Кибербезопасность: от нуля до результата

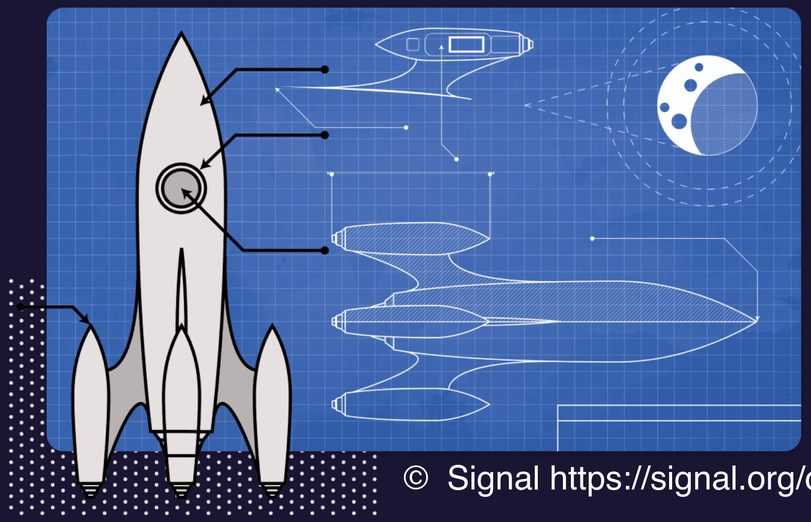
Протокол Signal

Елена Киршанова

БФУ имени И. Канта

Signal

- протокол мессенджера, обеспечивающего конфиденциальность и целостность сообщений
- предложен компанией Open Whisper Systems https://en.wikipedia.org/wiki/Open_Whisper_Systems
- используется в приложениях Signal, WhatsApp, Facebook Messenger, Google Allo
- опен-сорсная реализация

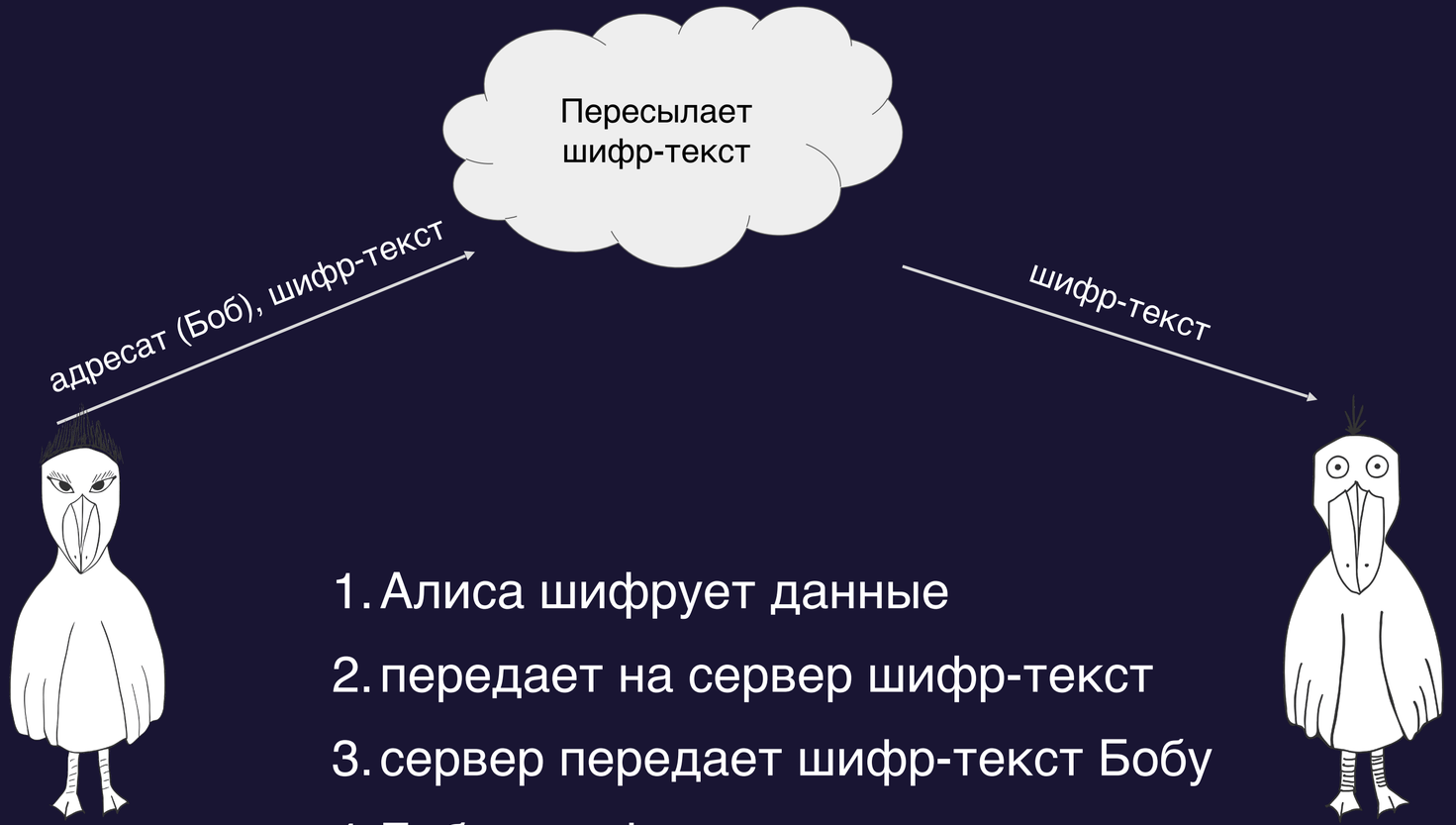


© Signal https://signal.org/docs/

“Безопасный” мессенджер обеспечивает

- корректность
- конфиденциальность
- аутентификацию
- стойкость к потере сообщения
- прямую секретность (forward secrecy)
- безопасность после компрометации

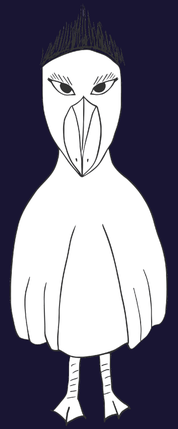
End-to-End (E2E) / Сквозное шифрование



1. Алиса шифрует данные
2. передает на сервер шифр-текст
3. сервер передает шифр-текст Бобу
4. Боб дешифрует

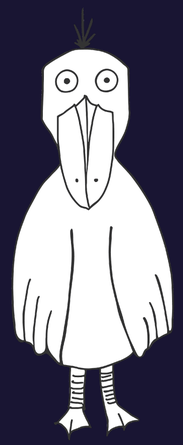
Сервер не знает ни ключ, ни открытый текст

Принцип работы Signal



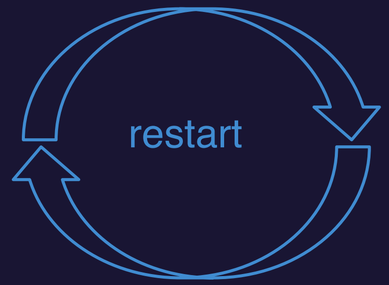
Шаг 1. Генерация общего ключа **k**

Шаг 2. Симметричное шифрование с ключом **k**



Отправитель

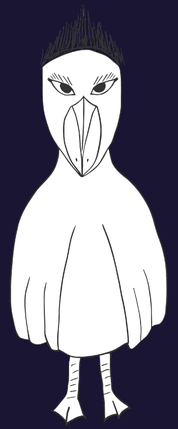
Получатель



Получатель

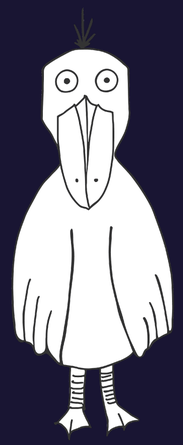
Отправитель

Принцип работы Signal



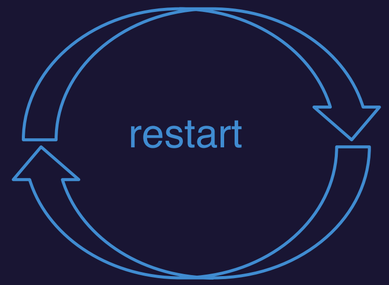
Шаг 1. Генерация общего ключа k

Шаг 2. Симметричное шифрование
с ключом **k**



Отправитель

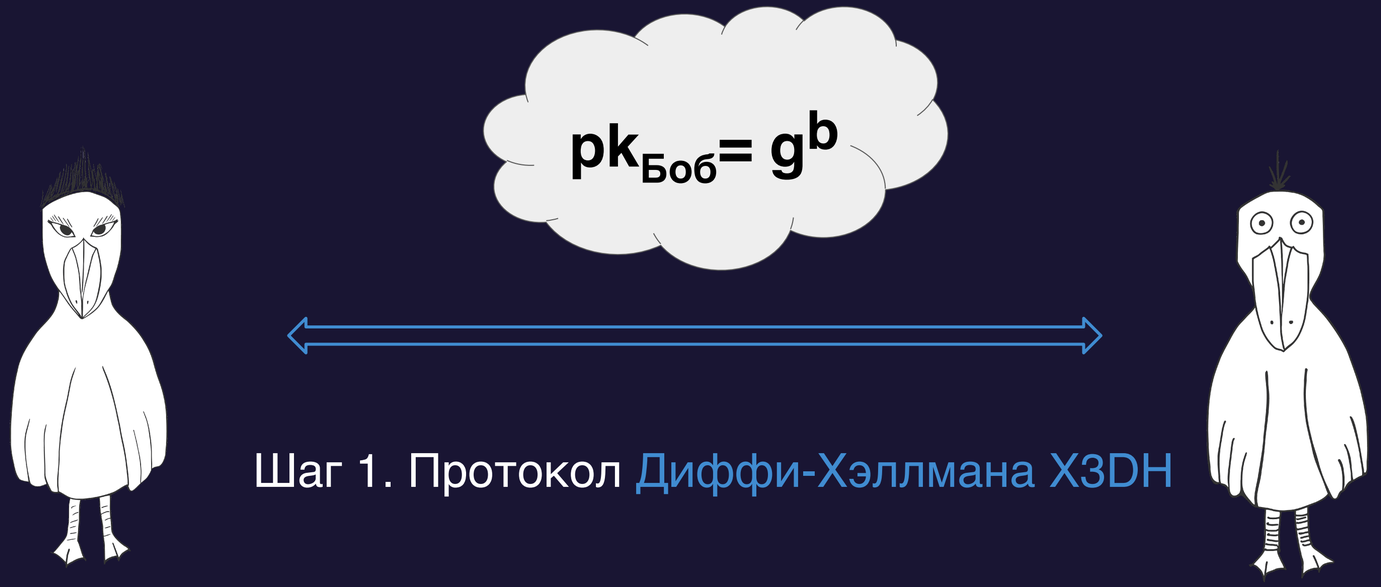
Получатель



Получатель

Отправитель

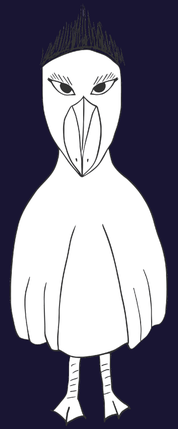
Генерация общего ключа



Шаг 1. Протокол Диффи-Хэллмана X3DH

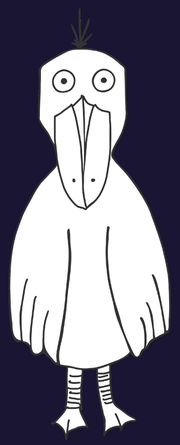
- Боб публикует свои открытые ключи на сервере
- Алиса может отправить сообщение Бобу, даже если он офф-лайн
- Сервер сохранит сообщения для Боба, пока он не в сети
- В реальном протоколе стороны аутентифицируют себя

Принцип работы Signal



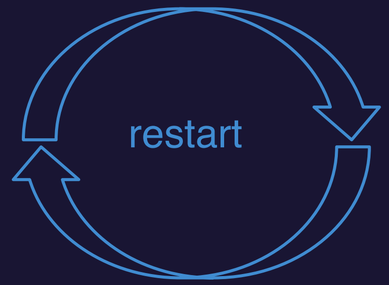
Шаг 1. Генерация общего ключа k

Шаг 2. Симметричное шифрование с ключом k



Отправитель

Получатель



Получатель

Отправитель

Double Ratchet / Двойной храповик

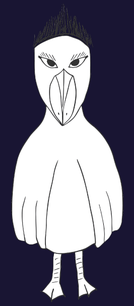
Храповик Диффи-Хэллмана

Периодическое обновление общего ключа

Симметричный Храповик

Уникальный симметричный ключ для каждого нового сообщения

Непрерывный Диффи-Хэллман



Отправитель

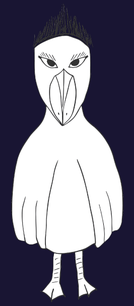
Получатель

g^{b_1}

a_1

b_1

Непрерывный Диффи-Хэллман



Отправитель

a_1

g^{b_1}

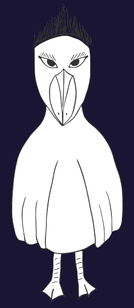
g^{a_1}

Общий ключ $g^{a_1 b_1}$

Получатель

b_1

Непрерывный Диффи-Хэллман



Отправитель

a_1

Получатель

b_1

g^{b_1}

g^{a_1}

Общий ключ $g^{a_1 b_1}$

Получатель

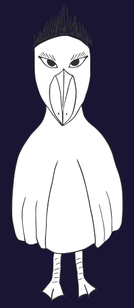
g^{b_2}

Общий ключ $g^{a_1 b_2}$

Отправитель

b_2

Непрерывный Диффи-Хэллман



Отправитель

a_1

g^{b_1}

g^{a_1}

Общий ключ $g^{a_1 b_1}$

Получатель

b_1

Получатель

b_2

g^{b_2}

$g^{a_1 b_2}$

Общий ключ $g^{a_1 b_2}$

Отправитель

b_2

Отправитель

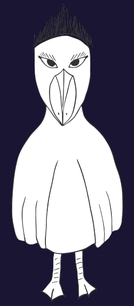
a_2

g^{a_2}

Общий ключ $g^{a_2 b_2}$

Получатель

Непрерывный Диффи-Хэллман



Отправитель

a_1

Получатель

b_1

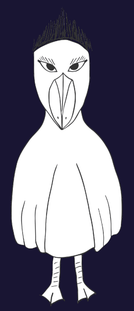
g^{b_1}

g^{a_1}

Общий ключ $g^{a_1 b_1}$

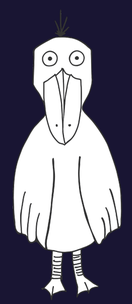
- Новый общий ключ генерируется всякий раз, когда одна из сторон меняет роль с Получателя на Отправителя
- Конфиденциальность регенерируется спустя 2 раунда

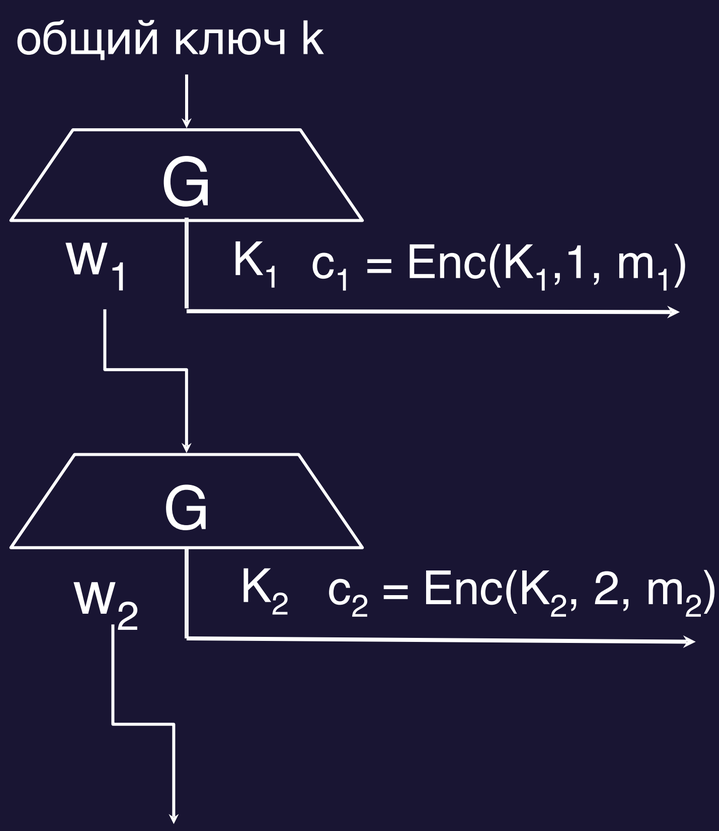
Симметричное шифрование

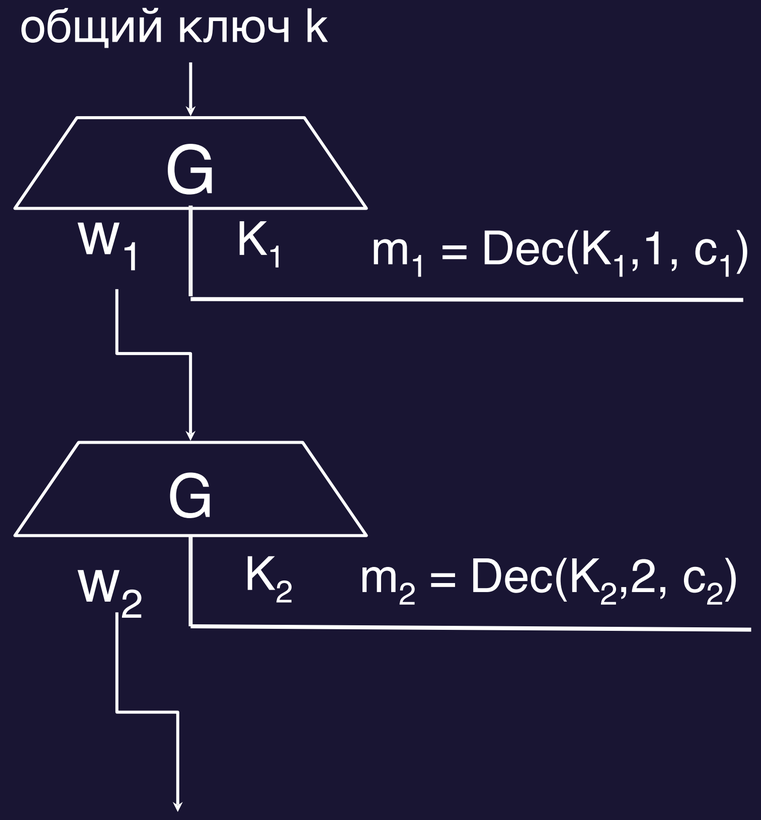


– ПСГ

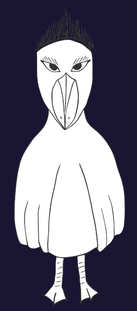
$G : \{0,1\}^n \rightarrow \{0,1\}^{2n}$





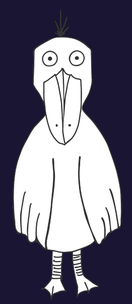


Потеря шифр-текста



G – ПСГ

$G : \{0,1\}^n \rightarrow \{0,1\}^{2n}$



общий ключ k

G

w_1 K_1 $c_1 = Enc(K_1,1,$

G

w_2 K_2 $c_2 = Enc(K_2, 2, m_2)$

общий ключ k

G

w_1 K_1 Сохранить K_1

G

w_2 K_2 $m_2 = Dec(K_2,2, c_2)$

Последний слайд

- в качестве ПСГ используется SHA-256
- для симметричного шифрования AES в режиме сцепления блоков