связи: злоумышленник не может перехватывать сообщения в нем.

А что если все драконы Дейнерис улетели на охоту, а переписываться с Джоном Сноу ей все-таки хочется?

Ничего не остается, как только отправлять свои письма с воронами. Но теперь уже не в открытом виде, а в зашифрованном. Если письмо Дейнерис абсолютно понятно и каждый может прочитать его, мы говорим, что это **открытый текст.** А после того как Дейнерис возьмет **ключ** – секретную информацию – и применит его к открытому тексту, она получит нечитаемый набор символов, или **шифртекст.**

Ключ – это секретная информация для зашифрования или расшифрования.

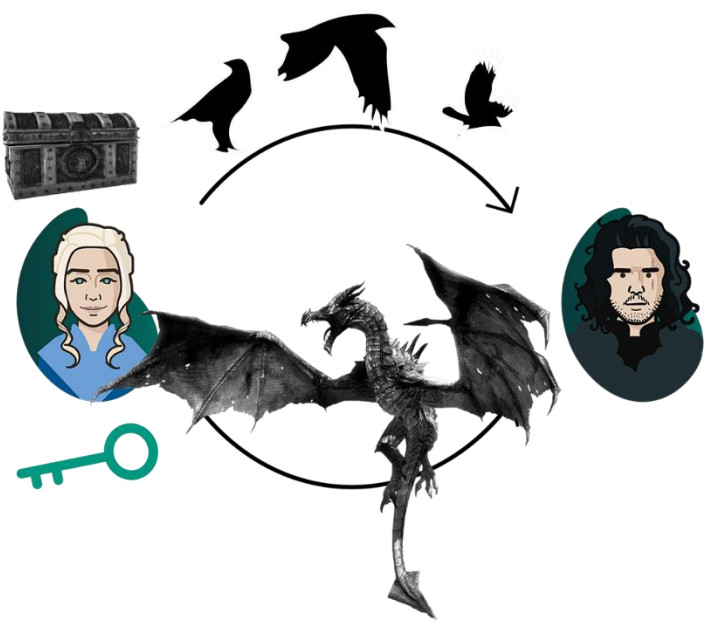
Шифрование – это отображение множества открытых текстов во множество шифртекстов

Давайте называть множество всех открытых текстов буквой P – plaintext, $P = \{\}$. А множество шифртекстов – буквой E – encrypted text, $E = \{\}$.

Симметричные и асимметричные шифры

Если для зашифрования и расшифрования подойдет один ключ, мы назовем шифр **симметричным.** Но если мы применяем симметричный шифр, то нам нужно будет еще как-то передать ключ, чтобы человек, получивший письмо, смог его прочесть.

Допустим, у Дейнерис есть сундук и ключ. И когда она кладет письмо в сундук и закрывает ключом, она **зашифровывает** его. **Сундук** она отправляет Джону Сноу по **незащищенному каналу** с воронами, а **ключ** отправляется по **защищенному каналу связи** – в пасти дракона.

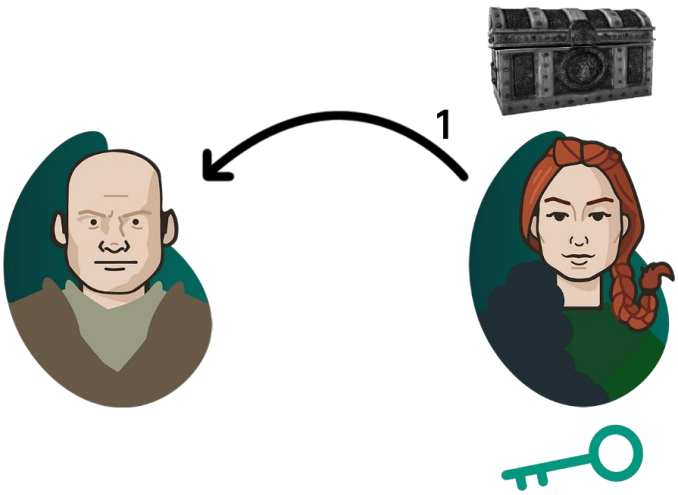


Сноу откроет сундук ключом и прочитает письмо Дейнерис.

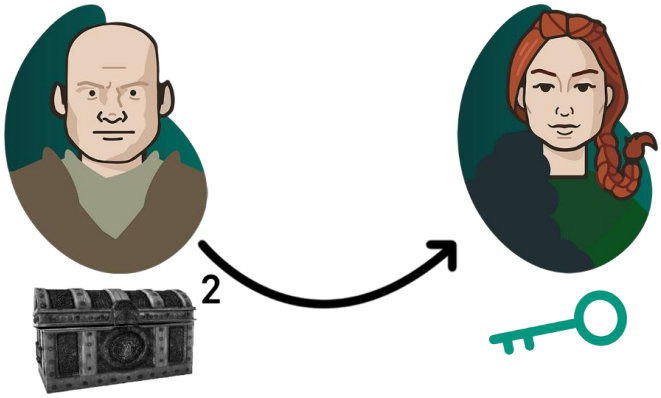
А вот если зашифровывать мы будем одним ключом, а расшифровывать другим, шифр уже станет **асимметричным**.

В конце долгой зимы в Вестеросе лорд Варис узнал, что именно Джон Сноу – истинный Таргариен. И Варис захотел написать письма всем лордам Вестероса, а первое письмо решил отправить Сансе Старк. Но он боялся, что письмо перехватит Дейнерис.

Тогда Варис просит Сансу сделать **сундук** и **ключ** от сундука. Санса делает сундук, который закрывается сразу, если захлопнуть крышку. А открыть его можно только с помощью ключа.



Шаг 1. Сундук Санса посылает Варису, а ключ оставляет себе и никому не отдает. И когда Варис положит свое письмо в сундук и захлопнет крышку, никто, даже сам Варис, не сможет его открыть.



Шаг 2. Варис отправит сундук с письмом Сансе, а Санса откроет его своим ключом, который не покидал Винтерфелл.

Так и работает ассиметричное шифрование.

Блочные и поточные шифры

Еще шифры можно разделить на **блочные** и **поточные**. Мы с вами будем рассматривать только поточные шифры, потому что для рассмотрения блочных нам понадобилось бы еще немного математики:) Но все-таки один простой пример блочного шифра мы приведем.

Давайте запишем слова **ДЖОН СНОУ** в две строки.

ДЖОН
СНОУ

А теперь давайте выпишем столбцы этого текста: ДСЖНООНУ.

Видите, мы шифруем сообщение сразу блоками. Этим блочные шифры отличаются от поточных, потому что **в поточных шифрах каждый символ шифруется отдельно.** Иногда поточные шифры использовать гораздо удобнее, потому что с их помощью можно шифровать сообщения прямо в процессе передачи, на лету.

Асимметричные шифры в жизни

А вы знаете, где и когда вы используете асимметричное шифрование в вашей жизни? Наверное, у всех сейчас есть **мессенджеры на телефонах**. Так вот, многие из них используют end-to-end-шифрование – сообщения шифруются и расшифровываются на самих телефонах.

На вашем телефоне создается условный «сундук» (и мы в нашем курсе рассмотрим, что именно будет являться сундуком) и условный «ключ». Вы отправляете «сундук» другу, который кладет в него свое сообщение. А когда «сундук» с письмом возвращается к вам, вы открываете его своим ключом.

И никакие ключи по сети не передаются, они существуют только на вашем телефоне. И, как правило, вырабатываются только для текущей сессии – и никто кроме вас получить их не может.

Об этом и о многом другом мы поговорим в модуле «Криптография». До встречи!