Защита информации

Павел Юдаев

МГТУ им. Баумана, Кафедра ИУ-9

Москва, 2014

Раздел 5 - Режимы блочных шифров CBC и CTR

Используем блочный шифр
для передачи сообщений произвольной длины
при многоразовом ключе.
Сообщение разобьем на блоки.
А дальше? ECB не подходит.

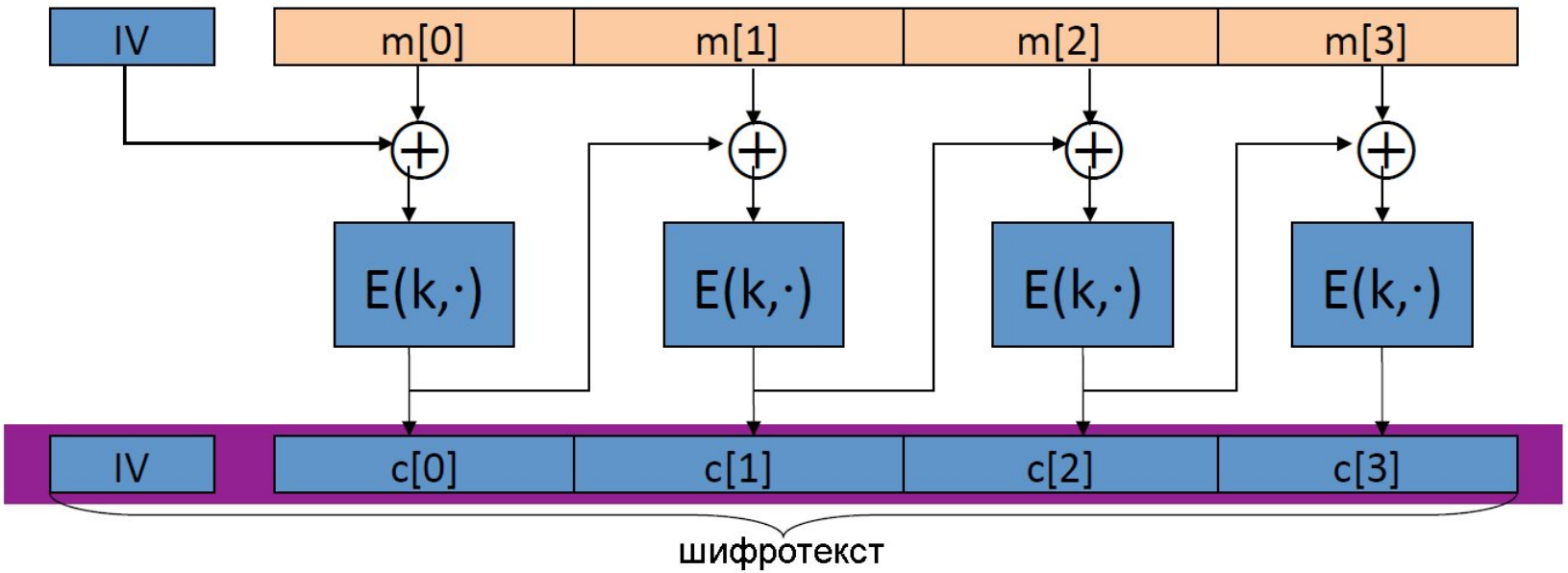
Режимы:

- CBC (1981)
- CFB (1981) - не рассм.
- OFB (1981) - не рассм.
- CTR (2001)
- и другие - не рассм.

Режим сцепления блоков - CBC

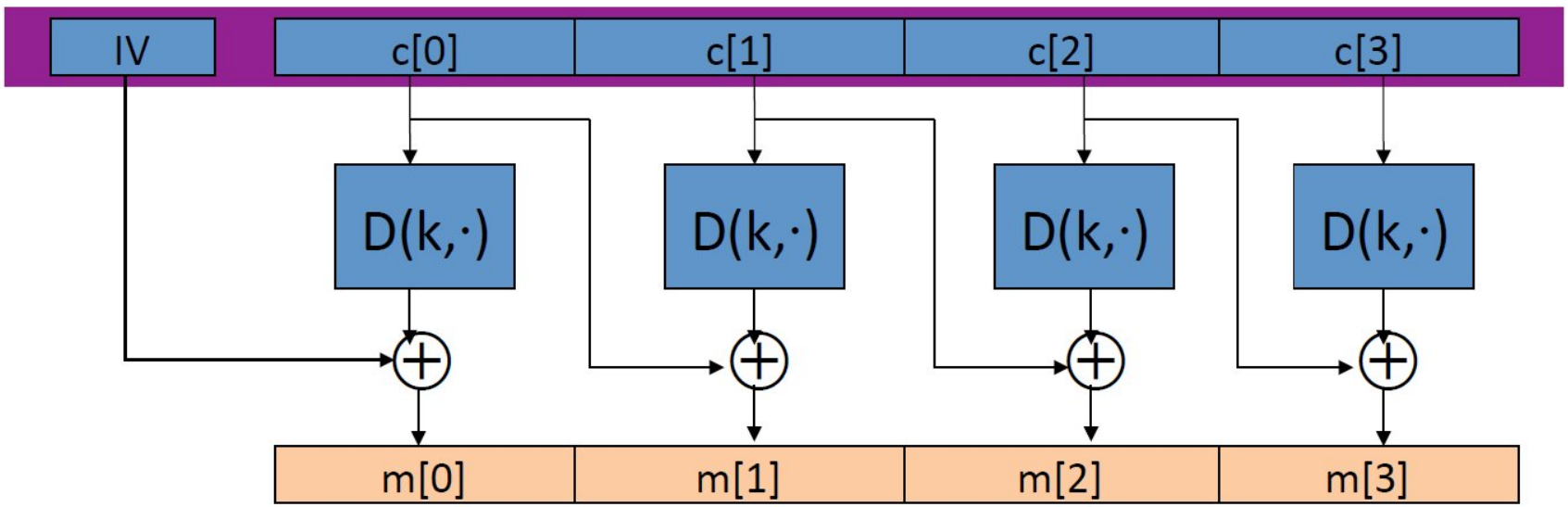
Cipher block chaining. (1981, NIST: FIPS 81)

Выбираем вектор инициализации IV (initialization vector) и:



Шифрование:
$c[0] = E(k, m[0] \oplus IV)$
$c[i] = E(k, m[i] \oplus c[i-1])$ только последовательно

Расшифрование:
$m[0] = D(k, c[0]) \oplus IV)$
$m[i] = D(k, c[i]) \oplus c[i-1])$ можно параллельно



Свойства IV для CBC:

- не секретный
- уникальный - зачем? (тривиально)
- не предсказуемый: нельзя предсказать IV для следующего сообщения по предыдущим сообщениям. Если можно предсказать, проходит атака с выбранным открытым текстом. Можно представить идею атаки. Это атака “Beast” на SSL/TLS 1.0.

Создание IV для CBC:

- IV = последний блок предыдущего сообщения (SSL 2.0, 3.0, TLS 1.0) - не годится!
- IV = криптостойкий ГПСЧ.
- IV = E(k_1, nonce), nonce - например, счетчик. Не повторяется для текущего ключа k. Требуем $k_1 \neq k$.

Задача

Почему требуем $k_1 \neq k$?
Подсказка: какой недостаток, если $k_1 = k$ и nonce не секретный?

Задача (Атака с выбранным открытым текстом на режим CBC с предсказуемым IV)

Нарисовать “эксперимент”, как злоум-к этим пользуется.

Цель злоум-ка - нарушить семантическую стойкость шифра.

Подсказка: первая пара сообщений: $m_0 = m_1 = 0$.

Вторая: $m_0 = IV_2 \oplus IV_1, m_1 \neq m_0$.

Утверждение (О стойкости CBC)

$\forall L > 0$, если E - ПСП: $K \times X \to X$, то
шифр E_{CBC} на основе этой ПСП -
семантически стойкий к атаке
с выбранным открытым текстом над (K, X^L, X^{L+1}).
При этом, если алгоритм атаки A делает q запросов к E_{CBC}, то
$\exists$ алгоритм B атаки на ПСП такой, что
$Adv_{CPA}[A, E_{CBC}] \leq 2 \cdot Adv_{PRP}[B, E] + 2q^2L^2/|X|$

Попробуйте сами доказать “на картинках”. Величину “добавки” можно не доказывать.

Пример

Влияние q, L:

q - число сообщений, L - макс. длина сообщения.

Пусть хотим $Adv < 1/2^{32}$.

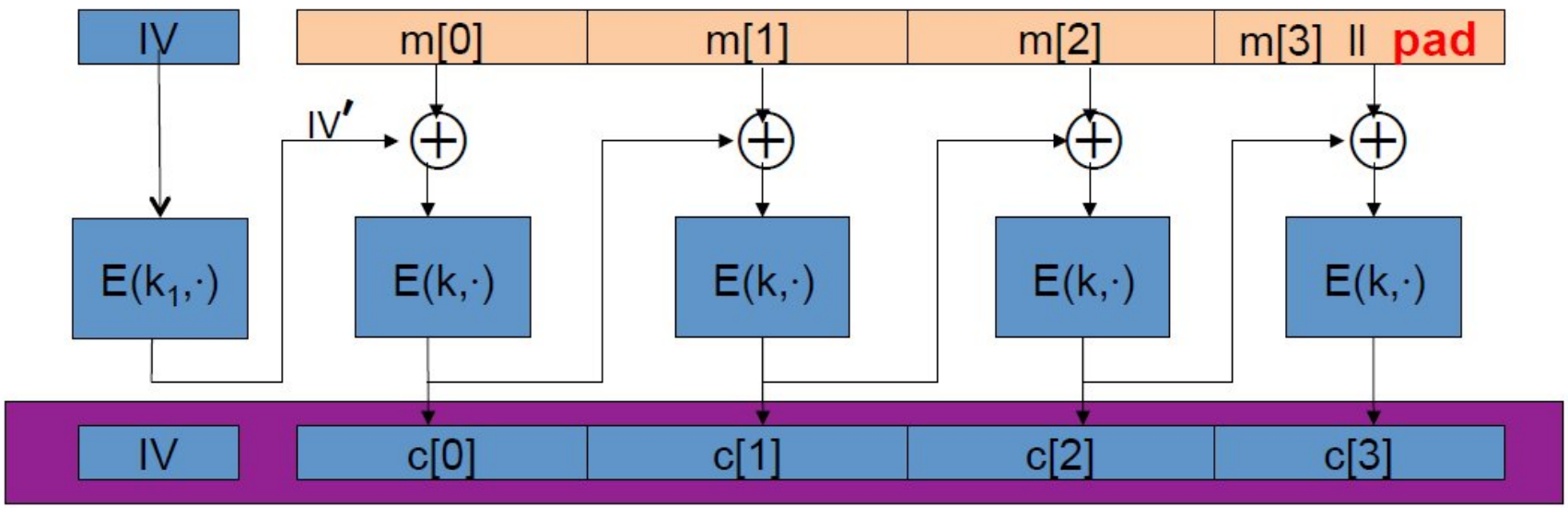
Тогда должны менять ключ после кол-ва блоков:

- 3DES, $|X| = 2^{64} \Rightarrow qL < 2^{16}$, после 2^{16} блоков
- AES, $|X| = 2^{128} \Rightarrow qL < 2^{48}$

CBC: Дополнение до длины блока перед шифрованием.

- Дополнение справа до длины блока. Если нужно дополнить n байтов, значение каждого из этих байтов равен n.
- Если длина текста кратна длине блока, добавим целый блок с нулями.

Это дополнение позволяет удалить его при расшифровании.



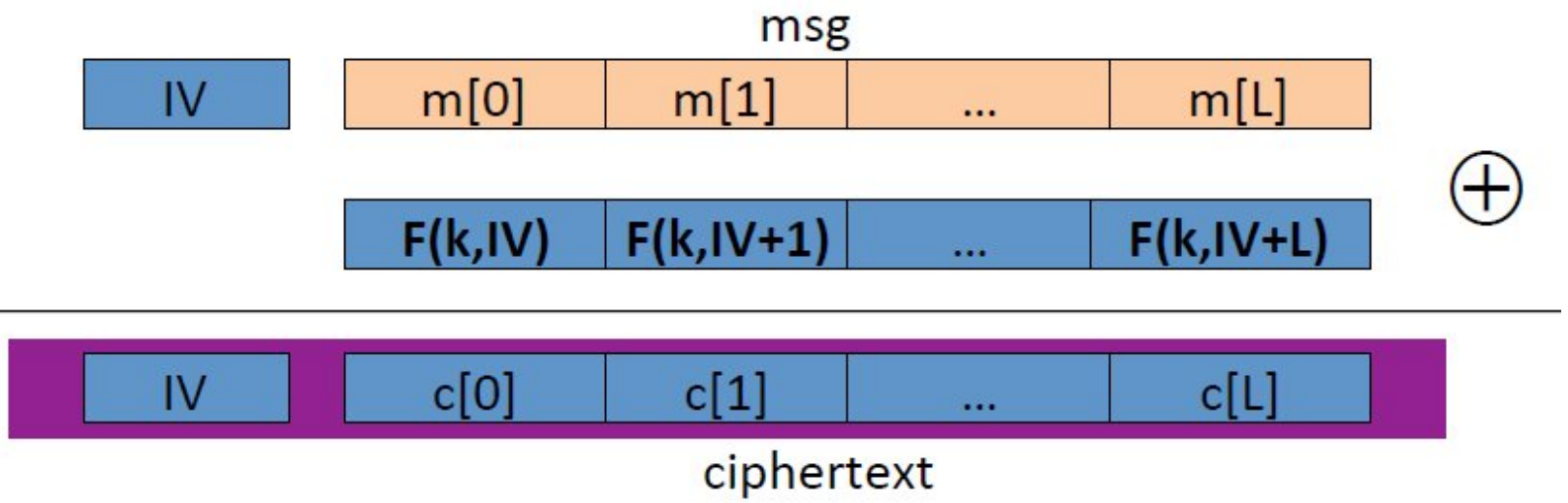
Проблемы использования режима CBC

- padding oracle attack на TLS (2002) - оракул правильного окончания блока: вторичный канал по возвращаемому значению или времени выполнения. Не проходит только из-за смены ключей в TLS.
- BEAST attack на TLS (2004, 2011) - предсказуемый IV
- Lucky 13 attack на TLS (2013) - развитие padding oracle attack

Раздел 5 - Режимы блочных шифров CBC и CTR

Режим случайного счетчика, RandCTR, CTR
Randomized counter mode (2001, NIST: SP800-38A)

$F : K \times \{0,1\}^n \to \{0,1\}^n$ - стойкая ПСФ.
Шифрование: выберем случайный IV длиной n и:

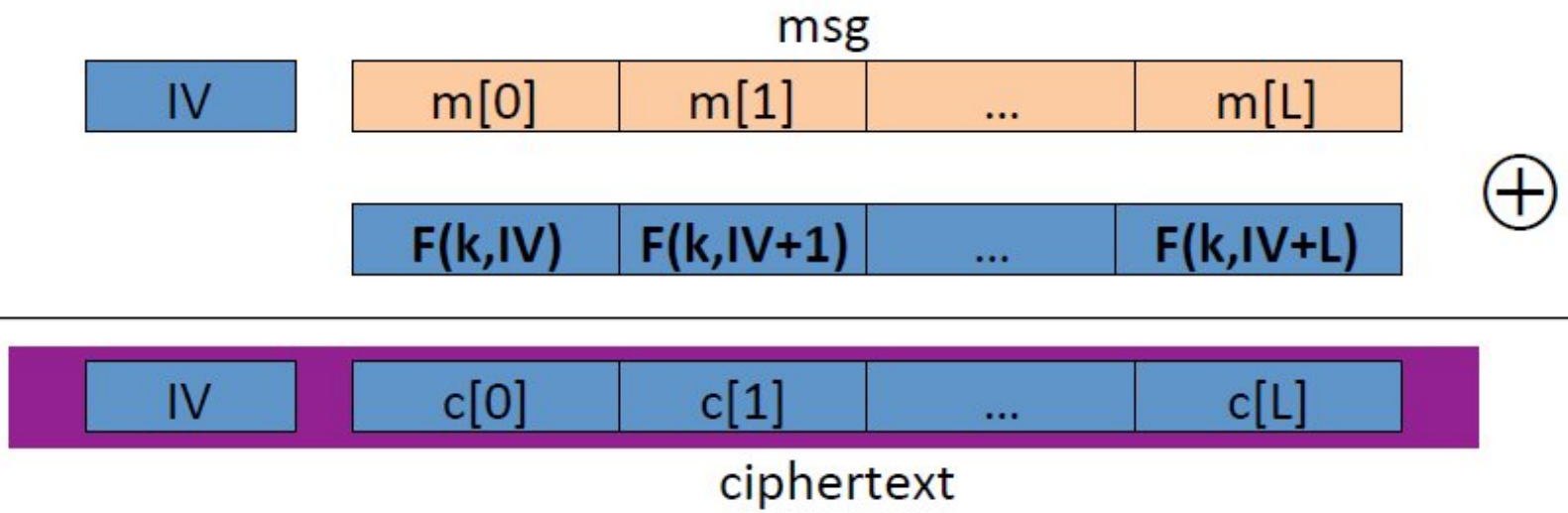


Шифрование: можно параллельно. CBC - нельзя.

Вариация: **режим nonce-счетчика**
Nonce counter mode.

Чтобы пара (k, x) не повторилась для разных сообщений,

IV = (nonce (64 bit) || counter (64 bit)),
counter начинается с 0 для каждого сообщения.



Режим CTR: не требуется дополнение до длины блока.

Утверждение (О стойкости CTR режима со случайным IV)

$\forall L > 0$, если F - криптостойкая ПСФ: $K \times X \to X$, то
шифр E_{CTR} семантически стойкий к
атаке с выбранным открытым текстом над (K, X^L, X^{L+1}).
При этом, если оракул A который делает q запросов к E_{CTR},
то $\exists$ оракул B для ПСФ:
$Adv_{CPA}[A, E_{CTR}] \leq 2 \cdot Adv_{PRF}[B, F] + 2qL^2/|X|$

Без док-ва. Попробуйте сами доказать “на картинках”.

Замечание

Необходимо, чтобы $2qL^2/|X|$ было пренебр. малым. Это лучше, чем CBC.

Задача

Если хотим $Adv_{CPA}[A, E_{CTR}] \leq 1/2^{32}$,
через сколько блоков надо менять ключ для шифров 3DES (блок - 64 бита) и AES (блок - 128 бит)?

Сравнение режимов CBC, RandCTR

- используем ПСП или ПСФ?
- параллельные вычисления при шифровании, расшифровании?
- чем определяется частота смены ключа при случайном IV?
- дополнение открытого текста до длины блока?
- увеличение длины 1-байтового сообщения?

Итак, мы исследовали стойкость к атаке с выбранным открытым текстом:

- при однократном использовании ключа
- при многократном использовании ключа

- Одноразовый ключ: стойкость имеют поточные шифры и DetCTR режим блочных шифров.
- Многоразовый ключ: стойкость имеют режимы блочных шифров CBC, RandCTR (и другие).

Семантическая стойкость шифра к этой атаке
не обеспечивает целостность шифротекста.
Любой ш/т будет принят и расшифрован.

Литература к лекции:

1. NIST, Recommendation for Block Cipher Modes of Operation,
http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf
- Режимы работы блочных шифров

2. S.Vaudenay, Security Flaws Induced by CBC Padding
Applications to SSL, IPSEC, WTLS...
http://www.iacr.org/cryptodb/archive/2002/EUROCRYPT/2850/2850.pdf
- Padding oracle attack на режим CBC