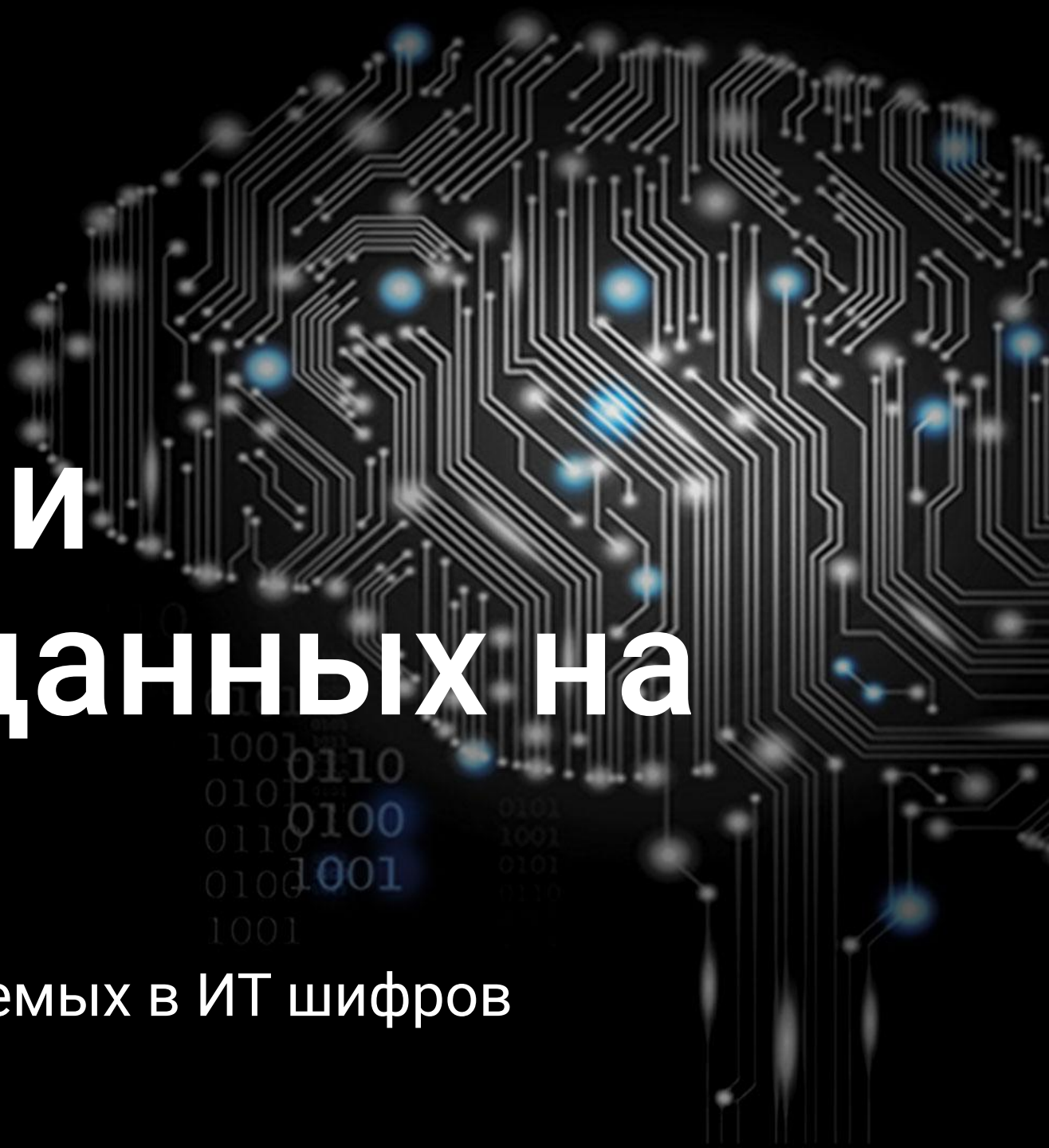
GeekBrains



Алгоритмы и структуры данных на языке C

Обзор современных используемых в ИТ шифров

GeekBrains

Обзор современных используемых в ИТ шифров

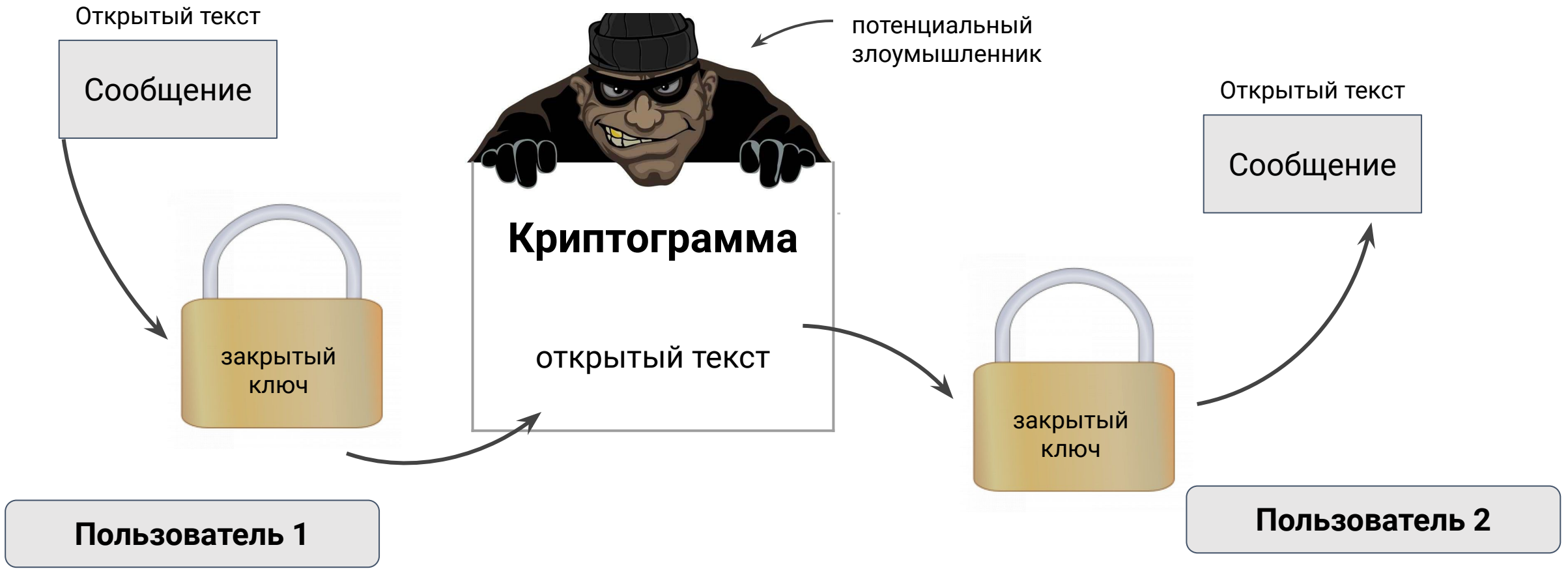
В этом видео

1. Краткий обзор современных шифров

Краткий обзор современных шифров

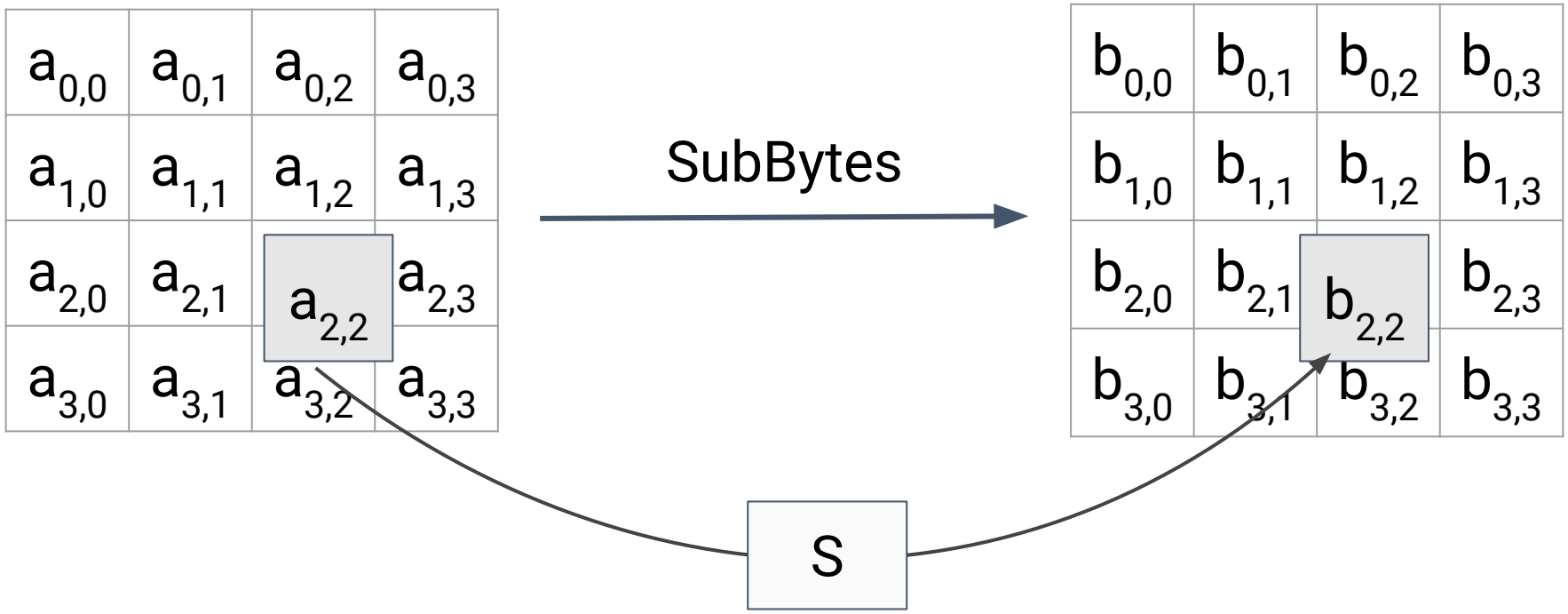
GeekBrains

Современное шифрование

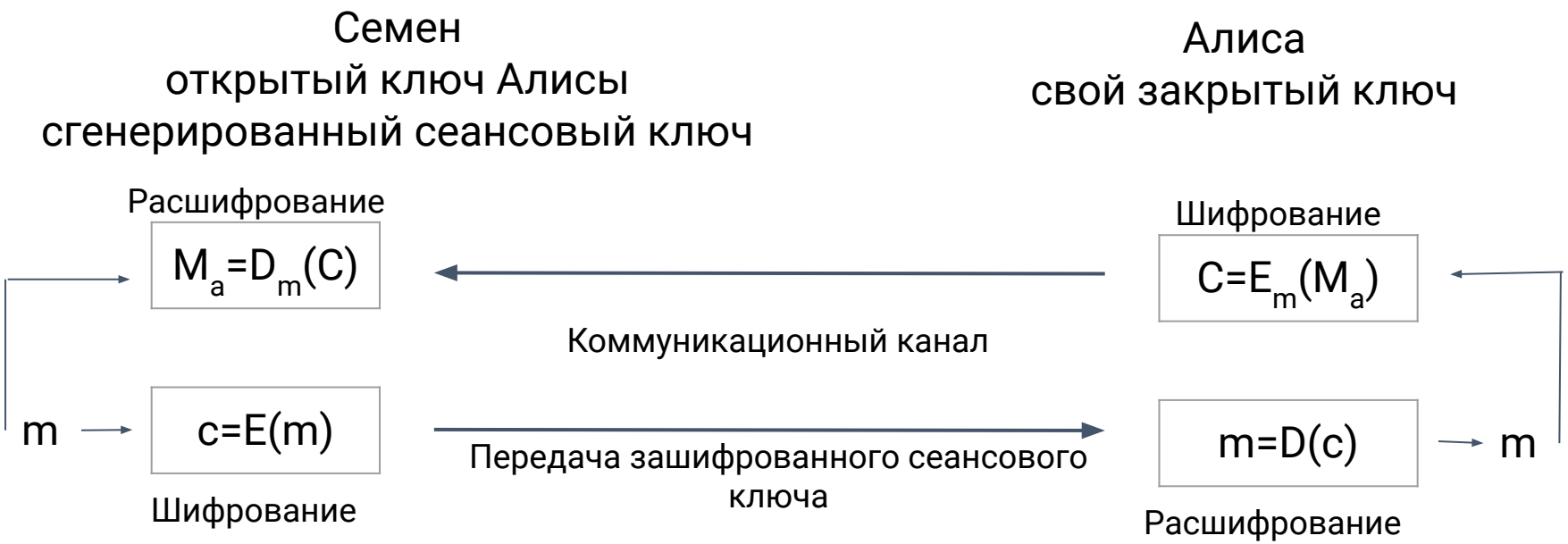


AES

Rijndael

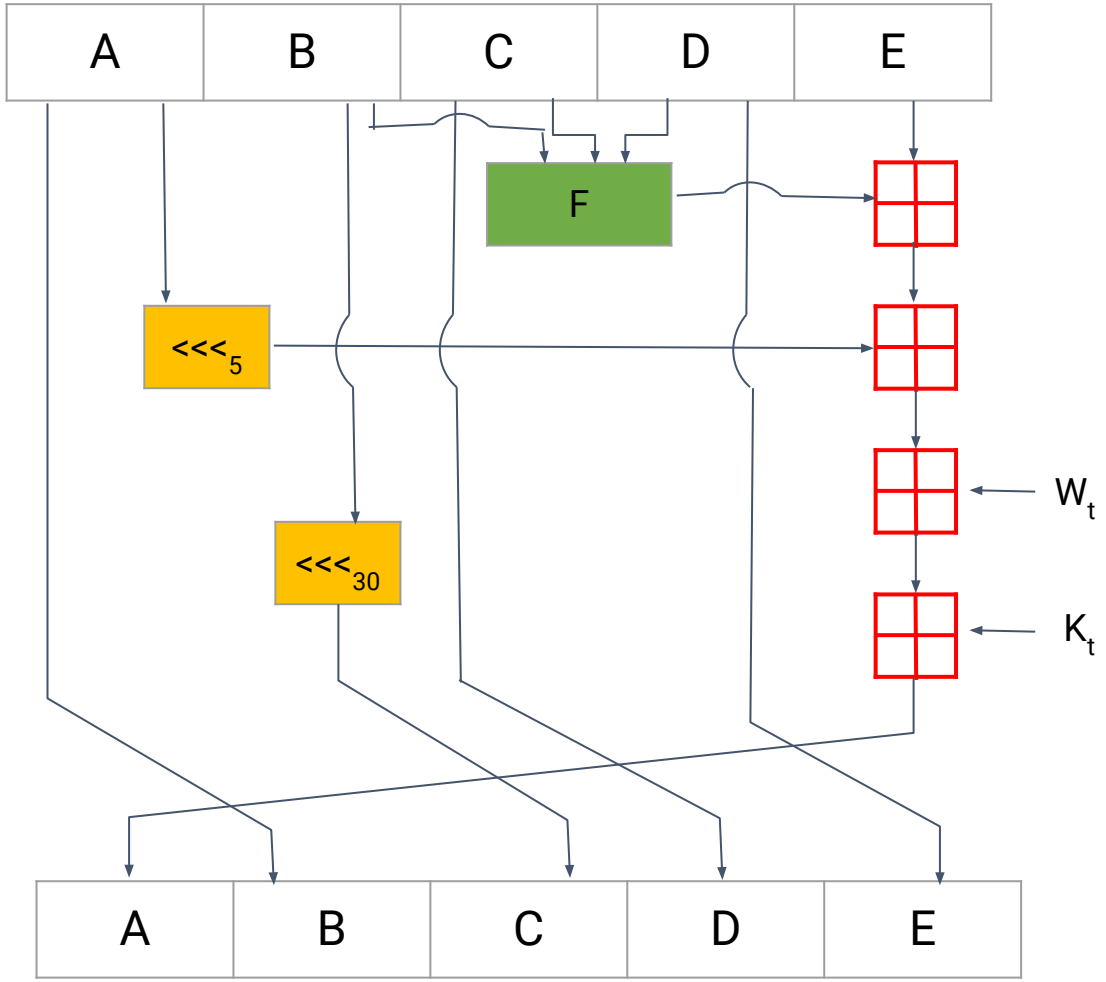


RSA

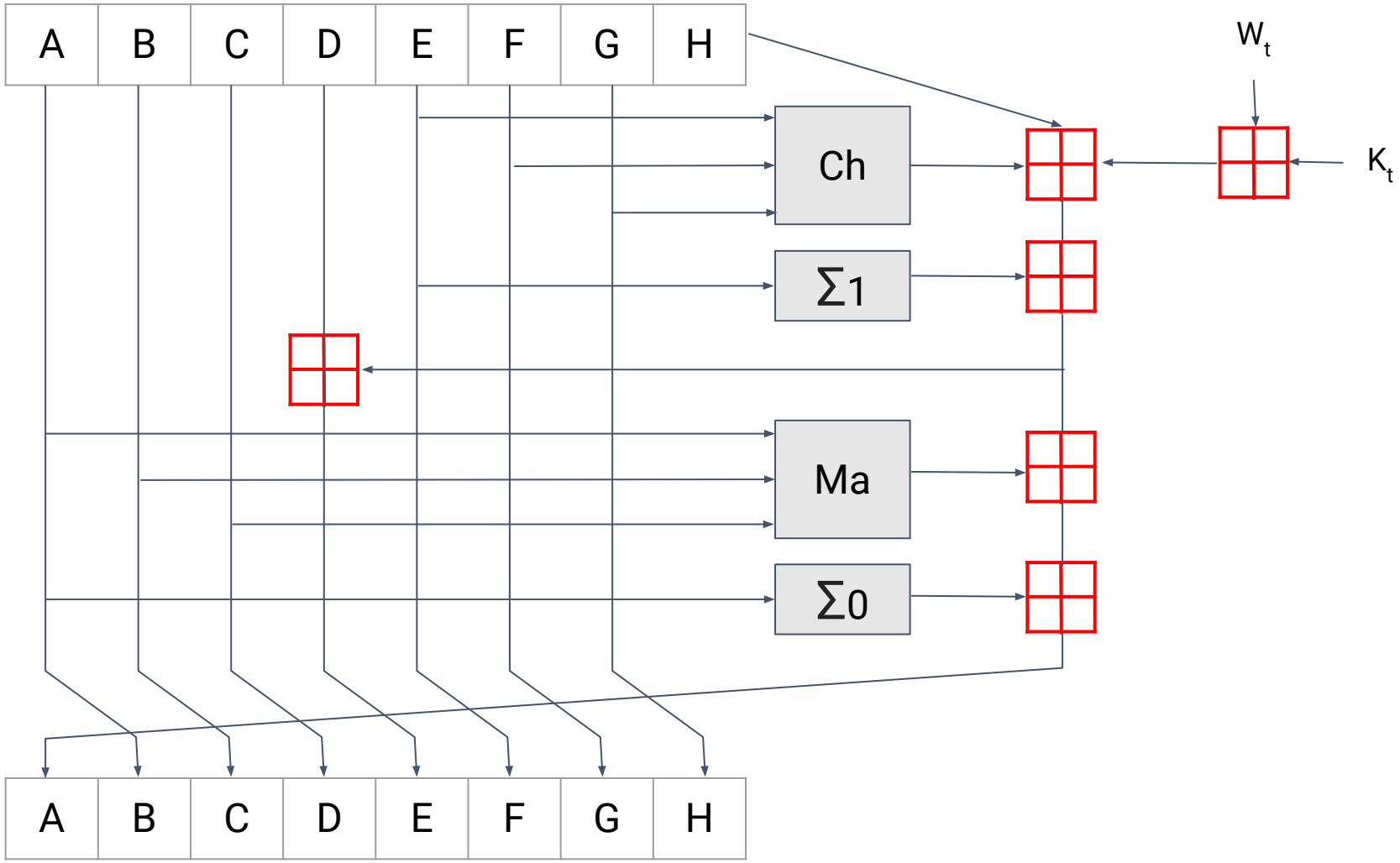


- Взять открытый ключ Алисы
- Создать случайный сеансовый ключ
- Зашифровать сеансовый ключ с использованием открытого ключа Алисы
- Расшифровать сообщение с помощью сеансового ключа симметричным алгоритмом
- Принять зашифрованный сеансовый ключ Семена
- Взять свой закрытый ключ
- Применить закрытый ключ для расшифровывания сеансового ключа
- Зашифровать сообщение с помощью сеансового ключа симметричным алгоритмом

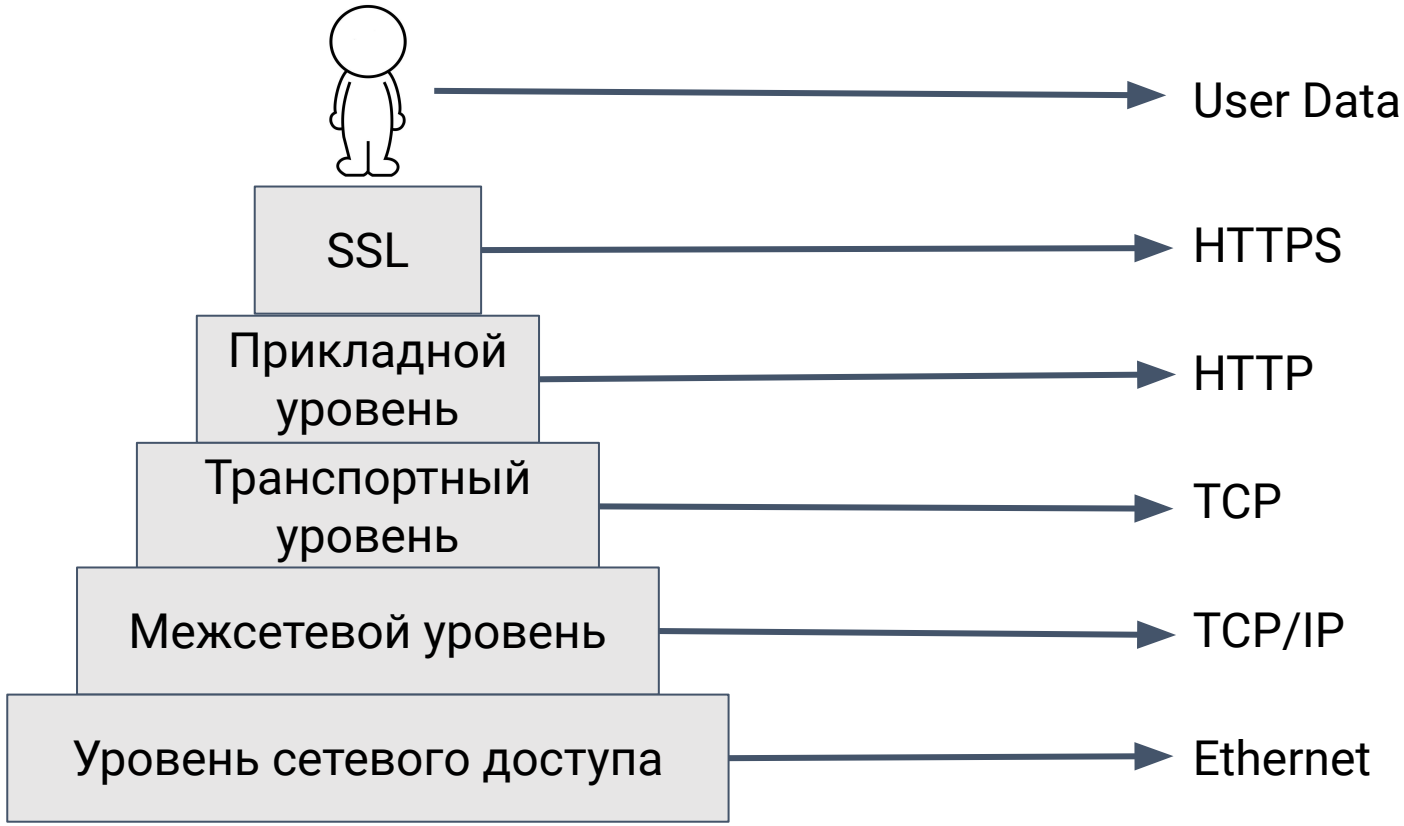
SHA-1



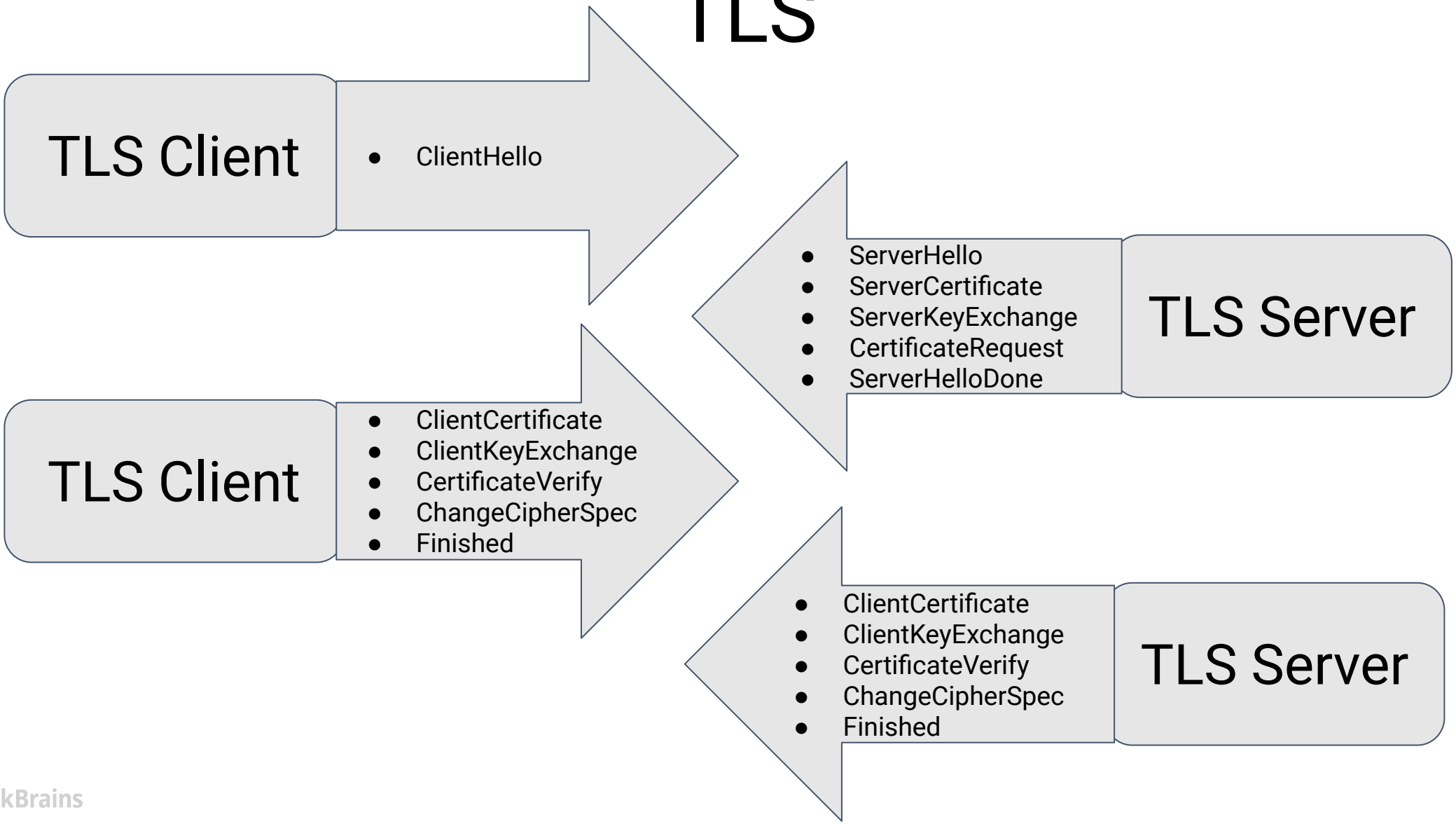
SHA-2



SSL


User Data
SSL
HTTPS
Прикладной уровень
HTTP
Транспортный уровень
TCP
Межсетевой уровень
TCP/IP
Уровень сетевого доступа
Ethernet

TLS



Итоги

Рассмотрели:

- Часто используемые шифры