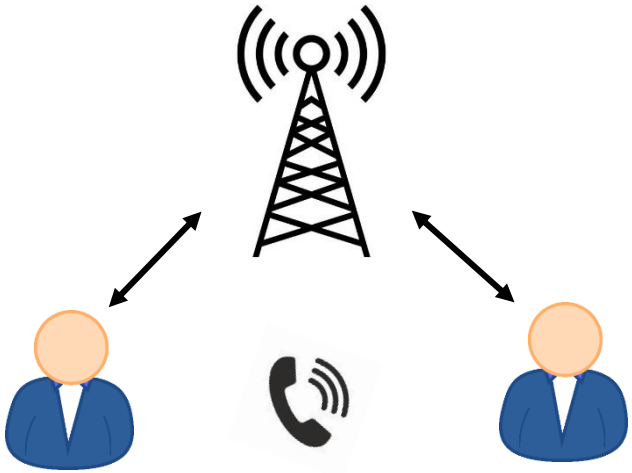
РусКрипто

«Подводные камни» при обеспечении защиты в системах VoIP

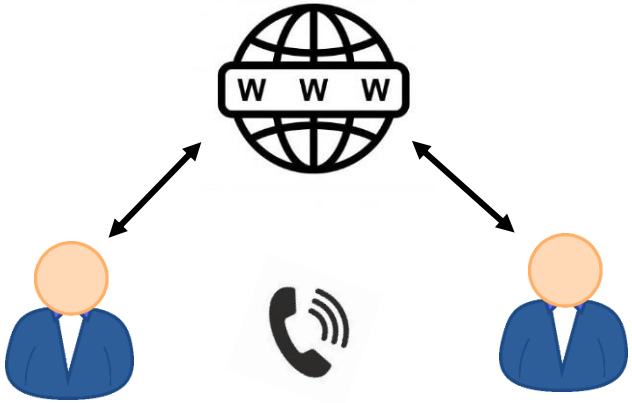
Ахметзянова Лилия, к.ф.-м.н.,
зам. начальника отдела криптографических исследований, КриптоПро
АНО «НТЦ ЦК»

Передача голосовой информации

РусКрипто



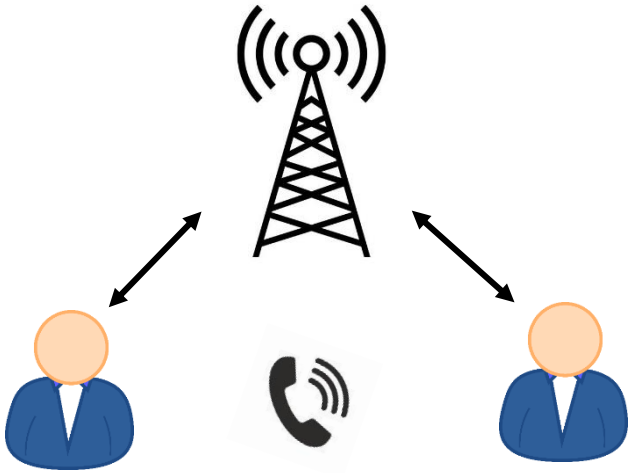
4G LTE



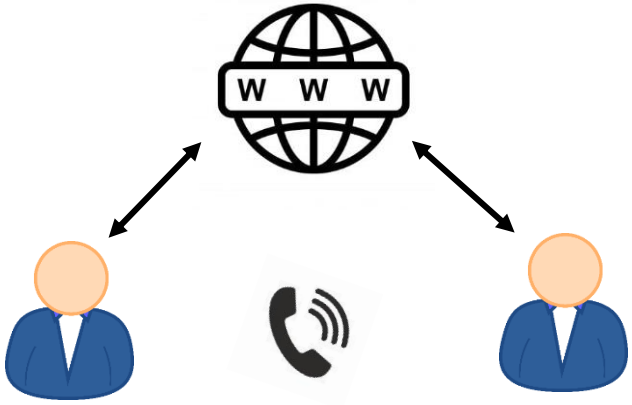
VoIP

Передача голосовой информации

РусКрипто



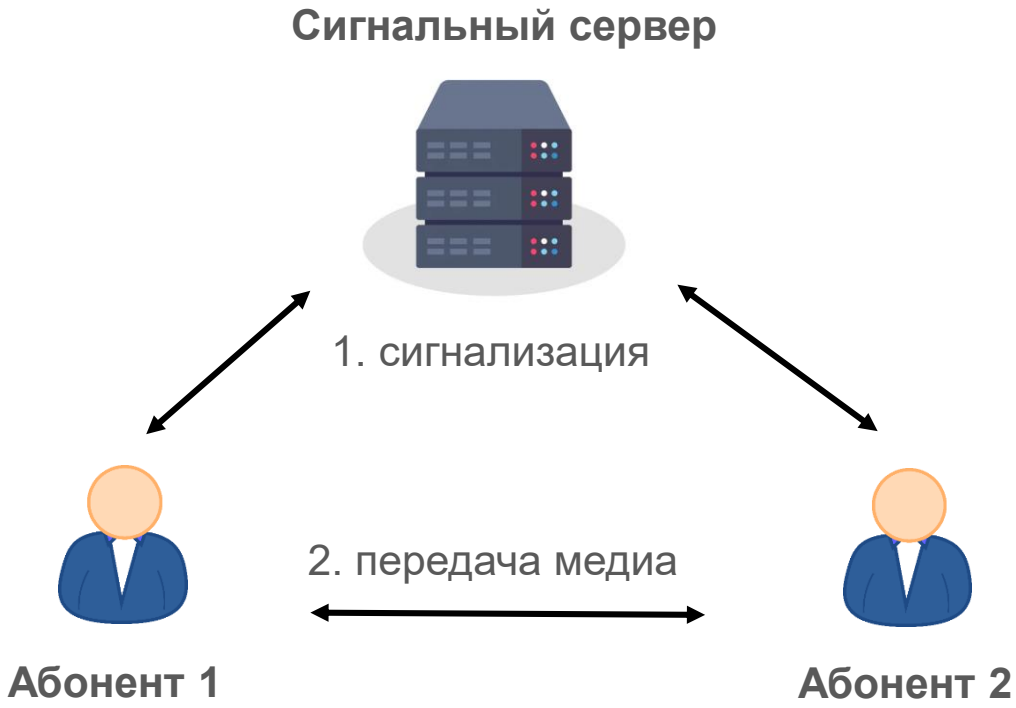
3G/4G/5G



VoIP

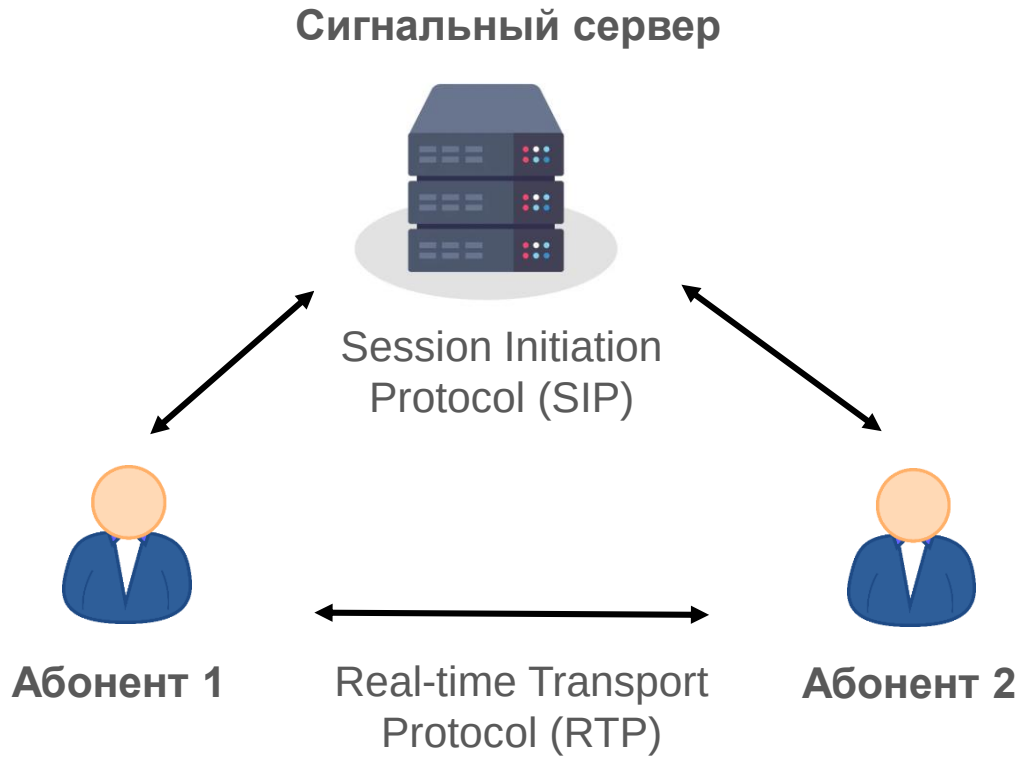
Системы VoIP

РусКрипто



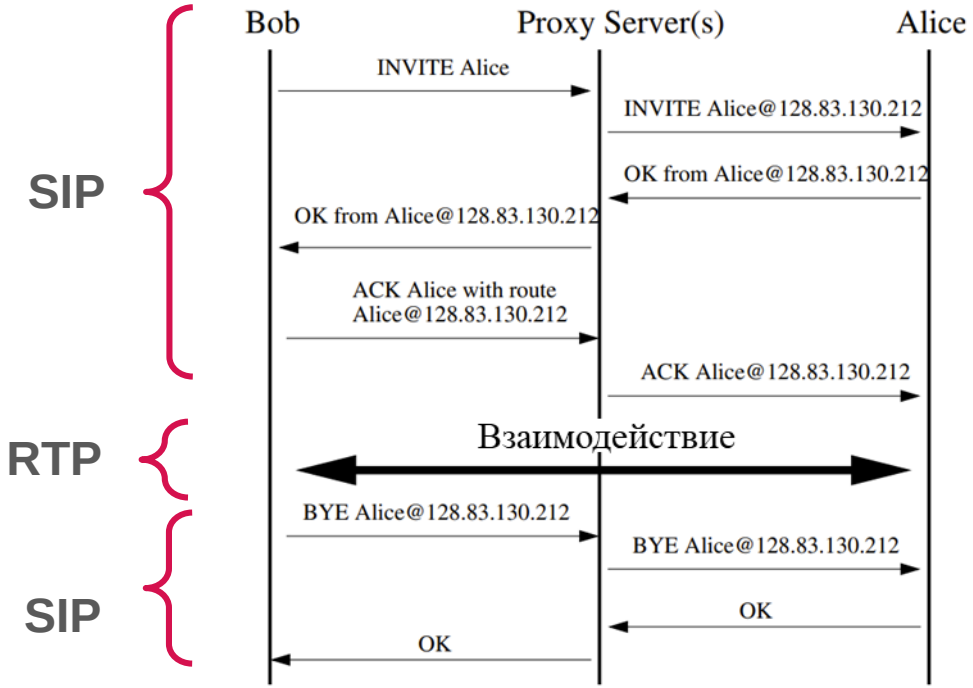
Системы VoIP

РусКрипто



Системы VoIP

РусКрипто



Системы VoIP

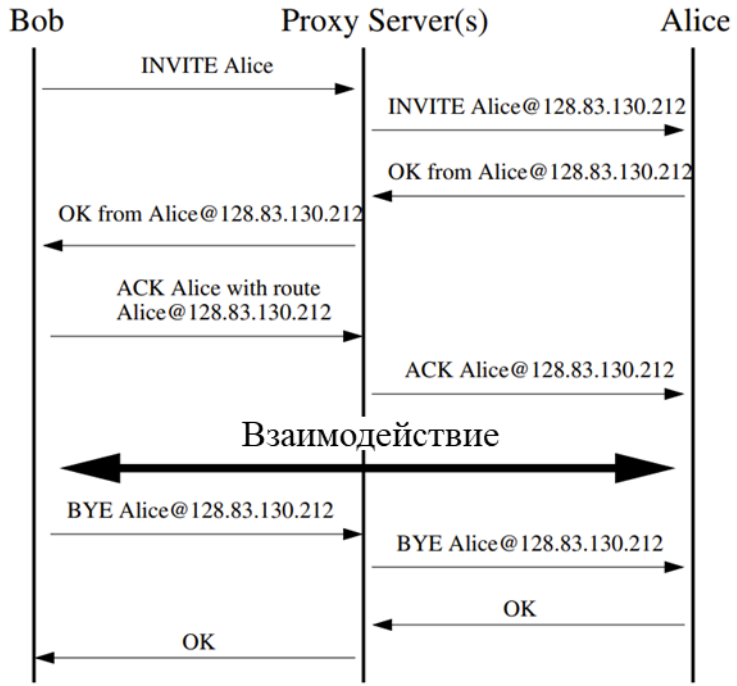
РусКрипто

- Согласование «адреса»
- Согласование инфо о медиа-потоках (SDP)
  - Количество
  - Кодеки
  - Защита

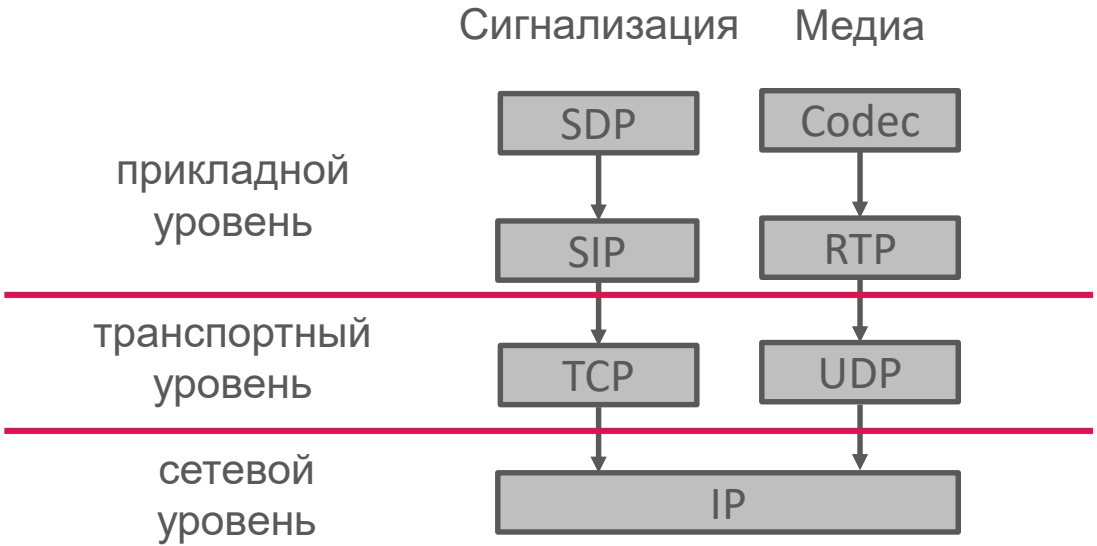
SIP

Передача RTP-пакетов и RTCP-пакетов

RTP

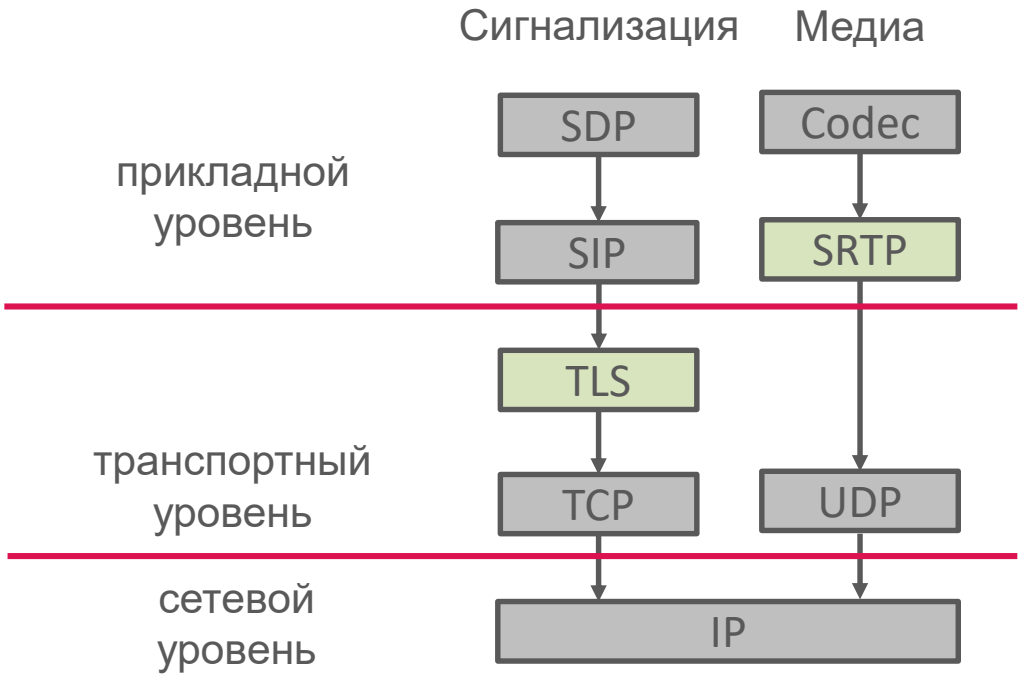


Системы VoIP



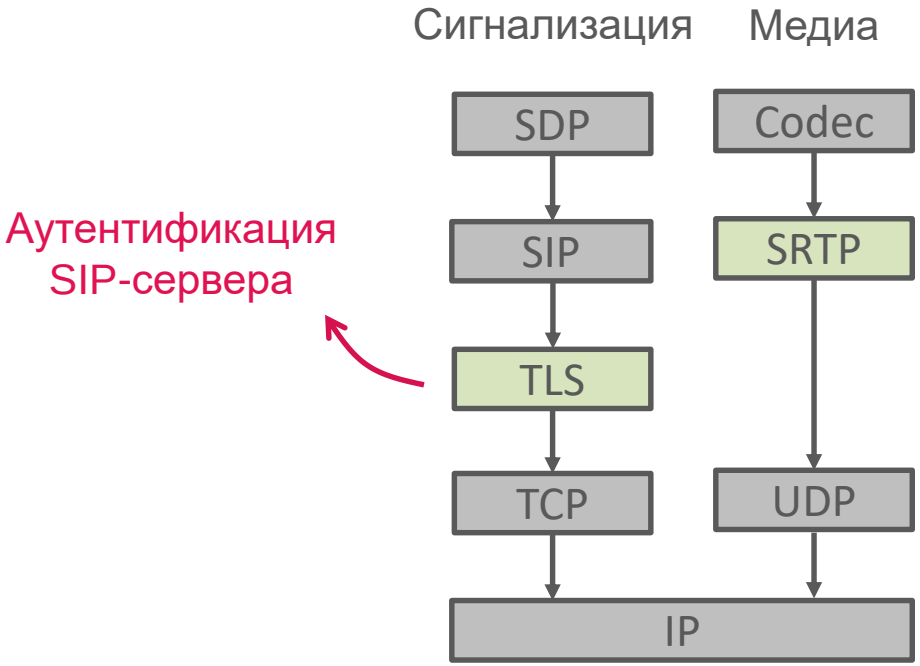
Криптография в VoIP

РусКрипто



Криптография в VoIP

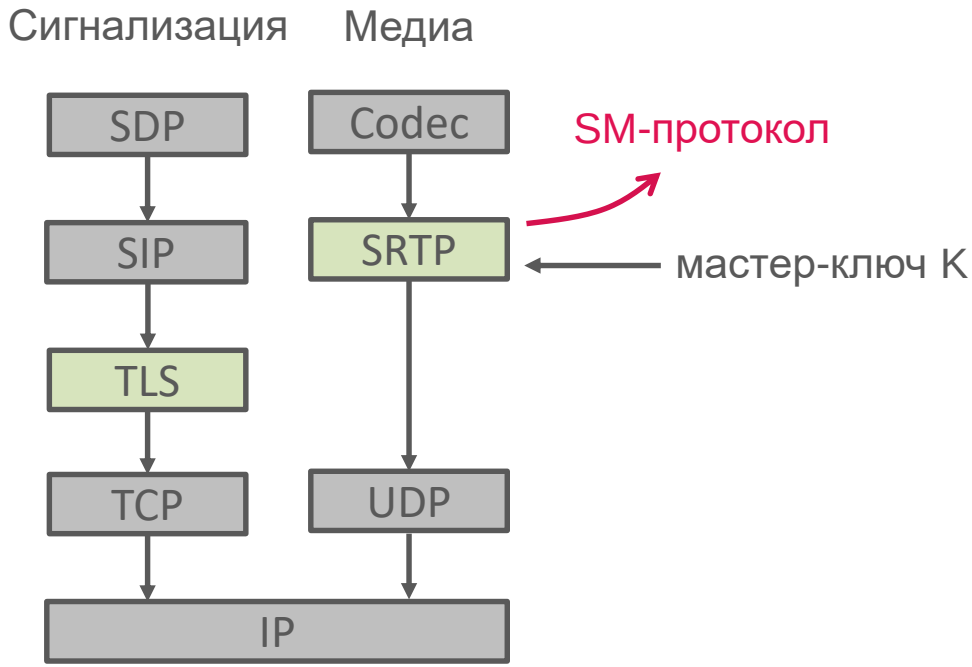
РусКрипто



Криптография в VoIP

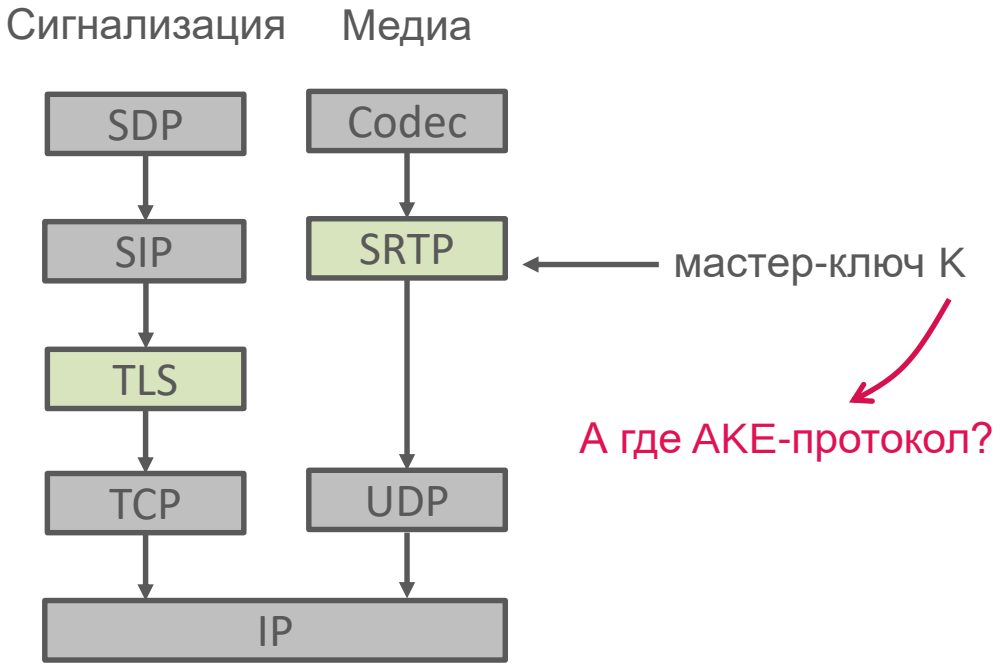
РусКрипто

Secure Real-time Transport Protocol



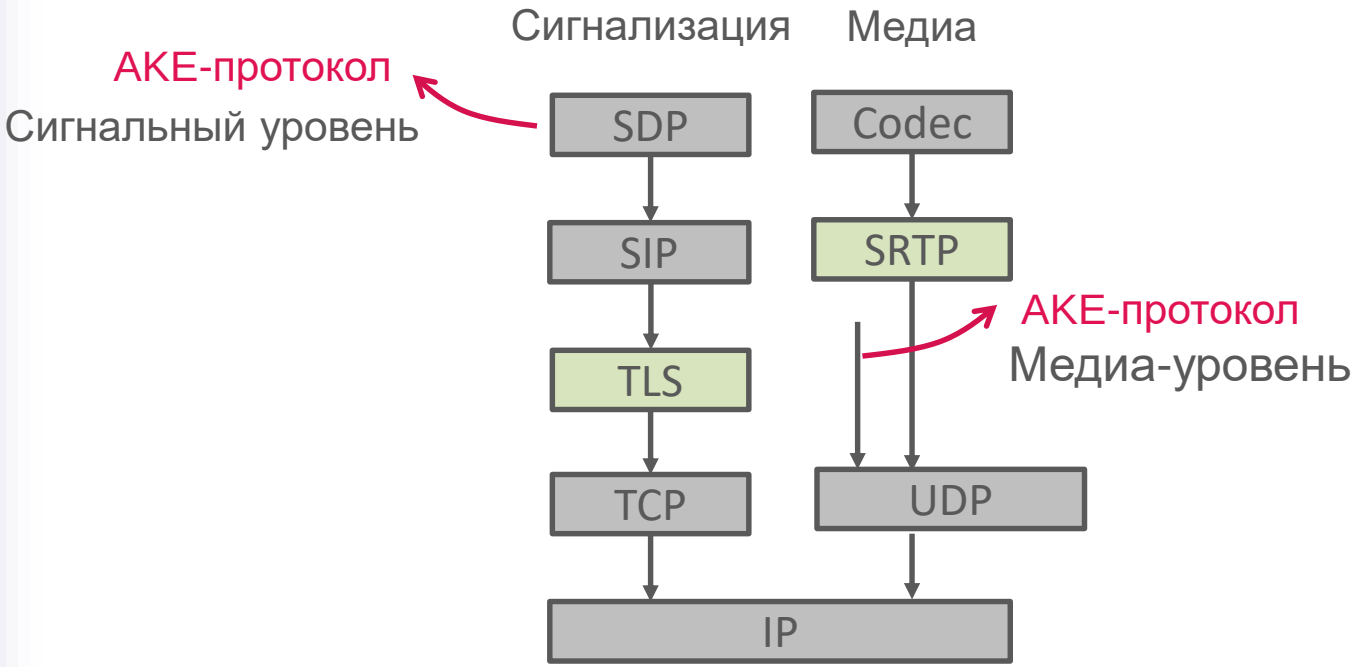
Криптография в VoIP

РусКрипто



Криптография в VoIP

РусКрипто



Аутентификация сторон

РусКрипто

end-to-end

с помощью долговременных ключей (PKI, IdP)

с помощью техники Short Authentication String (SAS)

либо абоненты аутентифицируются перед SIP-сервером, который является **доверенным**

AKE в VoIP

РусКрипто

Сигнальный уровень (в атрибутах SDP)

SDES: передача мастер-ключа в открытом виде (защита на уровне SIP)

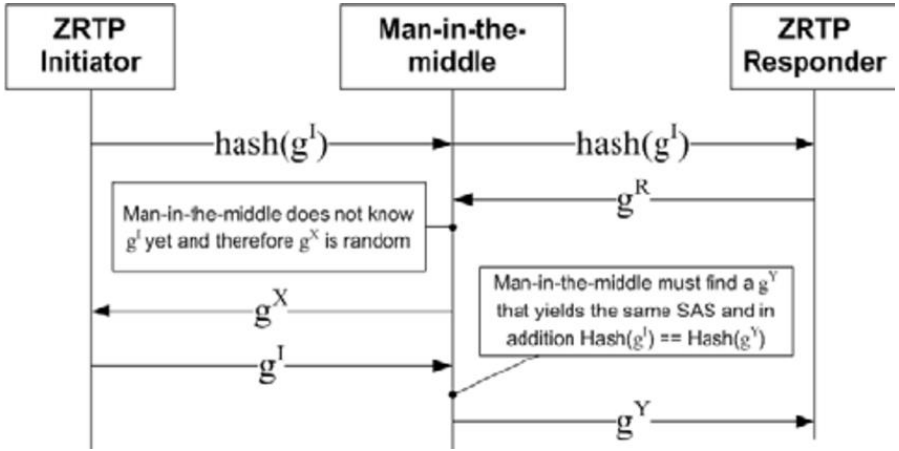
MIKEY: набор 1-RTT (запрос-ответ) протоколов (долг. ключи)
MIKEY-RSA, MIKEY-RSA-R, MIKEY-DH, …

Медиа-уровень

DTLS Handshake: мастер-ключ вырабатывается из MS (долг. ключи)

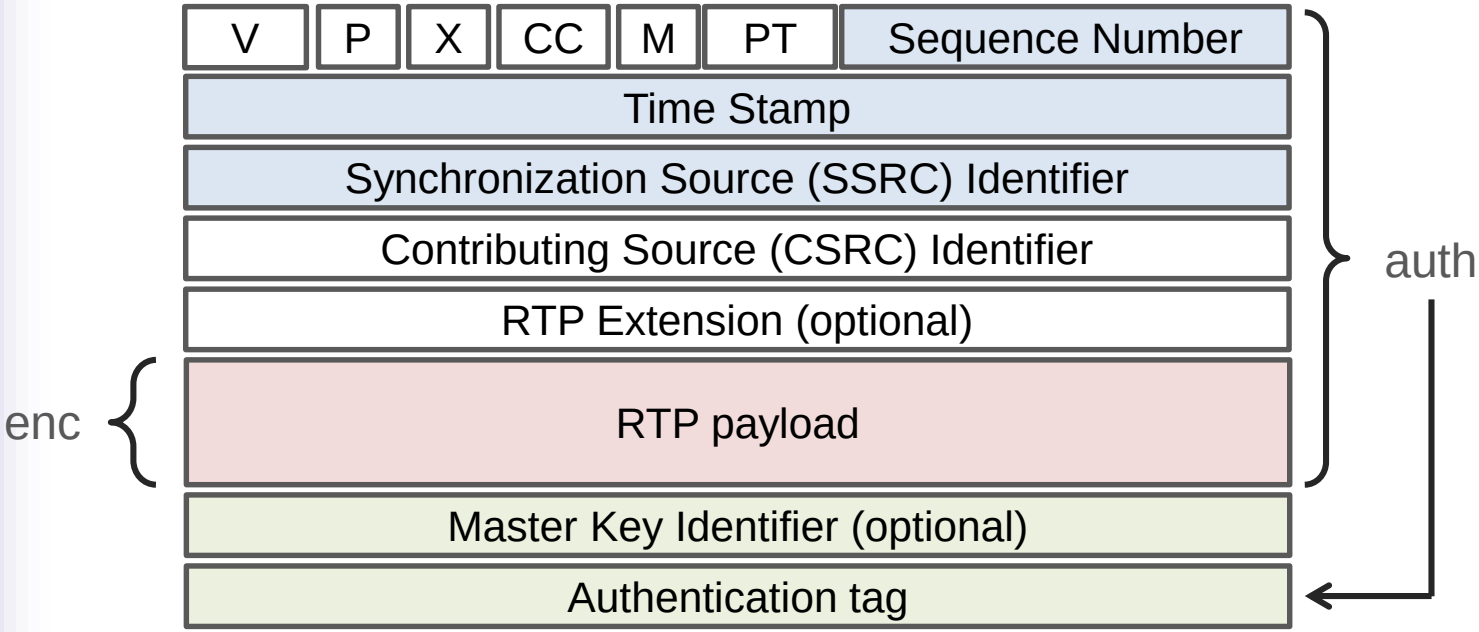
ZRTP: использует коммитмент (SAS)

«Идея» в ZRTP


ZRTP Initiator
Man-in-the-middle
ZRTP Responder
hash(g^I)
hash(g^I)
g^R
Man-in-the-middle does not know g^I yet and therefore g^X is random
Man-in-the-middle must find a g^Y that yields the same SAS and in addition Hash(g^I) == Hash(g^Y)
g^X
g^I
g^Y

SRTP в VoIP

РусКрипто



SRTP в VoIP

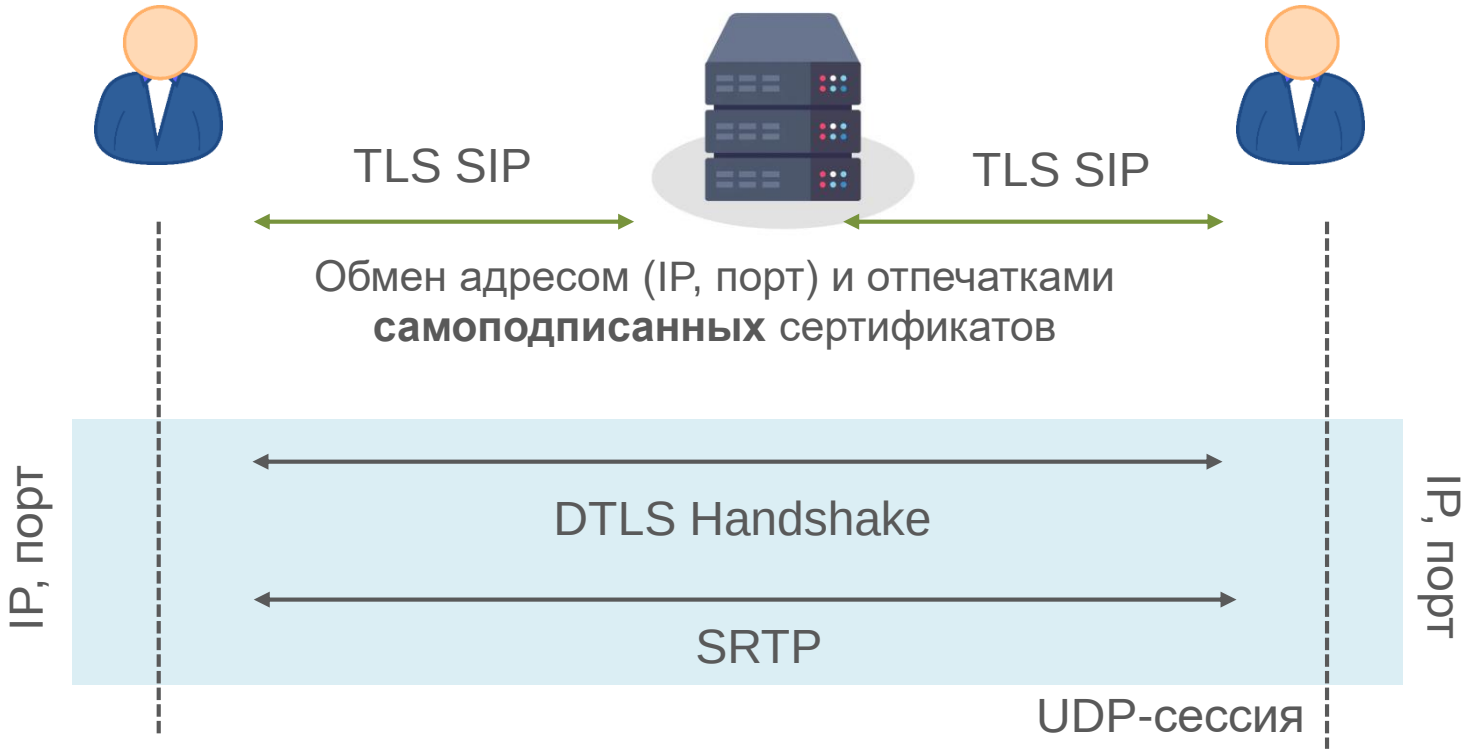
РусКрипто

SRTP (Real-Time Transport Protocol) – для передачи медиа
SRTCP (Real-Time Control Protocol) – для контроля качества связи

1. Один мастер-ключ на несколько RTP/RTCP-источников (SSRC)
2. Встроенная смена ключа
3. «Неявный» счетчик – в пакете содержатся младшие два байта (ROC)

Пример. WebRTC (VoIP в браузерах)

РусКрипто



Требования по безопасности

РусКрипто

AKE-протокол:

- Явная аутентификация ключа
  - Секретность ключа
  - Аутентификация сторон
  - Независимость ключей
  - Подтверждение ключа
- Анонимность сторон

SM-протокол:

- Конфиденциальность
- Целостность

Требования по безопасности

РусКрипто

AKE-протокол:

- Явная аутентификация ключа
  - Секретность ключа
  - Аутентификация сторон
  - **Независимость ключей**
  - **Подтверждение ключа**
- Анонимность сторон

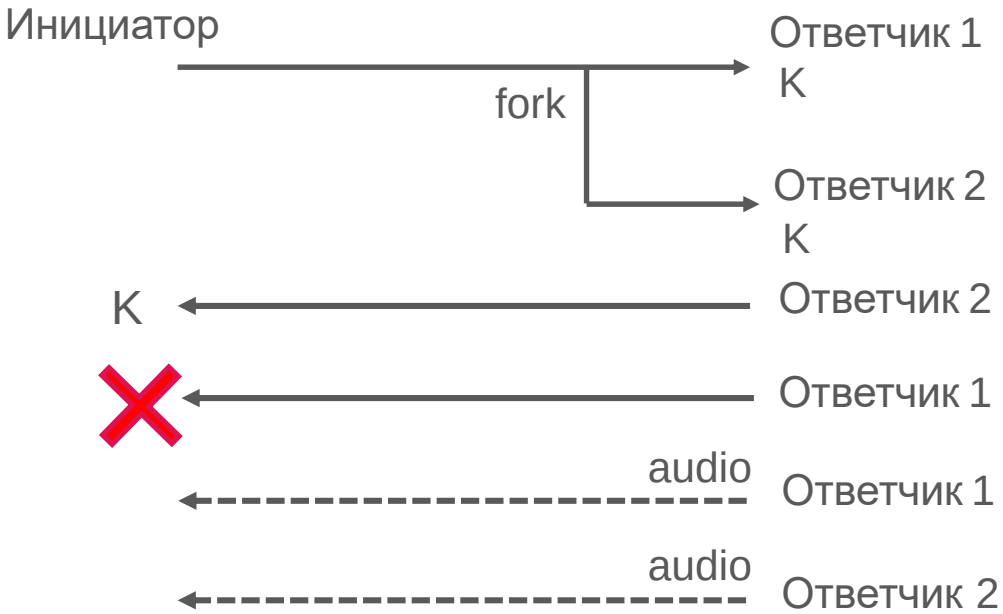
SM-протокол:

- **Конфиденциальность**
- **Целостность**

AKE-протокол. Подтверждение ключа

РусКрипто

AKE-протокол. Независимость ключей



Несколько адресатов

РусКрипто

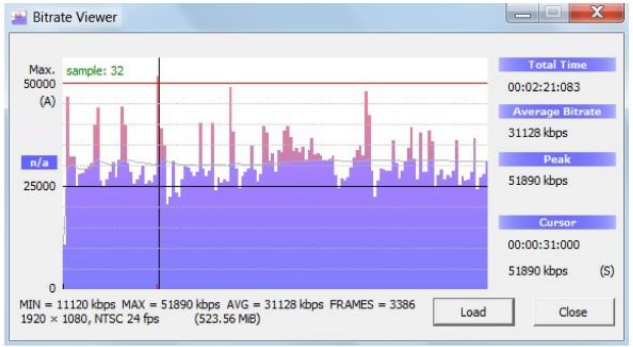
SM-протокол. Конфиденциальность

РусКрипто

В зависимости от характеристик кодека длина пакетов может зависеть от типа фонем и пауз в речи.

Constant Bit Rate

Variable Bit Rate



SM-протокол. Конфиденциальность

РусКрипто

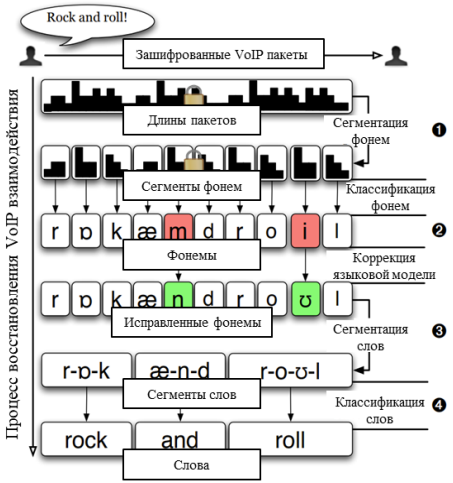
Spot me if you can:
Uncovering spoken phrases in encrypted VoIP conversations

Charles V. Wright Lucas Ballard Scott E. Coull Fabian Monrose Gerald M. Masson
Johns Hopkins University

Phonotactic Reconstruction of Encrypted VoIP Conversations:
Hookt on fon-iks

Andrew M. White* Austin R. Matthews*† Kevin Z. Snow* Fabian Monrose*
*Department of Computer Science †Department of Linguistics
University of North Carolina at Chapel Hill
Chapel Hill, North Carolina
{amw, kzsnow, fabian}@cs.unc.edu, armatthe@email.unc.edu

Если у нарушителя достаточно априорной информации, он может восстановить язык, слова и даже целые фразы



SM-протокол. Конфиденциальность

РусКрипто

Internet Engineering Task Force (IETF)
Request for Comments: 6562
Category: Standards Track
ISSN: 2070-1721

C. Perkins
University of Glasgow
JM. Valin
Mozilla Corporation
March 2012

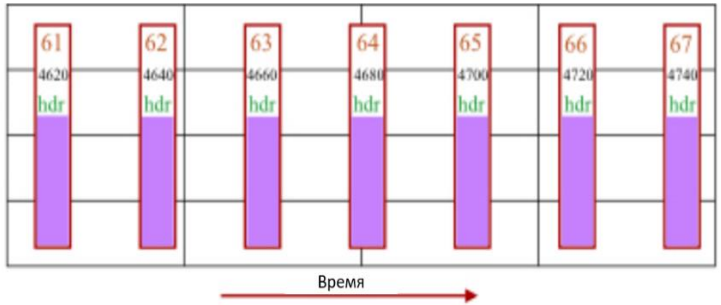
Guidelines for the Use of
Variable Bit Rate Audio with Secure RTP

Необходима конфиденциальность «на уровне потока»

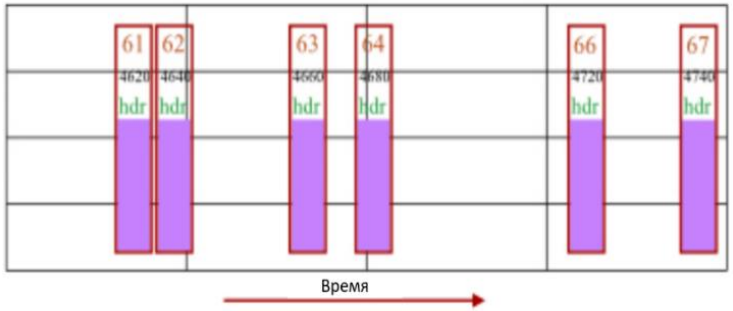
SM-протокол. Целостность

РусКрипто

Гарантированная доставка (TCP)



Негарантированная доставка (UDP)

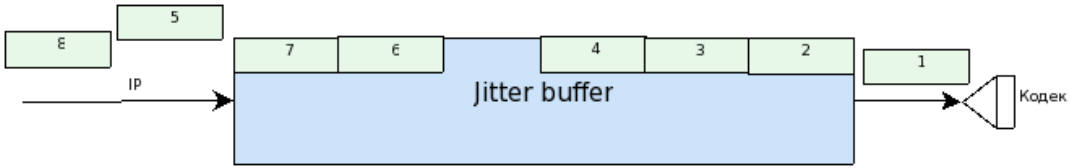


SM-протокол. Целостность

РусКрипто

- Неравномерность доставки (jitter)
- Задержка пакетов (latency)
- Утеря пакетов (loss)

решение



Пакеты «проигрываются» с небольшой задержкой
Утерянные пакеты замещаются «тишиной»

SM-протокол. Целостность

РусКрипто

Стандартно защищаемся от недектируемого:

- изменения содержимого пакетов;
- удаления пакетов из потока;
- изменения порядка пакетов в потоке;
- добавления пакетов в поток.

Однако …

SM-протокол. Целостность

РусКрипто

Если нарушитель может:

- удалить большое количество подряд идущих пакетов;
- задержать доставку пакетов

Голос передается асинхронно в обе стороны в режиме реального времени

Нарушитель может изменить смысл передаваемой информации

SM-протокол. Целостность

РусКрипто

Пример: Боб спрашивает у Алисы
- «Любишь пряники?»
- Да
- «Удалить твои данные безвозвратно»?
- Нет

Нарушитель задерживает первый ответ Алисы и удаляет второй ответ Алисы

Целостность аудиоинформации

РусКрипто

На стороне получателя необходимо контролировать:

- количество утерянных или некорректно обработанных пакетов;
- размер «скользящего окна».

Обеспечение качества связи неразрывно связано с обеспечением информационной безопасности этой связи!

РусКрипто

СПАСИБО
ЗА ВНИМАНИЕ