Целостность данных в TLS/SSL

Компьютерные сети

Целостность данных в TLS/SSL

TLS/SSL – протоколы безопасной передачи данных по небезопасной сети:

- Приватность
- Целостность
- Аутентификация

Целостность данных в Ethernet

Криптографические хэш функции

Хэш-функции (hash function):

- Преобразование массива данных в строку фиксированной длинны – хэш
- По хэшу нельзя определить, на основе каких данных он был создан
- Коллизия – одно и то же значение хэша для разных входных данных

Криптографические хэш функции:

- MD5 (Message Digest 5)
- SHA-1 (Secure Hash Algorithm 1), SHA-224, SHA-256, SHA-384, SHA-512

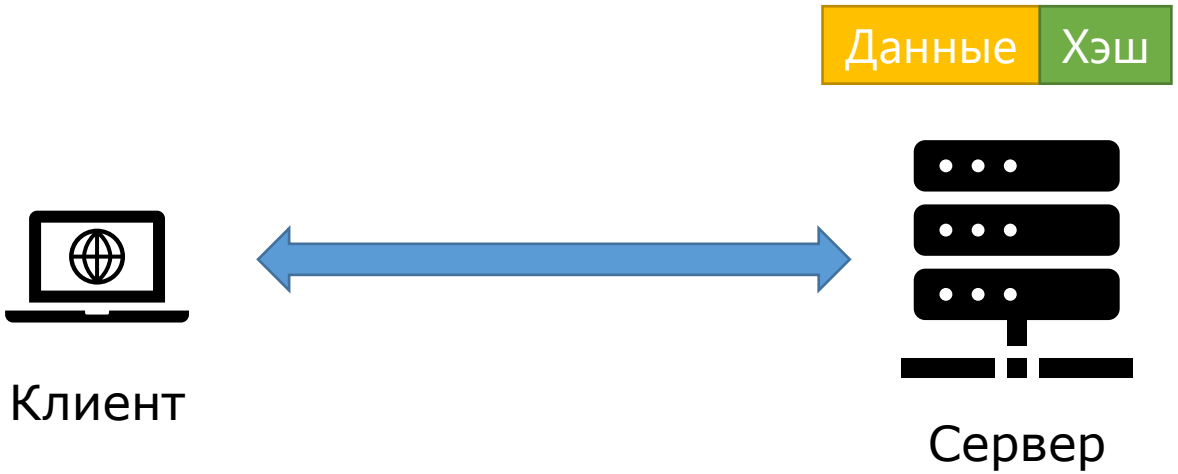
Криптографические хэш функции в Python

```
import hashlib
m = hashlib.sha256()
m.update(b"""The United States of America has adopted a suite of Secure Hash
   Algorithms (SHAs), including four beyond SHA-1, as part of a Federal
   Information Processing Standard (FIPS), specifically SHA-224 (RFC
   3874), SHA-256, SHA-384, and SHA-512.  The purpose of this document
   is to make source code performing these hash functions conveniently
   available to the Internet community.""")
print(m.hexdigest())
8f0fd83d40277c9cb8c3a1371cf0771c590c766c4775cbab56be860b83d6848a
```

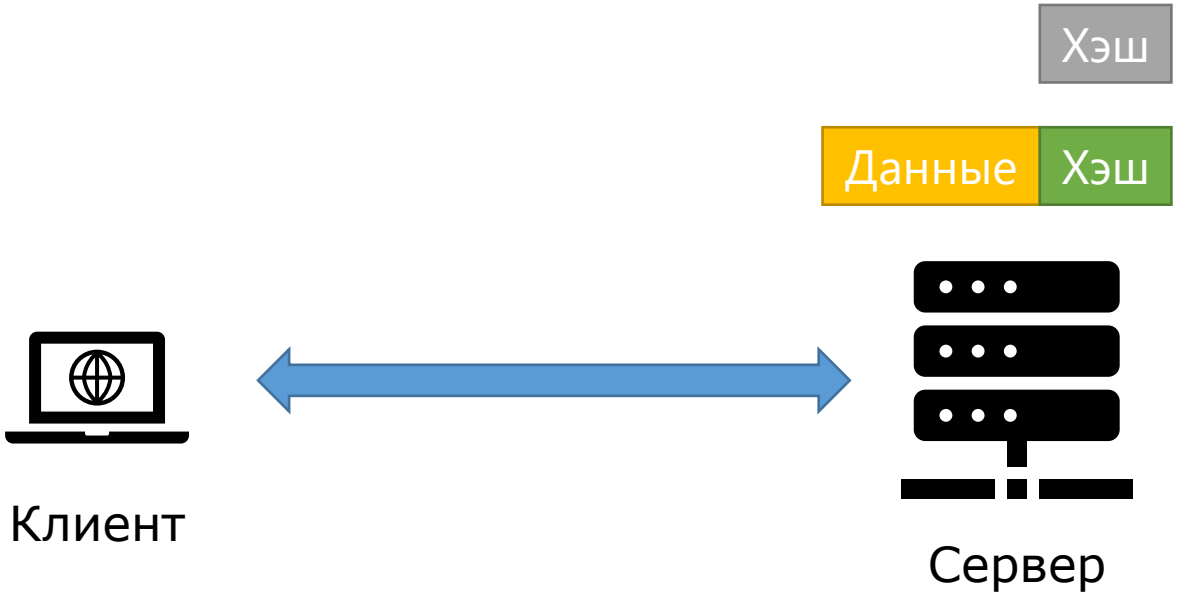
Целостность данных в TLS/SSL

Целостность данных в TLS/SSL

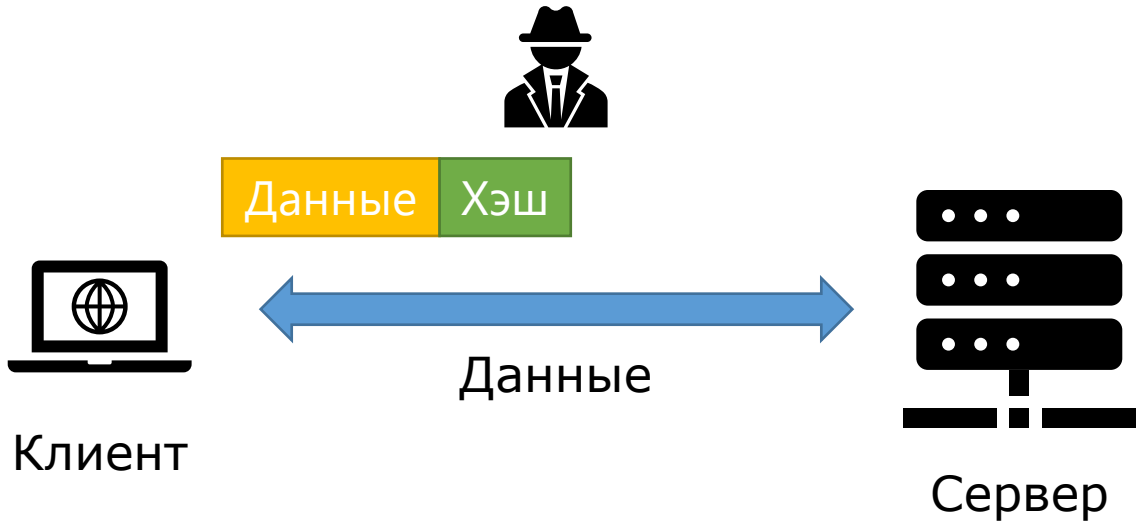
Целостность данных в TLS/SSL



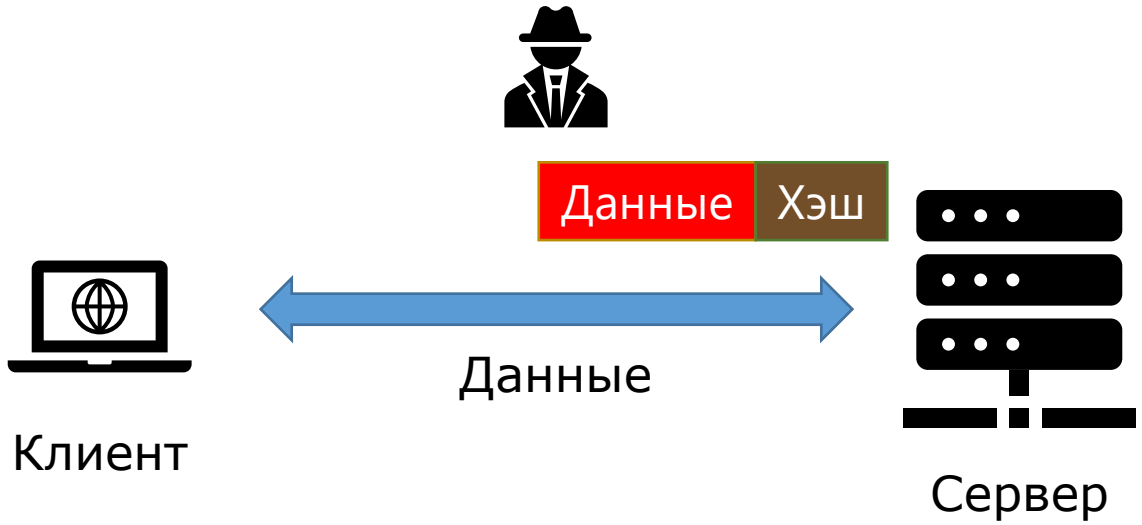
Целостность данных в TLS/SSL



Изменение данных и хэша в TLS/SSL

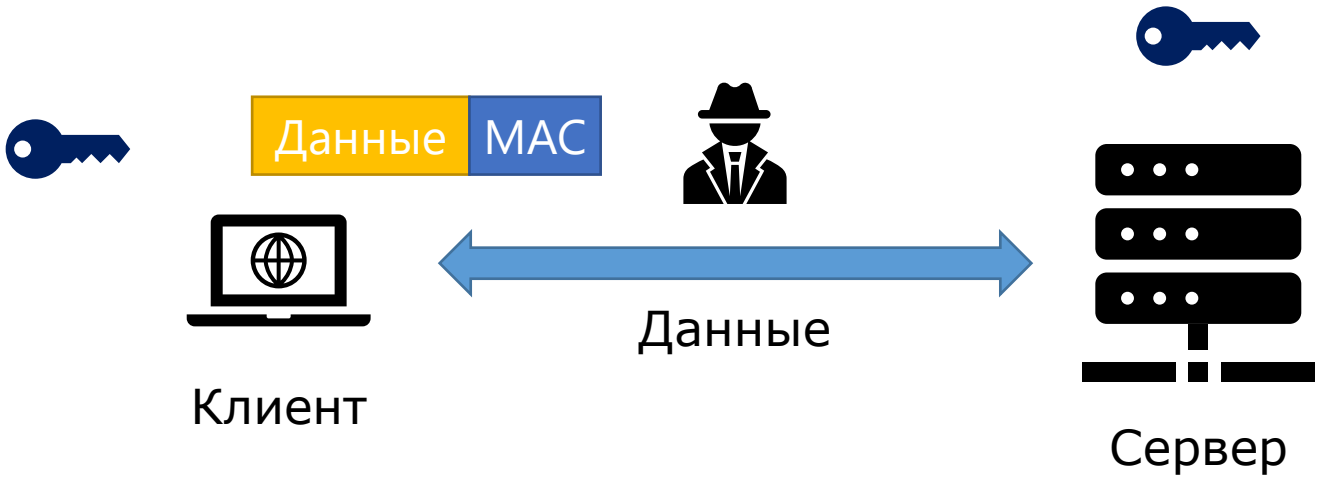


Изменение данных и хэша в TLS/SSL



Message Authentication Code

Message Authentication Code



Message Authentication Code

Набор шифров TLS/SSL

Алгоритм обмена ключами:

- RSA
- Диффи-Хеллмана

Алгоритм симметричного шифрования:

- AES
- 3DES

Хэш-функция для вычисления MAC:

- MD5 (Message Digest 5)
- SHA-1 (Secure Hash Algorithm 1), SHA-224, SHA-256, SHA-384, SHA-512

Итоги

Целостность данных в TLS/SSL:

- Защита от случайного или преднамеренного изменения данных

Message Authentication Code (код аутентификации сообщений, имитовставка):

- Рассчитывается на основе сообщения и разделяемого ключа
- Используются криптографические хэш-функции (MD5, SHA-1, SHA-256 и т.п.)

Ограничение MAC:

- Нет возможности подтвердить подлинность сервера (атака человек посередине)