ГОСТ 34.13-2018 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров»

Дата введения

2019-06-01 (6-ого января 2019-ого года).

Область применения

Настоящий стандарт распространяется на криптографическую защиту информации и определяет режимы работы блочных шифров.

Назначение стандарта

Режимы работы блочных шифров, определенные в настоящем стандарте, рекомендуется использовать при разработке, производстве, эксплуатации и модернизации средств криптографической защиты информации в системах обработки информации различного назначения.

Перечень применяемых терминов и определений

- Шифр (cipher): Криптографический метод, используемый для обеспечения конфиденциальности данных, включающий алгоритм зашифрования и алгоритм расшифрования.
- Шифртекст (ciphertext): Данные, полученные в результате зашифрования открытого текста в целях скрытия его содержания.
- Зашифрование (encryption): Обратимое преобразование данных с помощью шифра, который формирует шифртекст из открытого текста.
- Расшифрование (decryption): Операция, обратная к зашифрованию.
- Блок (block): Строка бит определенной длины.
- Открытый текст (plaintext): Незашифрованная информация.
- Блочный шифр (block cipher): Шифр из класса симметричных криптографических методов, в котором алгоритм зашифрования применяется к блокам открытого текста для получения блоков шифртекста.

Краткое (1-2 страницы) описание содержимого ГОСТа

Режимы работы алгоритмов блочного шифрования

Режим простой замены

Общие положения

Длина сообщений, зашифровываемых в режиме простой замены, должна быть кратна длине блока базового алгоритма блочного шифрования n, поэтому при необходимости к исходному сообщению должна быть предварительно применена процедура дополнения.

Зашифрование (расшифрование) в режиме простой замены заключается в зашифровании (расшифровании) каждого блока текста с помощью базового алгоритма блочного шифрования.

Зашифрование

Открытый и при необходимости дополненный текст $P \in V_n^*$, $|P| = n \cdot q$, представляется в виде: $P = P_1 \| P_2 \| \dots \| P_q$, $P_i \in V_n$, $i = 1, 2, \dots, q$.

Блоки шифртекста вычисляют по следующему правилу: $C_i = e_K(P_i)$, $i = 1, 2, \dots, q$.

Результирующий шифртекст имеет вид: $C = C_1 \| C_2 \| \dots \| C_q$.

Расшифрование

Шифртекст представляется в виде: $C = C_1 \| C_2 \| \dots \| C_q$, $C_i \in V_n$, $i = 1, 2, \dots q$.

Блоки открытого текста вычисляются по следующему правилу: $P_i = d_K(C_i)$, $i = 1, 2, \dots, q$.

Исходный (дополненный) открытый текст имеет вид: $P = P_1 \| P_2 \| \dots \| P_q$.

Режим гаммирования

Общие положения

Параметром режима гаммирования является целочисленная величина s, 0 < s < n. При использовании режима гаммирования не требуется применение процедуры дополнения сообщения.

Для зашифрования (расшифрования) каждого отдельного открытого текста на одном ключе используется значение уникальной синхропосылки $IV \in V_{n/2}$.

Зашифрование в режиме гаммирования заключается в покомпонентном сложении открытого текста с гаммой шифра, которая вырабатывается блоками длины s путем зашифрования последовательности значений счетчика $CTR_i \in V_n$, $i = 1, 2, \dots$, базовым алгоритмом блочного шифрования с последующим усечением. Начальным значением счетчика является $CTR_1 = I_n(IV) = IV \| 0^{n/2}$. Последующие значения счетчика вырабатываются с помощью функции Add: $V_n \to V_n$ следующим образом: $CTR_{i+1} = \mathrm{Add}(CTR_i) = \mathrm{Vec}_n(\mathrm{Int}_n(CTR_i) \boxplus_n 1)$.

Зашифрование

Открытый текст $P \in V_s^*$ представляется в виде $P = P_1 \| P_2 \| \dots \| P_q$, $P_i \in V_s$, $i = 1, 2, \dots, q-1$, $P_q \in V_r$, $r \le s$. Блоки шифртекста вычисляются по следующему правилу $\begin{cases} C_i = P_i \oplus T_s(e_K(CTR_i)), & i = 1, 2, \dots, q-1, \\ C_q = P_q \oplus T_r(e_K(CTR_q)). \end{cases}$.

Результирующий шифртекст имеет вид: $C = C_1 \| C_2 \| \dots \| C_q$.

Расшифрование

Шифртекст представляется в виде: $C = C_1 \| C_2 \| \ldots \| C_q,\ C_i \in V_s,\ i = 1, 2, \ldots, q-1,\ C_q \in V_r,\ r \le s.$ Блоки открытого текста вычисляются по следующему правилу: $\begin{cases} P_i = C_i \oplus T_s(e_K(CTR_i)),\ i = 1, 2, \ldots, q-1, \\ P_q = C_q \oplus T_r(e_K(CTR_q)). \end{cases}$.

Исходный открытый текст имеет вид: $P = P_1 \| P_2 \| \ldots \| P_q.$

Режим выработки имитовставки

Общие положения

Режим выработки имитовставки. описание которого представлено ниже, реализует конструкцию OMAC1 (стандартизован в ISO под названием CMAC).

Параметром режима является длина имитовставки (в битах) 0 < s <= n.

Выработка вспомогательных ключей

При вычислении значения имитовставки используются вспомогательные ключи, которые вычисляются с использованием ключа К. Длины вспомогательных ключей равны длине блока n базового алгоритма блочного шифрования.

Процедура выработки вспомогательных ключей может быть представлена в следующем виде:

$R = e_K(0^n);$

$K_1 = \begin{cases} R \ll 1, & \text{если } MSB_1(R) = 0, \\ (R \ll 1) \oplus B_n, & \text{иначе;} \end{cases}$

$K_2 = \begin{cases} K_1 \ll 1, & \text{если } MSB_1(K_1) = 0, \\ (K_1 \ll 1) \oplus B_n, & \text{иначе,} \end{cases}$, где $B_{64} = 0^{59} \| 11011,\ B_{128} = 0^{120} \| 10000111.$

Вычисление значения имитовставки

Процедура вычисления значения имитовставки похожа на процедуру зашифрования в режиме простой замены с зацеплением при m = n и инициализации начального заполнения регистра сдвига значением 0^n: на вход алгоритму шифрования подается результат покомпонентного сложения очередного блока текста и результата зашифрования на предыдущем шаге. Основное отличие заключается в процедуре обработки последнего блока: на вход базовому алгоритму блочного шифрования подается результат покомпонентного сложения последнего блока, результата зашифрования на предыдущем шаге и одного из вспомогательных ключей. Конкретный вспомогательный ключ выбирается в зависимости от того, является ли последний блок исходного сообщения полным или нет. Значением имитовставки MAC является результат применения процедуры усечения к выходу алгоритма шифрования при обработке последнего блока.

Исходное сообщение $P \in V^*$, для которого требуется вычислить имитовставку. представляется в виде: $P = P_1 \| P_2 \| \ldots \| P_q$, где $P_i \in V_n,\ i = 1, 2, \ldots, q-1,\ P_q \in V_r,\ r \le n.$

Процедура вычисления имитовставки описывается следующим образом: $\begin{aligned} &C_0 = 0^n, \\ &C_i = e_K(P_i \oplus C_{i-1}),\ i = 1, 2, \ldots, q-1, \\ &MAC = T_s(e_K(P_q^* \oplus C_{q-1} \oplus K^*)), \end{aligned}$

, где $K^* = \begin{cases} K_1, & \text{если } |P_q| = n, \\ K_2, & \text{иначе,} \end{cases}$.

P_q^* - последний блок сообщения, полученного в результате дополнения исходного сообщения.