TLS/SSL

By Miroshnichenko Denis

There are just my notes that I wrote down while studying TLS/SSL technology. I am not responsible for the correctness of this information.

Protocols TLS/SSL

- **TLS** - Transport Layer Security - протокол защиты транспортного уровня
- **SSL** - Secure Sockets Layer - уровень защищенных сокетов

Transport layer in TCP/IP model

TLS/SSL provides:
- Privacy
- Integrity
- Authentication

Encryption:
- Symmetric
- Asymmetrical

Symmetric:

Cryptographic key is used for encryption and decryption on each part of system.

Algorithms:
- AES
- 3DES
- RC4, RC5, RC6

Asymmetrical:

Has public and private key

```
[public_key]            [private_key]
client  <---------------->  server
```

Asymmetrical:

- Public key can distribute across systems
- Slow

Symmetric:

- Key should be in secret
- Fast

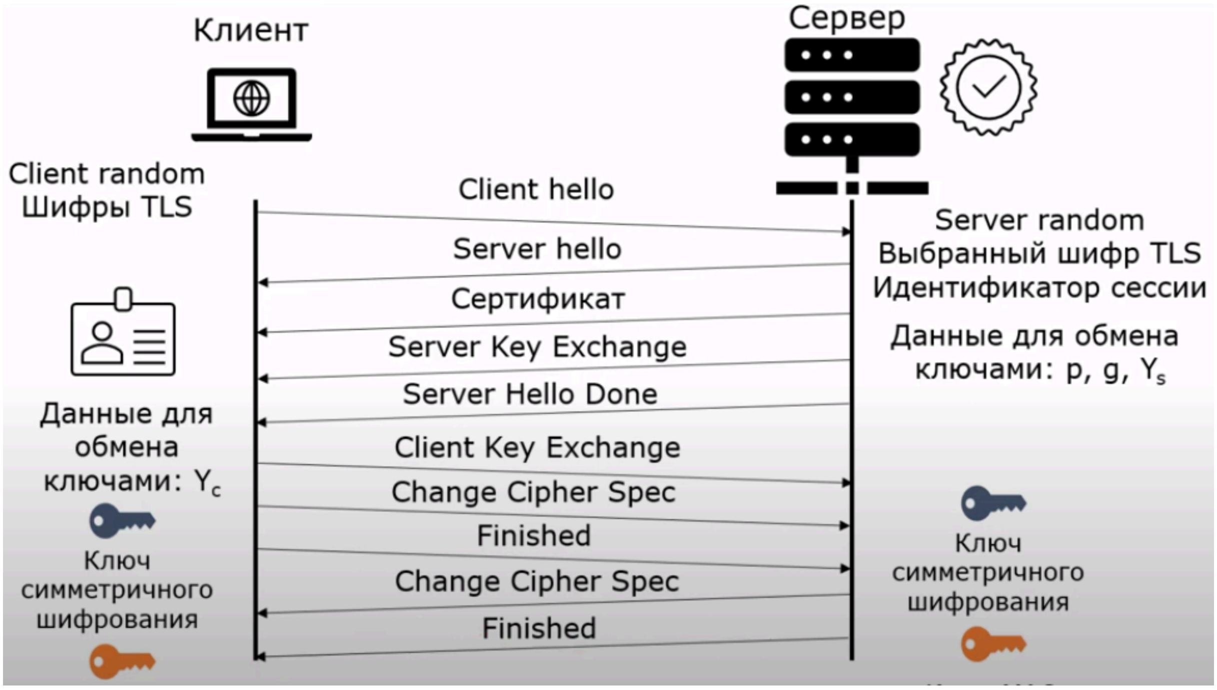
Integrity:

Hash-functions:

- MD5
- SHA-1, SHA-224, SHA-256
- SHA-384, SHA-512

Client compute hash by data and special key and transfer this hash per connection. Server receives data and compare received data with own key to be sure that data not be counterfeit.

Establish TLS 1.2 connection



Клиент

Сервер

Client random
Шифры TLS

Client hello

Server hello

Сертификат

Server Key Exchange

Server Hello Done

Client Key Exchange

Change Cipher Spec

Finished

Change Cipher Spec

Finished

Server random
Выбранный шифр TLS
Идентификатор сессии

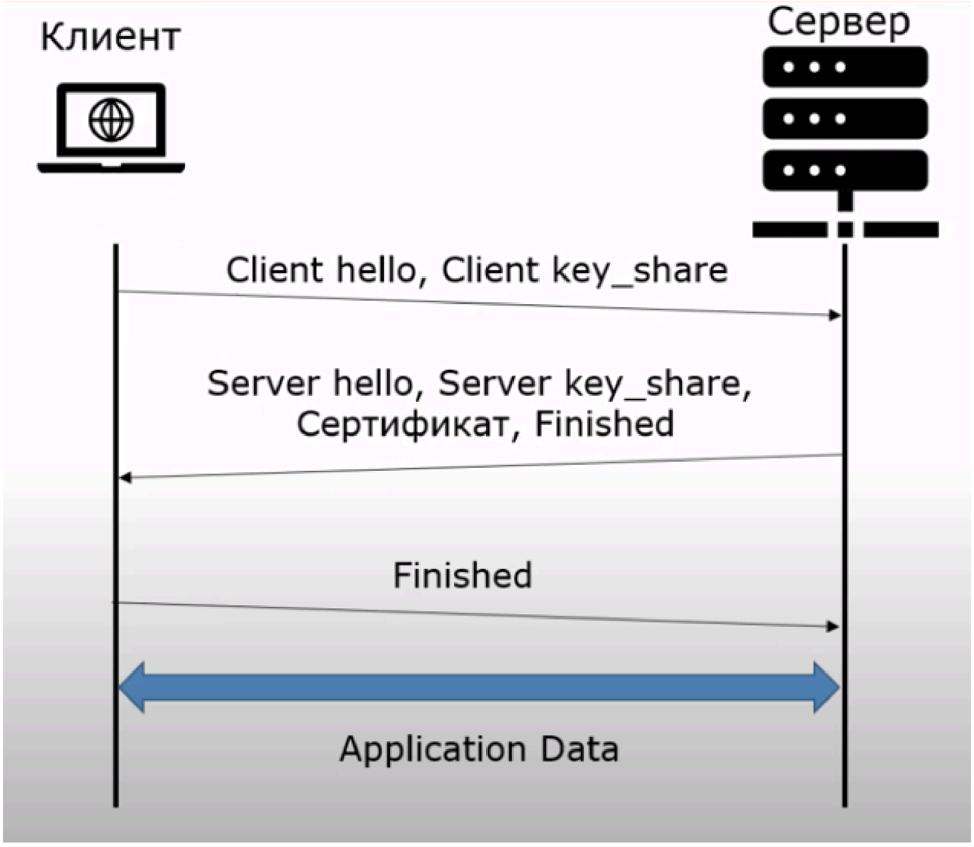
Данные для обмена ключами: p, g, Y_s

Данные для обмена ключами: Y_c

Ключ симметричного шифрования

Ключ симметричного шифрования

Establish TLS 1.3 connection



Клиент

Сервер

Client hello, Client key_share

Server hello, Server key_share,
Сертификат, Finished

Finished

Application Data