> Конспект > 2 урок > Data Security

> Оглавление

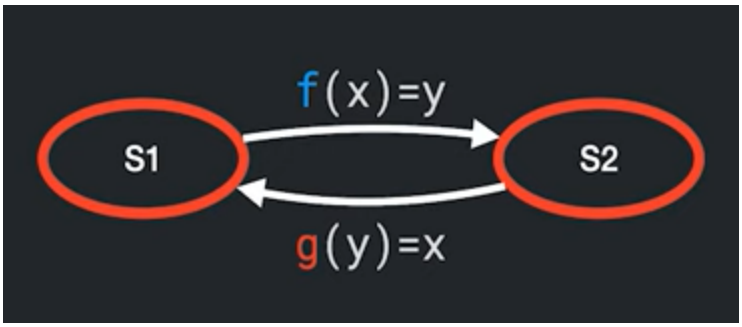
Компании имеют огромные объемы различных данных, которые скорее всего необходимо каким то образом защищать. При использовании термина защита данных, существует 2 типа данных:

- Пользовательские данные (ФИО, номер телефона и тд.)
- Корпоративные данные (продажи, отчеты и тд.)

Как правило, создают специальные отделы, которые занимаются кибербезопасностью с целью выявлять утечки и “узкие места” систем, которые используются в компании.

> Немного математики

Обратимые функции - функция обратима, если каждое свое значение она принимает один-единственный раз.

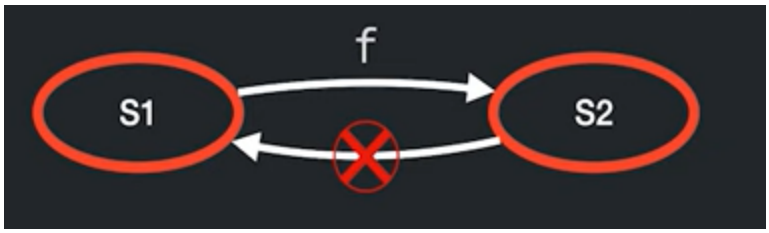



```
f(x) = 2*x g(y) = y/2

f(2) = 4   g(4) = 2
f(3) = 6   g(6) = 3
f(4) = 8   g(8) = 4

g(f(x)) = f(g(x)) = x
```

Односторонняя функция - математическая функция, которая легко вычисляется для любого входного значения, но трудно найти аргумент по заданному значению функции (трудно обратимая или необратимая).




```
f(X) = md5(X)
f('Alex') = a08372b70196c21a9229cf04db6b7ceb
f('Tom') = d9ffaca46d5990ec39501bcdf22ee7a1
```

Нужно отметить, что обязательно условие, что односторонняя функция существует.

> Подходы к безопасности данных

> Маскирование данных

Маскирование данных (Обезличивание) - это способ защиты конфиденциальной информации от несанкционированного доступа путем замены исходных данных фиктивными данными или произвольными символами. При этом замаскированная информация выглядит реалистично и непротиворечиво.

Процесс обезличивания должен являться односторонней функцией. Процесс обезличивания может быть реализован собственноручно либо можно использовать сторонние сервисы.

Способы изменения данных:

- Замена - замена данных подготовленными или случайными

- Перемешивание - случайное перемешивание значений в колонке

- Редактирование - замена символов частично или полностью произвольными символами

- Метод разброса - отклонение замаскированного числового значения от исходного на определенную или случайную величину.

Маскированные данные не должны быть подвержены реверс-инжинирингу.

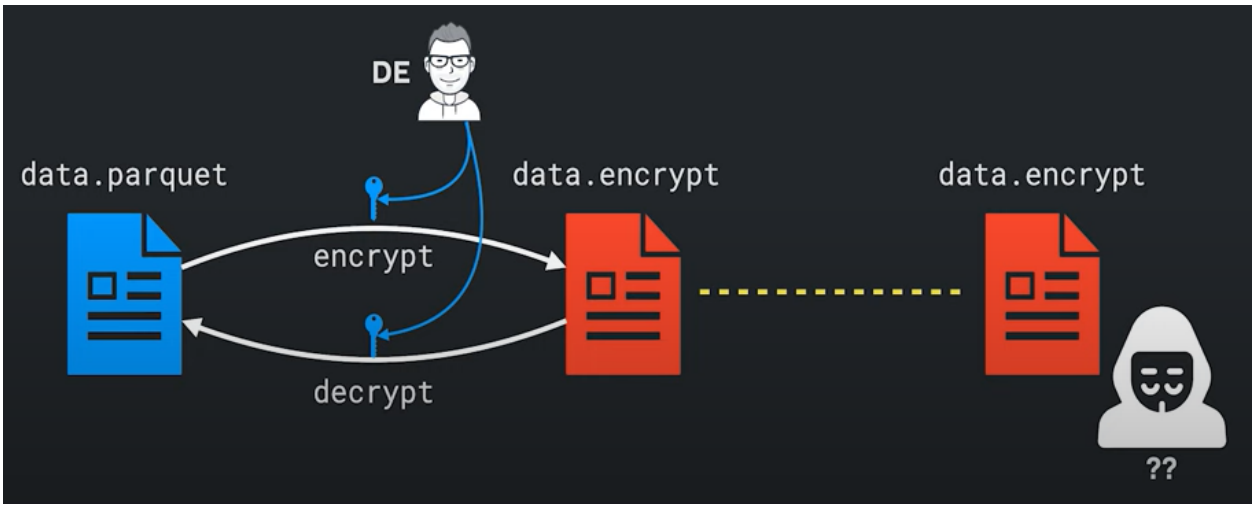
> Шифрование данных

Шифрование данных - обратимое преобразование информации в целях сокрытия от неавторизованных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ним.

В шифровании данных у нас есть 2 процесса:

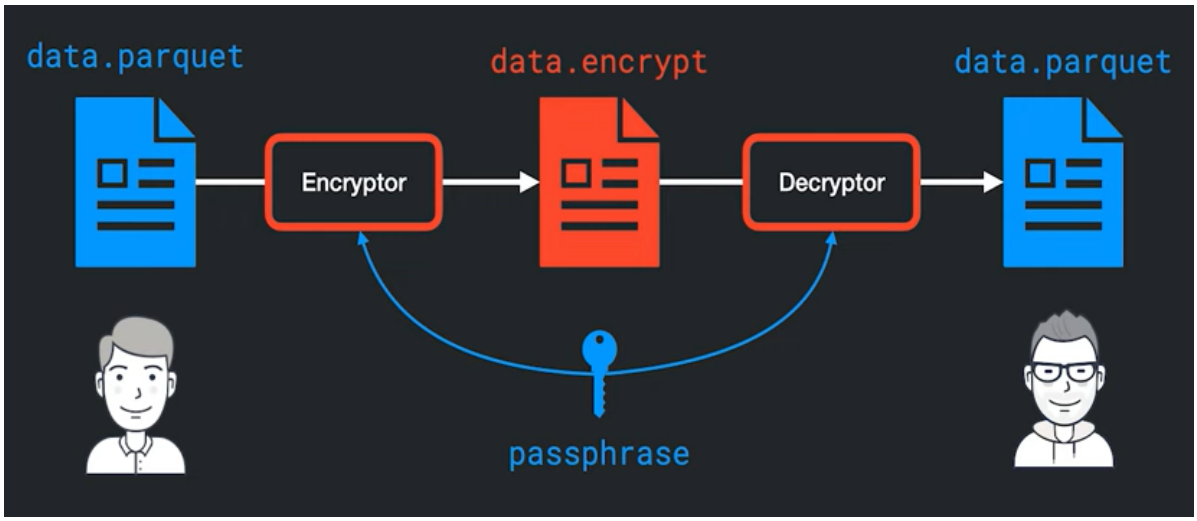
- encrypt - зашифровка
- decrypt - дешифровка

В обоих случаях необходим ключ, который позволяет получить доступ к данным.

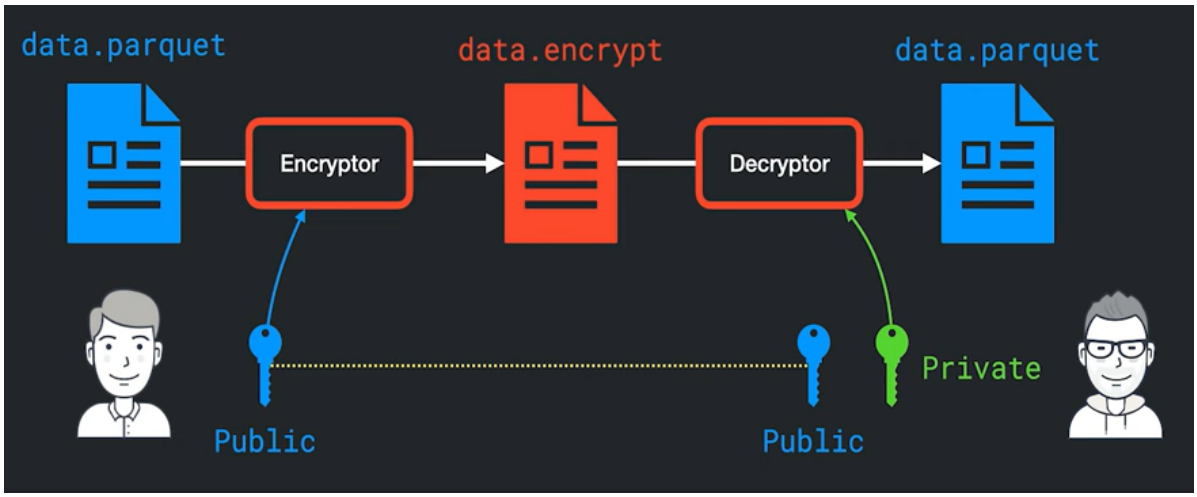


> Типы шифрования

1. Симметричное шифрование - для шифрования и расшифровывания используется один и тот же ключ.

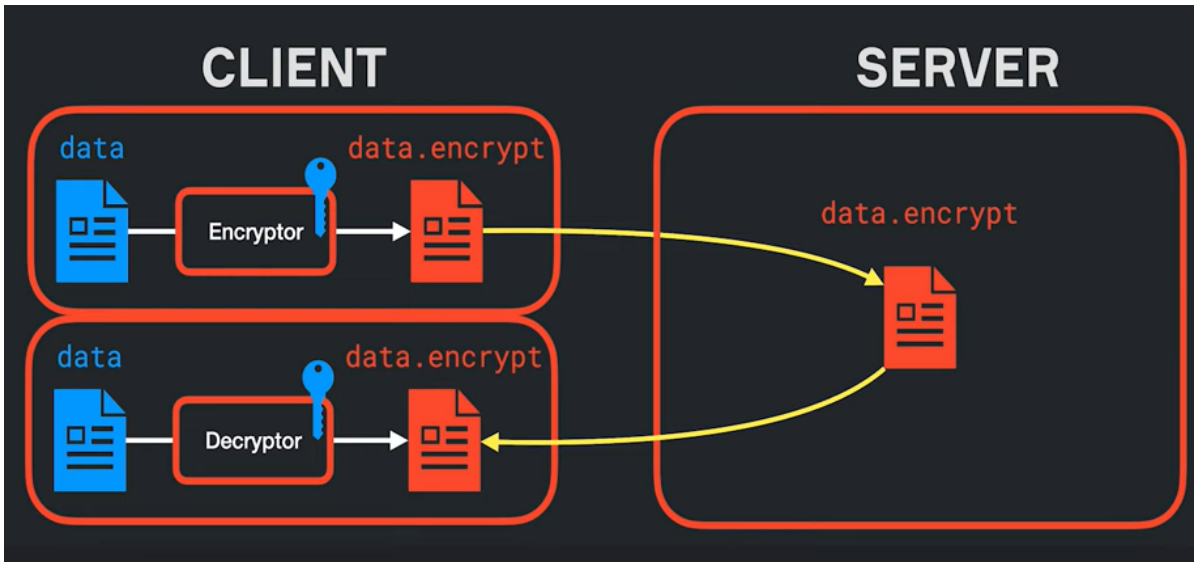


2. Ассиметричное шифрование - для шифрования используется открытый ключ, для расшифровывания используется закрытый ключ, при этом ключи связаны определенным математическим образом друг с другом.

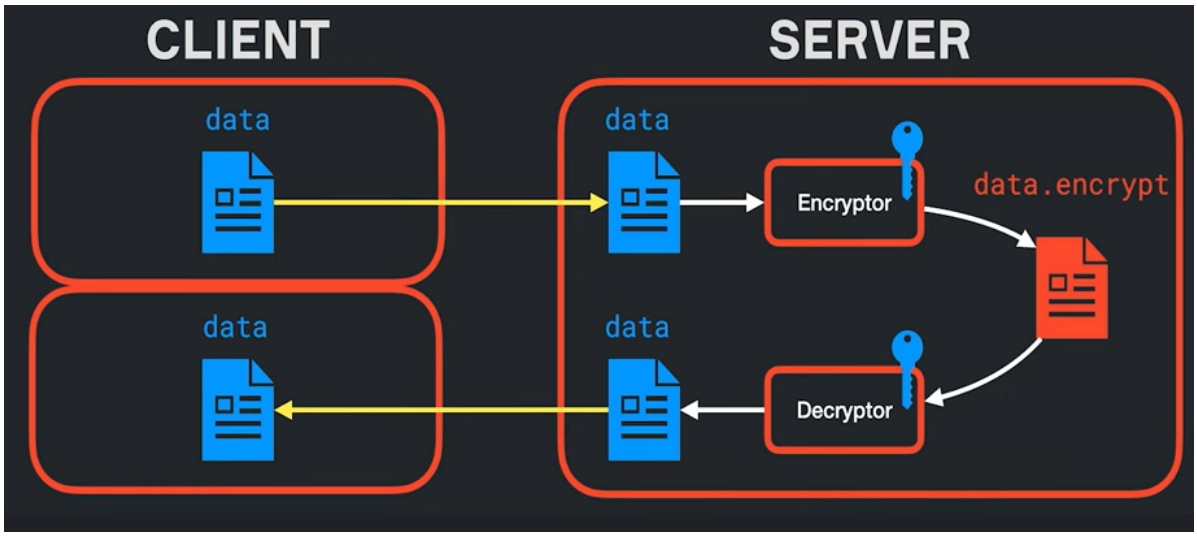


> Способы применения

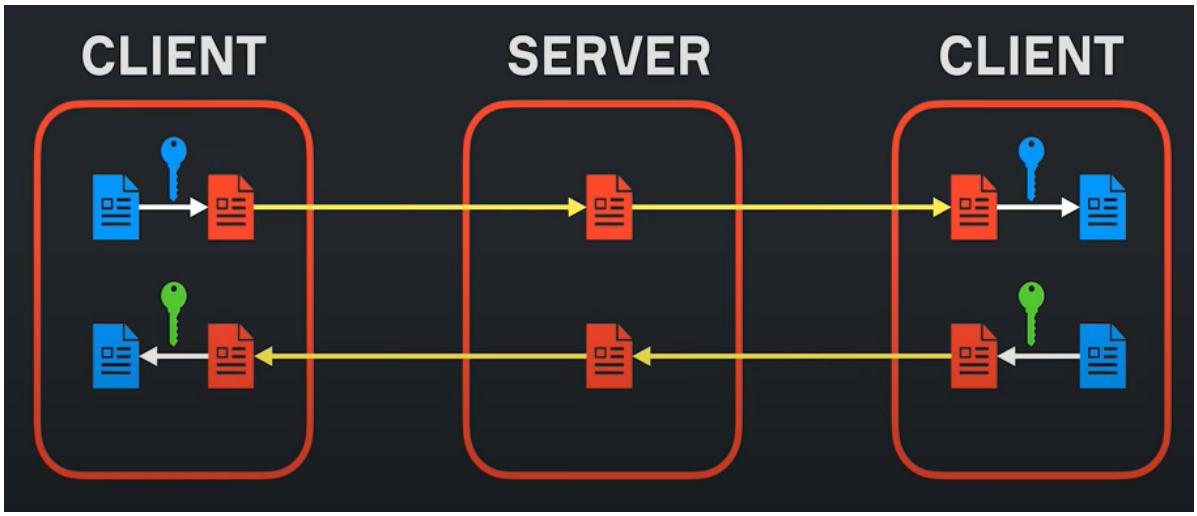
1. Client side - шифрование на стороне клиента.



2. Server side - шифрование на стороне сервера.



3. End-to-end - сквозное шифрование (только участники канала передачи имеют доступ к данным).



> Токенизация данных

Токенизация данных - процесс замены конфиденциального элемента данных на не конфиденциальный эквивалент, называемый токеном. Применяется какое-то окружение, в котором происходит токенизация исходных данных и в котором может поработать сотрудник. По итогу, сотрудник не будет даже знать, как выглядят исходные данные. Для злоумышленников это полностью необратимая операция. Процесс токенизации требует большей организованности от компании.