Нужно, чтобы длина в битах(s) открытого текста(m) была кратна длине блока(n), чтобы мочь воспользоваться блочным шифром

- есть различные **режимы дополнения текста**, чтобы сделать его длину кратной длине блока

Самый простой способ дополнения это добить 1 и нулями, т.е

$$m' = m10\cdots0$$

- это работает, т.к получается однозначно находить конец текста - это последний бит перед последней единицей
- если текст изначально был кратен длине блока, то придётся добавить дополнительный блок, чтобы смочь распознать конец

Режимы использования блочных шифров

Режим электронной кодовой книги(ECB, Electronic Code Book)

разбиваем открытый текст на блоки

$m = m_1 m_2 \cdots m_t$

- $\forall m_i \in \{0,1\}^n$

$c = c_1 c_2 \cdots c_t$

- $\forall c_i = E(m_i, k)$
- т.е к каждому блоку применяем блочный шифр, а затем просто склеиваем результаты
- $\forall m_i = D(c_i, k)$

Достоинства

Шифровать очень просто, по сути это шифр простой замены на огромном алфавите

Недостатки

- Одинаковые блоки шифруются одинаково, позволяет получить инфу
- Сохранение структуры открытого текста в шифр тексте

Режим сцепления блоков(CBC, Cipher Block Chaininh)

Создадим несекретный начальный блок(начальный вектор)

$$C_0 = IV$$

Шифрование

$c_i = E(c_{i-1} + m_i, k)$

Шифрование расшифрование

$m_i = c_{i-1} \bigoplus D(c_i, k)$

Теперь если регулярно менять начальный вектор, то блоки в начале и в конце будут разные, т.к видно что они зависят от предыдущих

Если при искажении испортился один блок криптограммы, то расшифровании испортится 2 соседних блока открытого текста(m_i и m_{i+1})

Режим обратной связи по шифртексту(CFB Cipher feed back)

Опять создаём начальный вектор $c_0 = IV$

Шифрование

$c_i = m_i \bigoplus E(c_{i-1})$

Расшифрование

$m_i = c_i \bigoplus E(c_{i-1})$

- В этом режиме не требуется отдельная функция расшифрования, нужно уметь только шифровать
- Ошибка из-за искажений в одном блоке криптограммы влияет на 2 соседних блока открытого текста при расшифровании

- не сохраняет структуру открытого текста

Режим обратной связи по выходу (OFB output feed back)

Берём $z_0 = IV$ начальный вектор
с помощью функции E делаем цепочку: * $z_i = E(z_{i-1}, k)$
используем цепочки z_i в качестве одноразового щита

- $c_i = m_i \bigoplus z_i$
- $m_i = c_i \bigoplus z_i$

по существу создаём одноразовый щиты с помощью ключа, а затем используем их по одному разу

- Не выдерживает атаки номер 2
- маленькая длина периода порядка 2^{32}. т.е есть шанс, что используем один и тот же одноразовый счит 2 раза

Режим Гаммирования

это доработка режима OFB
$\measuredangle$ бесконечную непереодическую последовательность
Пусть $z_i = E(i, k)$, где $i \in \mathbb{N}$. Теперь последовательность $\{z_i\}$ - не содержит периодов, т.к их не было в $\mathbb{N}$

- $c_i = m_i \bigoplus z_i$
- $m_i = c_i \bigoplus z_i$

теперь период это 2^n

Эти режимы есть в госте 34,13-2015

- пункт 1 это ECB
- пункт 2 это Гаммирование
- пункт 3 это OFB
- пункт 4 это CBC
- пункт 5 это CFB

начальный вектор IV может оказаться длиннее блока

Пример изменение работы CBC когда IV больше длины блока

- n - длина блока
- m - длина начального вектора, т.е $IV \in \{0,1\}^m$
- R - регистр сдвига длины m

$R_i = IV$
MSB_n - взятие n старших битов от аргумента
LSB_n - взятие n младших битов от аргумента
$c_i = E(m_i \bigoplus MSB_n(R_i), k)$
$R_{i+1} = LSB_{m-n}(R_i)||c_i$