Лекция №4

Шифрование с аутентификацией.

Елена Киршанова

Курс “Основы криптографии”

Сегодня

До сегодняшнего дня

- Конфиденциальность (Симметрическое шифрование)
- Целостность (MAC, HMAC)

Эти примитивы защищают данные от пассивного (eavesdropping) злоумышленника

В этой лекции:
Безопасность данных относительно активного (tampering) злоумышленника

Шифрование с аутентификацией (Authenticated Encryption)

Шифрование с аутентификацией: определение

Шифрование с аутентификацией (AE) состоит из трех ppt алгоритмов

- Генерация ключа: $\mathsf{KeyGen}(1^\lambda) : k \leftarrow \mathcal{K}$
- Шифрование: $\mathsf{Enc} : \mathcal{K} \times \mathcal{M} \times \mathcal{N} \to \mathcal{C}$
- Дешифрование: $\mathsf{Dec} : \mathcal{K} \times \mathcal{C} \times \mathcal{N} \to \mathcal{M} \cup \{\perp\}$

$\mathcal{K}$ - мн-во ключей, $\mathcal{M}$ - мн-во открытых текстов, $\mathcal{C}$ - мн-во шифр-текстов, $\mathcal{N}$ - мн-во нонсов.

НОВОЕ: $\{\perp\}$ – шифр-текст отклонен

Нонсе (nonce) = “number that can only be used once”

Нонс может быть предсказуем, но он не должен быть использован дважны для одного ключа.

Корректность, безопасность шифрования с аутентификацией

Шифрование с аутентификацией (AE) состоит из трех ppt алгоритмов

- Генерация ключа: $\mathsf{KeyGen}(1^\lambda) : k \leftarrow \mathcal{K}$
- Шифрование: $\mathsf{Enc} : \mathcal{K} \times \mathcal{M} \times \mathcal{N} \to \mathcal{C}$
- Дешифрование: $\mathsf{Dec} : \mathcal{K} \times \mathcal{C} \times \mathcal{N} \to \mathcal{M} \cup \{\perp\}$

Корректность: $\forall m, \forall k, \forall n : \mathsf{Dec}(k, \mathsf{Enc}(k, m, n), n) = m$

Безопасность (неформально):

- $\mathsf{Enc}(k, m_0, n)$ неотличимо от $\mathsf{Enc}(k, m_1, n)$ $\forall m_0 ! = m_1$ (без знания k)
- Эффективный злоумышленник не в состоянии сформировать шифр-текст, которые не дешифруется в $\{\perp\}$.

Безопасность шифрования с аутентификацией

Шифрование с аутентификацией обеспечивает

- Аутентификацию: Если $\mathsf{Dec}(k, c, n) != \{\perp\}$, получатель знает, что сообщение пришло от того, кто знает k

Безопасность шифрования с аутентификацией

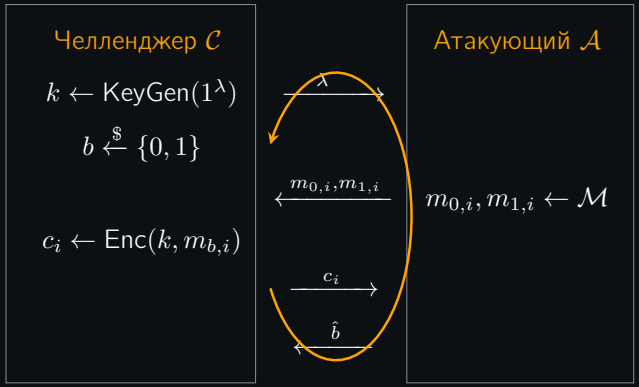
Шифрование с аутентификацией обеспечивает

- Аутентификацию: Если $\mathrm{Dec}(k, c, n) != \{\perp\}$, получатель знает, что сообщение пришло от того, кто знает k
- AE $\implies$ стойкость относительно атаки на выбранный шифр-текст

В атаке на выбранный шифр-текст (Chosen Ciphertext Attack, CCA) злоумышленник может

- получить шифрования сообщений по своему выбору
- запросить дешифрование любого шифр-текста по своему выбору кроме кроме одного фиксированного чалленджа c

Атака на выбранный открытый текст/ Chosen Plaintext Attack(CPA)

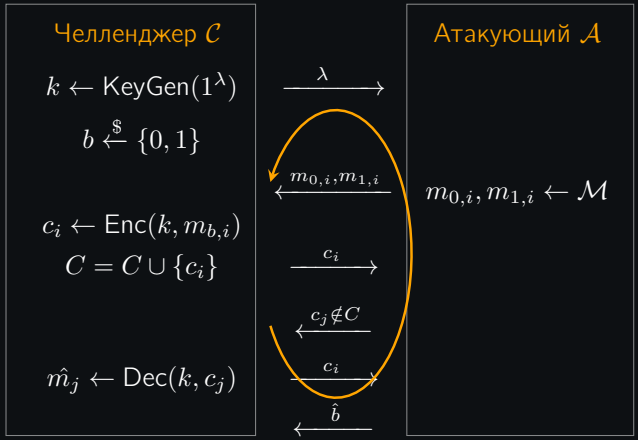


$\mathtt{W}_{\Pi,\mathcal{A}}$ – событие $b == \hat{b}$.

$\mathtt{CPAAdv} = \left|\Pr[\mathtt{W}_{\Pi,\mathcal{A}}] - \frac{1}{2}\right|$ –выигрыш $\mathcal{A}$.

Шифр-схема Π CPA безопасна, если для любого ppt $\mathcal{A}$: $\mathtt{CPAAdv} = \mathrm{negl}(\lambda)$.

Атака на выбранный шифр-текст/ Chosen Ciphertext Attack(CCA)



$\mathtt{W}_{\Pi,\mathcal{A}}$ – событие $b == \hat{b}$.

$\mathtt{CCAAdv} = \left|\Pr[\mathtt{W}_{\Pi,\mathcal{A}}] - \frac{1}{2}\right|$ –выигрыш $\mathcal{A}$.

Шифр-схема Π CCA безопасна, если для любого ppt $\mathcal{A}$: $\mathtt{CCAAdv} = \mathrm{negl}(\lambda)$.

Пример of CCA атаки (IPSec, упрощенна версия)

Пусть Enc шифрование в режиме CTR
Сообщение m состоит из хэдера “Боб’+ текст сообщения

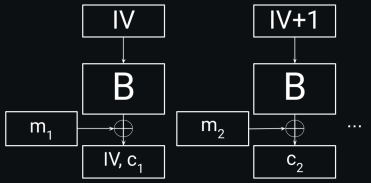
Пример of CCA атаки (IPSec, упрощенна версия)

Пусть Enc шифрование в режиме CTR
Сообщение m состоит из хэдера “Боб’+ текст сообщения

Алиса k $\xrightarrow{c = \text{Enc}(k, m=\text{Боб}||\ldots)}$ Почтовый сервер k $\xrightarrow{m}$ Боб

$\xrightarrow{c}$ Ева $\xrightarrow{\hat{c}}$

Положим `len`(“Боб”) == `len`(“Ева”) == длине блока.



$\hat{c_1} = c_1 \oplus$[“Боб”] $\oplus$ [“Ева”]

Оставшиеся блоки $\hat{c}$ равны c.

Ева узнает m, запрашивая Dec($\hat{c}$).

Атака на выбранный шифр-текст

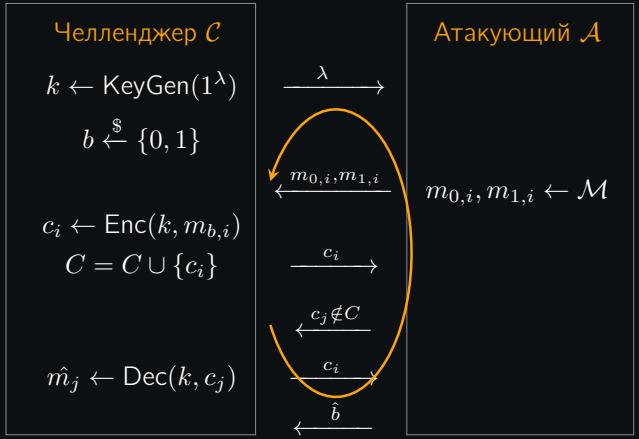
В реальных протоколах атакующий может получить доступ к (частичной) функции дешифрования.

Пример: атакующий может знать ответ на вопрос “корректно ли сформирован шифр-текст” (атака Bleichenbacher на RSA)

Симметрическое шифрование “из коробки” (CBC, CTR) не являются стойкими к таким атакам. Причина: измененный шифр-текст является корректным шифр-текстом.

Решение: шифрование с аутентификацией

Шифрование с аутентификацией стойко к CCA атаке на выбранный шифр-текст



Теорема:

1. CPA безопасная схема
2. целостность шифр-текста

$\Big\}$ $\Longrightarrow$ CCA безопасная схема

Конструкции шифрований с аутентификацией

AE = Безопасное шифрование + Криптографический MAC

Два ключа: Ключ шифрования k_E, ключ MACa K_M

Две основные парадигмы:

I. Encrypt-then-MAC

1. $c = \text{Enc}(k_E, m)$
2. $t = \text{MAC}(k_M, c)$
3. return (c, t)

Пример: IPSec

II. MAC-then-Encrypt

1. $t = \text{MAC}(k_M, n)$
2. $c = \text{Enc}(k_E, m||t)$
3. return c

Пример: SSL

Конструкции шифрований с аутентификацией

AE = Безопасное шифрование + Криптографический MAC

Два ключа: Ключ шифрования k_E, ключ MACa K_M

Две основные парадигмы:

I. Encrypt-then-MAC

1. $c = \mathsf{Enc}(k_E, m)$
2. $t = \mathsf{MAC}(k_M, c)$
3. return (c, t)

Пример: IPSec

II. MAC-then-Encrypt

1. $t = \mathsf{MAC}(k_M, n)$
2. $c = \mathsf{Enc}(k_E, m||t)$
3. return c

Пример: SSL

- Encrypt-then-MAC всегда даёт AE
- MAC-then-Encrypt даёт AE, если в Enc используются режимы шифрования CTR/CBC
- Другие комбинации MAC / Enc обычно не дают безопасное AE

AE стандарты

1. **GCM (Galois Counter Mode)**. Encrypt-then-MAC
   Шифрование: CTR mode + быстрый Mac (Carter-Wegman Mac).
   Применение: TLS
   Преимущество: скорость

AE стандарты

1. **GCM (Galois Counter Mode)**. Encrypt-then-MAC
   Шифрование: CTR mode + быстрый Mac (Carter-Wegman Mac).
   Применение: TLS
   Преимущество: скорость

2. **CCM**. MAC-then-Encrypt
   Шифрование: CBC MAC (AES)+ CTR mode (AES)
   Применение: 802.11i
   Преимущество: компактный код

AE стандарты

1. **GCM (Galois Counter Mode).** Encrypt-then-MAC
   Шифрование: CTR mode + быстрый Mac (Carter-Wegman Mac).
   Применение: TLS
   Преимущество: скорость

2. **CCM.** MAC-then-Encrypt
   Шифрование: CBC MAC (AES)+ CTR mode (AES)
   Применение: 802.11i
   Преимущество: компактный код

3. **ChaCha20-Poly1305.** Encrypt-then-MAC
   Шифрование: ChaCha20 (Enc) + Poly1305 MAC
   Применение: TLS
   Преимущество: скорость

AEAD: Authenticated Encryption with Associated Data

Часто не всё сообщение должно быть зашифровано.

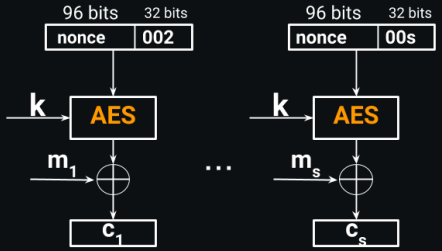
Пример: [`header`||`payload`] в интернет протоколах.

$$\underbrace{[\texttt{Associated data}||\texttt{Encrypted data}]}_{\text{Аутентификация}}$$

Самое популярное AEAD: AES-GCM AEAD

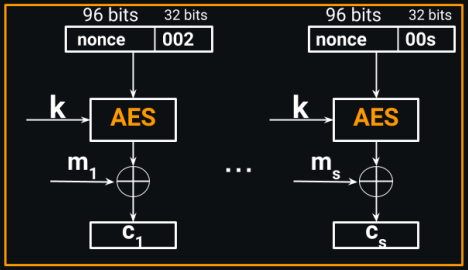
AES-GCM AEAD

Сообщение $m = (m_1, \ldots, m_s)$



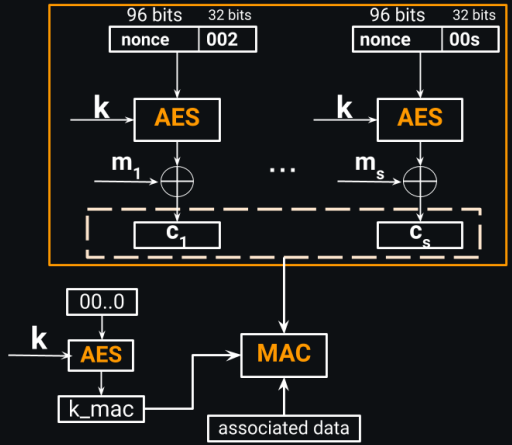
AES-GCM AEAD

Сообщение $m = (m_1, \ldots, m_s)$



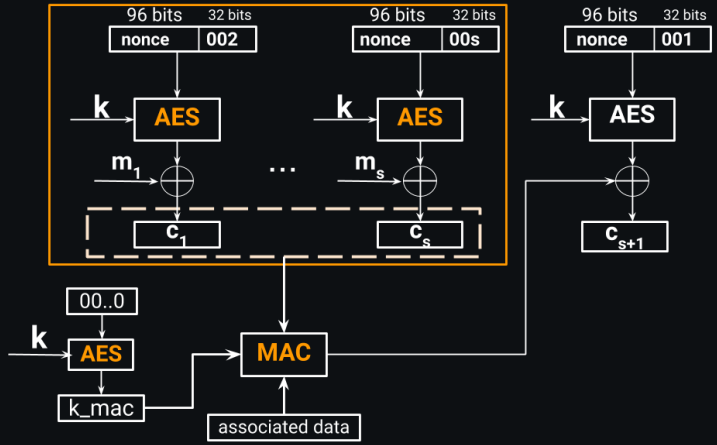
AES-GCM AEAD

Сообщение $m = (m_1, \ldots, m_s)$



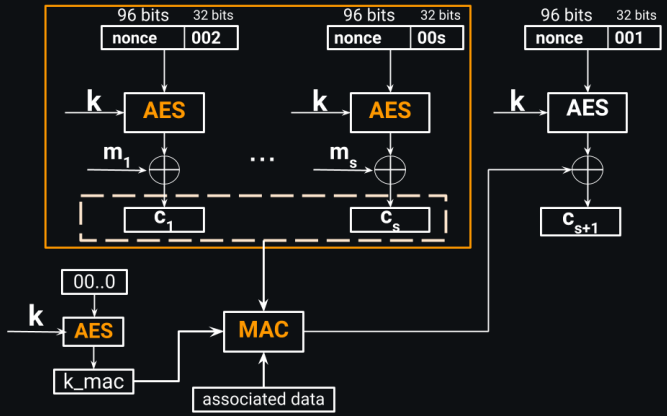
AES-GCM AEAD

Сообщение $m = (m_1, \ldots, m_s)$



Выход $(c_1, \ldots, c_s, c_{s+1})$

AES-GCM AEAD



- Используется лишь один ключ
- MAC: конструкция Картера-Вегмана на основе GHASH
- Дешифрование:
  1. Проверка MACa
  2. Dec$(c_1, \ldots, c_s)$

AEAD в TLS 1.3

Браузер

Фаза 1 Рукопожатие

Ассиметрическое Шифрование

Формирование ключей

Веб-сервер

$k_{b \to s}$

$k_{s \to b}$

$k_{b \to s}$

$k_{s \to b}$

Фаза 2 TLS протокол передачи данных

AEAD