ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ

РЕЖИМЫ РАБОТЫ ДЛЯ АЛГОРИТМА *n*-РАЗРЯДНОГО БЛОЧНОГО ШИФРОВАНИЯ

Издание официальное

ГОССТАНДАРТ РОССИИ
Москва

ПРЕДИСЛОВИЕ

1 РАЗРАБОТАН И ВНЕСЕН Техническим комитетом ТК 22 «Информационная технология»

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Постановлением Госстандарта России от 28.12.93 № 272

Настоящий стандарт подготовлен на основе применения аутентичного текста международного стандарта ИСО/МЭК 10116—91 «Информационная технология. Режимы работы для алгоритма n-разрядного блочного шифрования»

3 ВВЕДЕН ВПЕРВЫЕ

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

РЕЖИМЫ РАБОТЫ ДЛЯ АЛГОРИТМА *n*-РАЗРЯДНОГО БЛОЧНОГО ШИФРОВАНИЯ

Information technology. Modes of operation for an n-bit block cipher algorithm

Дата введения 1994—07—01

1 ОБЛАСТЬ ПРИМЕНЕНИЯ

Настоящий стандарт описывает четыре режима работы для алгоритма *n*-разрядного блочного шифрования.

Примечание 1 — Приложение А содержит пояснения характеристик каждого режима.

Настоящий стандарт устанавливает четыре определенных режима так, что при применении алгоритма *n*-разрядного блочного шифрования (например, защиты передачи данных, хранения данных, подтверждения подлинности) этот стандарт представляет полезную справку, например для требований к режиму работы и значениям параметров (соответственно).

Для некоторых режимов набивка может требовать гарантий, чтобы все переменные открытого текста были необходимой длины.

Примечание 2 — Для режима работы шифрования с обратной связью — CFB (Cipher Feedback) (см. раздел 6) определяются два параметра: *j* и *k*. Для режима работы с обратной связью по выходу — OFB (Output Feedback) (см. раздел 7) задается один параметр *j*. При использовании одного из этих режимов работы значение(я) параметров должно быть выбрано и применено всеми сторонами при передаче сообщений.

Издание официальное

2 ОПРЕДЕЛЕНИЯ

В настоящем стандарте использованы следующие определения.

2.1 Открытый текст — незашифрованная информация.

2.2 Шифротекст — зашифрованная информация.

2.3 Алгоритм n-разрядного блочного шифрования — алгоритм блочного шифрования, в котором блоки открытого текста и блоки шифротекста имеют длину n разрядов.

2.4 Связывание блоков — такое шифрование информации, при котором каждый блок шифротекста является криптографически зависимым от предшествующего блока шифротекста.

2.5 Начальное значение — IV (Initializing Value) — значение, используемое в определении начальной точки процесса шифрования.

2.6 Запускающая переменная — SV (Starting Variable) — переменная, полученная от начального значения и используемая в определении запускающей точки режимов работы.

Примечание 3 — Метод получения запускающей переменной от начального значения не определен в настоящем стандарте. Он требует описания при любом использовании режимов работы.

2.7 Криптографическая синхронизация — согласование процесса шифрования и дешифрования.

3 ОБОЗНАЧЕНИЯ

В настоящем стандарте функциональное отношение, определяемое алгоритмом блочного шифрования, записывается как

$$C = eK(P),$$

где P — блок открытого текста;

C — блок шифротекста;

K — ключ.

Выражение eK является операцией шифрования, использующей ключ K.

Соответствующая функция дешифрования записывается как

$$P = dK(C).$$

Переменная, обозначенная заглавной буквой, как например вышеуказанными буквами P и C, представляет собой одномерный массив разрядов.

Например,

$$A = (a_1, a_2, \ldots, a_m) \text{ и } B = (b_1, b_2, \ldots, b_m)$$

представляют собой массивы m разрядов, пронумерованных от 1 до m. Все массивы разрядов записываются с наибольшего значащего разряда в левой позиции.

Операция сложения по модулю 2, известная также как функция «исключающее ИЛИ», представляется символом $\oplus$. Операция, относящаяся к массивам, например к A и B, определяется как

$$A \oplus B = (a_1 \oplus b_1, a_2 \oplus b_2, \ldots, a_m \oplus b_m).$$

Операция выбора совокупности j старших слева разрядов массива A, чтобы генерировать j-разрядный массив, записывается как

$$A \sim j = (a_1, a_2, \ldots, a_j).$$

Эта операция определена только для $j \leqslant m$, где m — число разрядов в массиве A.

«Функция сдвига» S_k определяется следующим образом.

Для заданных m-разрядной переменной X и k-разрядной переменной F, где $k \leqslant m$, действие функции сдвига $S_k\ (X|F)$ таково, что образует m-разрядную переменную

$$S_k\ (X|F) = (x_{k+1}, x_{k+2}, \ldots x_m, f_1, f_2, \ldots, f_k) \text{ при } k < m.$$

В результате происходят сдвиг разрядов массива X влево на k позиций с отбрасыванием $x_1, \ldots, x_k$ и размещение массива F на самых правых k позициях массива X. Если $k = m$, происходит полное замещение массива X на F.

Используется особый случай этой функции, в котором берется m-разрядная переменная $I(m)$ из последующих «1» битов и сдвигается переменной F из k разрядов, где $k \leqslant m$.

В результате:

$$S_k(I(m)\,|\,F) = (1, 1, \ldots, 1, f_1, f_2, \ldots, f_k) \text{ при } k < m;$$

$$S_k(I(m)\,|\,F) = (f_1, f_2, \ldots, f_k) \text{ при } k = m,$$

где m—k наиболее старших разрядов представляют собой «1».

4 РЕЖИМ ЭЛЕКТРОННОГО КОДОВОГО СПРАВОЧНИКА — ECB (ELECTRONIC CODEBOOK)

4.1 Переменные, используемые для режима шифрования ECB:

a) последовательность из q блоков открытого текста $P_1, P_2, \ldots, P_q$, каждый по n разрядов;

b) ключ K;

c) получающаяся в результате последовательность q блоков шифротекста $C_1, C_2, \ldots, C_q$, каждый по n разрядов.

4.2 Режим ECB при шифровании описывается следующим образом:

$$C_i = eK(P_i) \text{ для } i = 1, 2, \ldots, q. \qquad (1)$$

4.3 Режим ECB при дешифровании описывается следующим образом:

$$P_i = dK(C_i) \text{ для } i = 1, 2, \ldots, q. \qquad (2)$$

5 РЕЖИМ ПОСЛЕДОВАТЕЛЬНОГО БЛОЧНОГО ШИФРОВАНИЯ — CBC (CIPHER BLOCK CHAINING)

5.1 Переменные, используемые для режима CBC при шифровании:

a) последовательность q блоков открытого текста P_1, $P_2, \ldots,$ P_q, каждый по n разрядов;

b) ключ K;

c) запускающая переменная SV из n разрядов;

d) последовательность q блоков шифротекста $C_1, C_2, \ldots, C_q$, каждый по n разрядов.

5.2 Режим CBC при шифровании описывается следующим образом:

шифрование первого блока открытого текста

$$C_1 = eK(P_1 \oplus SV), \qquad (3)$$

далее

$$C_i = eK(P_i \oplus C_{i-1}) \text{ для } i = 2, 3, \ldots, q. \qquad (4)$$

Данная процедура показана в верхней части рисунка 1. Запускающая переменная SV используется для генерации первых выходных данных шифротекста. Затем шифротекст суммируется по модулю 2 к последующему открытому тексту перед шифрованием.

5.3 Режим CBC при дешифровании описывается следующим образом:

дешифрование первого зашифрованного блока

$$P_i = dK(C_i) \oplus SV, \qquad (5)$$

далее

$$P_i = dK(C_i) \oplus C_{i-1} \text{ для } i = 2, 3, \ldots, q. \qquad (6)$$

Эта процедура показана в нижней части рисунка 1.

6 РЕЖИМ ШИФРОВАНИЯ С ОБРАТНОЙ СВЯЗЬЮ — CFB (CIPHER FEEDBACK)

6.1 Работу режима CFB определяют два параметра:

— размер переменной обратной связи k, где $1 \leqslant k \leqslant n$;

— размер переменной открытого текста j, где $1 \leqslant j \leqslant k$.

Переменные, используемые при работе в режиме CFB, следующие:

a) входные переменные:

1) последовательность q переменных открытого текста P_1, $P_2, \ldots, P_q$, каждая по j разрядов;

2) ключ K;

3) запускающая переменная SV, имеющая n разрядов;

b) промежуточные результаты:

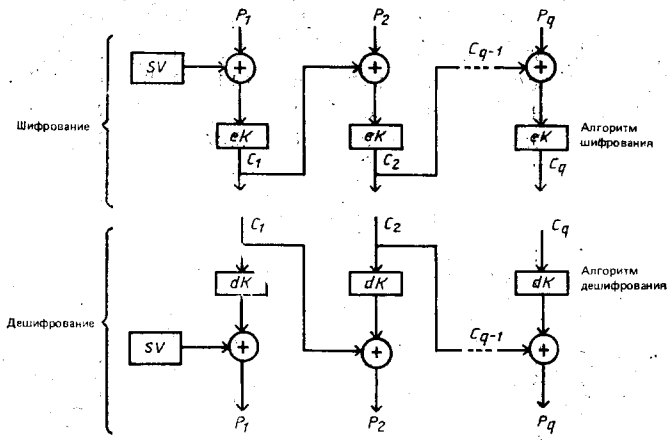

Рисунок 1 — Режим работы последовательного блочного шифрования (CBC)

1) последовательность q входных блоков алгоритма X_1, X_2, ..., X_q, каждый по n разрядов;
2) последовательность q выходных блоков алгоритма Y_1, Y_2, ..., Y_q, каждый по n разрядов;
3) последовательность q переменных E_1, E_2, ..., E_q, каждая по n разрядов;
4) последовательность $q-1$ переменных обратной связи F_1, F_2, ..., F_{q-1}, каждая по k разрядов;

c) выходные переменные, т. е. последовательность q переменных шифротекста C_1, C_2, ..., C_q, каждая по j разрядов.

6.2 Входной блок X представляет собой ряд его начальных значений

$$X_1 = SV. \tag{7}$$

Операция шифрования каждой переменной открытого текста включает в себя пять этапов:

a) использование алгоритма шифрования

$$Y_i = eK(X_i); \tag{8}$$

b) выбор старших слева j разрядов

$$E_i = Y_i \sim j; \tag{9}$$

c) формирование переменной шифротекста

$$C_i = P_i \oplus E_i; \tag{10}$$

d) формирование переменной обратной связи

$$F_i = S_i(I(k) \mid C_i); \tag{11}$$

e) функцию сдвига

$$X_{i+1}=S_k(X_i|F_i). \qquad (12)$$

Эти этапы повторяются для $i=1, 2, \ldots, q$, заканчиваясь уравнением (12) на последнем цикле. Процедура представлена на левой стороне рисунка 2. Старшие слева j битов выходного блока Y алгоритма шифрования используются для шифрования j-разрядной переменной открытого текста сложением по модулю 2. Оставшиеся разряды блока Y отбрасываются. Переменные открытого текста и шифротекста имеют разряды, пронумерованные от 1 до j.

Переменная шифротекста дополняется размещением $k—j$ битов «1» в позиции ее старших слева разрядов так, чтобы она стала k-разрядной переменной обратной связи F. Затем разряды входного блока X сдвигаются влево на k позиций и F вставляется в самые правые k позиций, чтобы образовать новое значение X. В этой операции сдвига самые левые k разрядов блока X отбрасываются.

6.3. Переменные, используемые для дешифрования, являются такими же, как и те, которые используются для шифрования. Входной блок X представляет собой начальные значения $X_i=SV$.

Операция дешифрования каждой переменной шифротекста включает в себя пять этапов:

a) использование алгоритма шифрования

$$Y_i=eK(X_i); \qquad (13)$$

b) выбор самых левых j разрядов

$$E_i=Y_i\sim j; \qquad (14)$$

c) формирование переменной открытого текста

$$P_i=C_i \oplus E_i; \qquad (15)$$

d) формирование переменной обратной связи

$$F_i=S_j(I(k)\,|\,C_i); \qquad (16)$$

e) функцию сдвига

$$X_{i+1}=S_k(X_i|F_i). \qquad (17)$$

Эти этапы повторяются для $i=1, 2, \ldots, q$, заканчиваясь уравнением (17) в последнем цикле. Процедура представлена в правой части рисунка 2. Самые левые j разрядов выходного блока Y алгоритма шифрования используются для дешифрования j-разрядной переменной шифротекста сложением по модулю 2. Оставшиеся разряды блока Y отбрасываются. Переменные открытого текста и шифротекста имеют разряды, пронумерованные от 1 до j.

Переменная шифротекста дополняется размещением $k—j$ битов «1» в позициях самых левых разрядов так, чтобы она стала k-разрядной переменной обратной связи F. Затем разряды входного блока X сдвигаются влево на k позиций и F вставляется в самые правые k позиций, чтобы образовать новое значение X. В этой операции сдвига самые левые k разрядов блока X отбрасываются.

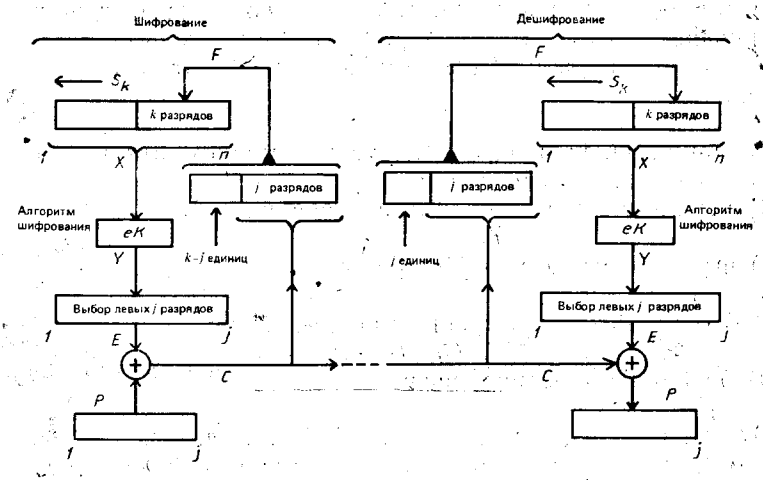

Рисунок 2 — Режим работы шифрования с обратной связью (CFB)

6.4 Рекомендуется, чтобы режим CFB использовался с равными значениями j и k. При этой рекомендации ($j=k$) уравнений (11) и (16) могут быть записаны в виде

$$F_i = C_i \qquad \text{(подставлено } j=k\text{)}.$$

7 РЕЖИМ С ОБРАТНОЙ СВЯЗЬЮ ПО ВЫХОДУ — OFB (OUTPUT FEEDBACK)

7.1 Режим работы OFB определяет один параметр, т. е. размер переменной открытого текста j, где $1 \leqslant j \leqslant n$.

Переменные, используемые при работе в режиме OFB:

a) входные переменные:

1) последовательность q переменных открытого текста P_1, $P_2, \ldots, P_q$, по j разрядов каждая;

2) ключ K;

3) запускающая переменная SV из n разрядов;

b) промежуточные результаты:

1) последовательность q входных блоков алгоритма X_1, X_2, $\ldots, X_q$, по n разрядов каждый;

2) последовательность q выходных блоков алгоритма Y_1, $Y_2, \ldots, Y_q$, по n разрядов каждый;

3) последовательность q переменных $E_1, E_2, \ldots, E_q$, по j разрядов каждая;

c) выходные переменные, т. е. последовательность q переменных шифротекста $C_1, C_2, \ldots, C_q$, по j разрядов каждая.

7.2. Входной блок X представляет собой ряд его начальных значений

$$X_i = SV. \tag{18}$$

Операция шифрования каждой переменной открытого текста включает в себя четыре этапа:

a) использование алгоритма шифрования

$$Y_i = eK(X_i); \tag{19}$$

b) выбор самых левых j разрядов

$$E_i = Y_i \sim j; \tag{20}$$

c) формирование переменных шифротекста

$$C_i = P_i \oplus E_i; \tag{21}$$

d) операцию обратной связи

$$X_{i+1} = Y_i. \tag{22}$$

Эти этапы повторяются для $i = 1, 2, \ldots, q$, заканчиваясь уравнением (21) на последнем цикле. Процедура показана в левой части рисунка 3. Результат каждого применения алгоритма шифрования, которым является блок Y_i, используется для обратной связи и становится следующим значением X_i, а именно X_{i+1}. Самые левые j разрядов в Y_i используются для шифрования входной переменной.

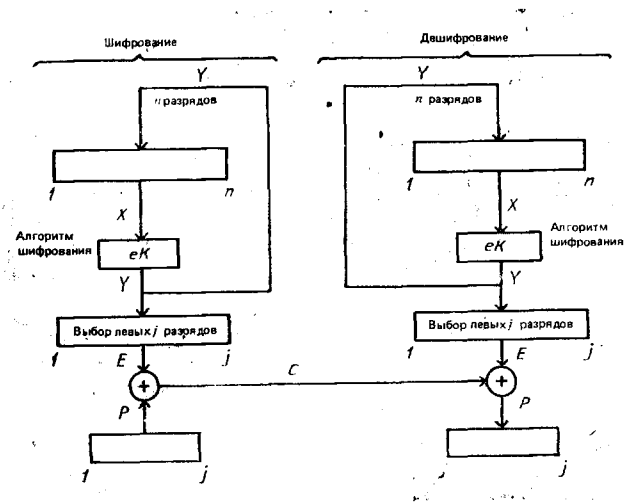

Рисунок 3 — Режим работы шифрования с обратной связью по выходу (OFB)

7.3. Переменные, используемые для дешифрования, являются такими же, как и используемые для шифрования. Входной блок X представляет собой ряд его начальных значений $X_i = SV$.

Операция дешифрования каждой переменной шифротекста включает в себя четыре этапа:

a) использование алгоритма шифрования

$$Y_i = eK(X_i); \quad (23)$$

b) выбор самых левых j разрядов

$$E_i = Y_i \sim j; \quad (24)$$

c) формирование переменной открытого текста

$$P_i = C_i \oplus E_i; \quad (25)$$

d) операцию обратной связи

$$X_{i+1} = Y_i. \quad (26)$$

Эти этапы повторяются для $i = 1, 2, \ldots, q$, заканчиваясь уравнением (26) на последнем цикле. Процедура представлена в правой части рисунка 3. Значения X_i и Y_i, используемые как для дешифрования, так и для шифрования, одинаковы; отличается только уравнение (25).

ПРИЛОЖЕНИЕ А

(информационное)

СВОЙСТВА РЕЖИМОВ РАБОТЫ

А.1 Свойства режима работы электронного кодового справочника (ECB)

А.1.1 Условия применения

Передаваемые блоки информации — это такой перенос информации между ЭВМ и людьми, который может иметь повторения или обычно используемые последовательности. В режиме ECB идентичный открытый текст синтезирует (при том же ключе) идентичные блоки шифротекста.

А.1.2 Характеристики режима ECB:

a) шифрование и дешифрование блоков могут осуществляться независимо от других блоков;

b) переупорядочение блоков шифротекста приведет к соответствующему переупорядочению блоков открытого текста;

c) тождественный блок открытого текста всегда породит тождественный блок шифротекста (при одном и том же ключе), делая его уязвимым к «словарной атаке».

Режим ECB обычно не рекомендуется для сообщений длиннее чем один блок. Применение режима ECB может в дальнейшем быть установлено в международных стандартах для таких специальных целей, когда повторение характеристик допустимо или блоки доступны индивидуально.

А.1.3 Требования к набивке

Только блоки по n разрядов могут быть зашифрованы и дешифрованы. Блоки другой длины должны быть дополнены до n-разрядного предела.

А.1.4 Распространение ошибки

В режиме ECB один или более ошибочных битов внутри отдельного блока шифротекста будут воздействовать только на дешифрование блока, в котором ошибка(ки) произошла(ли). При предположении, что шифр обладает свойством, при котором замена одного бита открытого текста вызывает в среднем 50 %-е изменение шифротекста, каждый бит восстановленной версии открытого текста этого блока будет иметь среднюю ошибку порядка 50 %.

А.1.5 Если границы блока утрачиваются между шифрованием и дешифрованием (например, обусловлены ошибкой бита), синхронизация между операциями шифрования и дешифрования будет утеряна до тех пор, пока не будут восстановлены правильные границы блока. Результат всех операций дешифрования будет неверным, пока границы блока утрачены.

А.2 Свойства режима работы последовательного блочного шифрования (CBC)

А.2.1 Условия применения

Режим CBC порождает тождественный шифротекст всякий раз, когда шифруется тождественный открытый текст с использованием тождественных ключа и запускающей переменной. Пользователям, которых интересует эта характеристика, необходимо знать, как следует заменять запуск открытого текста, ключа или запускающей переменной. Во-первых, это введение уникального идентификатора (например, счетчика прироста) в начало каждого передаваемого в режиме CBC блока информации. Во-вторых, для случая, когда шифруют записи, размеры которых не должны увеличиваться, — использование некоторой переменной, например запускающей переменной, которая может быть вычислена из записи без

знания ее компонентов (например, ее адреса в запоминающем устройстве с произвольной выборкой).

А.2.2 Свойства

Свойства режима CBC:

a) последующая операция делает блоки шифротекста зависимыми от текущего и всех предыдущих блоков открытого текста, и поэтому блоки не могут быть переставлены;

b) использование различных значений SV исключает шифрование тождественного открытого текста в тождественный шифротекст.

А.2.3 Требование к набивке

Только блоки по n разрядов могут быть зашифрованы и дешифрованы. Блоки другой длины должны быть дополнены до n-разрядного предела. Если это не допустимо, последняя переменная может обрабатываться специальным путем Два примера специальной обработки приведены ниже.

Первой возможностью обработать неполную последнюю переменную (т. е. переменную P_q при $j<n$ разрядов, где q должно быть больше 1) является шифрование в режиме OFB, как описано ниже:

a) шифрование

$$C_q = P_q \oplus (eK(C_{q-1}) \sim j); \qquad (27)$$

b) дешифрование

$$P_q = C_q \oplus (eK(C_{q-1}) \sim j). \qquad (28)$$

Тем не менее эта последняя переменная уязвима к «выбранной атаке открытого текста», если SV не является секретной или если она используется более одного раза с тождественным ключом (см. А.4).

Вторая возможность известна как «шифротекст—упрятывание». Допустим, что последние две переменные открытого текста представляют собой P_{q-1} и P_q, где P_{q-1} есть n-разрядный блок, P_q является переменной из $j<n$ разрядов и q должно быть больше 1.

a) Шифрование.

Пусть C_{q-1} является блоком шифротекста, получаемым из P_{q-1} с использованием метода, описанного в 5.2. В таком случае

$$C_q = eK(S_j(C_{q-1}|P_q). \qquad (29)$$

Последние две переменные шифротекста в таком случае представляют собой $C_{q-1} \sim j$ и C_q.

b) Дешифрование

C_q должна быть дешифрована первой, в результате чего она дает переменную P_q и самые правые $n-j$ разрядов C_{q-1}:

$$S_j(C_{q-1}|P_q) = dK(C_q). \qquad (30)$$

Законченный блок C_{q-1} теперь доступен, и P_{q-1} может быть получен с использованием метода, описанного в 5.3.

Две замыкающие переменные шифротекста дешифруются в обратном порядке, что делает это решение менее пригодным для аппаратной реализации.

А.2.4 Распространение ошибки

В режиме CBC один и более ошибочных разрядов внутри отдельного блока шифротекста будут влиять на дешифрование двух блоков (блока, в котором ошибка совершена, и последующего блока). Если ошибки есть в i-ом блоке шифротекста, каждый разряд i-го дешифрованного блока открытого текста будет иметь в среднем порядка 50 % ошибок при предположении, что шифр обладает таким свойством, при котором изменение одного разряда открытого текста приводит в среднем к 50 %-ному изменению в шифротексте. Дешифрованный $(i+1)$ блок открытого текста будет иметь только те разряды в ошибке, которые прямо зависят от разрядов шифротекста в ошибке. Если ошибки содержит переменная из менее чем n разрядов, распространение ошибки зависит от выбранного

метода специальной обработки. В первом примере дешифрованный короткий блок будет иметь те разряды в ошибке, которые прямо связаны с разрядами шифротекста в ошибке. Если ошибки есть в блоке, предшествующем блоку из менее чем n разрядов, дешифрованный короткий блок будет иметь среднее значение разрядов ошибки порядка 50 %. В шифротексте, имеющем случайные ошибки, короткий блок или последний блок шифротекста приводит к ошибочным разрядам порядка 50 %.

А.2.5 Границы блока

Если границы блока утрачиваются между шифрованием и дешифрованием (например, обусловлены ошибкой разряда), синхронизация между операциями шифрования и дешифрования будет утеряна до тех пор, пока не будут восстановлены правильные границы блока. Результат всех операций дешифрования будет неверным, пока границы блока утрачены.

А.3 Свойства режима работы шифрования с обратной связью (CFB)

А.3.1 Условия применения

Режим CFB порождает тождественный шифротекст всякий раз, когда шифруется тождественный открытый текст с использованием тождественных ключа и запускающей переменной. Пользователям, которых интересует эта характеристика, необходимо знать, как заменить запуск открытого текста, ключ или запускающую переменную. Во-первых, это введение уникального идентификатора (например, счетчика прироста) в начало каждого передаваемого в режиме CFB блока информации. Во-вторых, в случае, когда шифруют записи, размеры которых не должны увеличиваться, — использование некоторой переменной, например запускающей переменной, которая может быть вычислена из записи без знания ее компонентов (например, ее адреса в запоминающем устройстве с произвольной выборкой).

А.3.2 Свойства

Свойства режима CFB:

a) последующая операция делает переменные шифротекста зависимыми от текущей и всех предыдущих переменных открытого текста, и поэтому j-разрядные переменные связаны вместе и не могут быть переставлены;

b) использование различных значений SV делает невозможным шифрование тождественного открытого текста в тождественный шифротекст;

c) оба процесса шифрования и дешифрования в режиме CFB используют формулу шифрования алгоритма;

d) мощность режима CFB зависит от размера k (максимальна, если $j=k$);

e) выбор малого значения j будет требовать больше циклов на единицу открытого текста из-за алгоритма шифрования и, таким образом, вызовет большие непроизводительные издержки процесса.

А.3.3 Требования к набивке

Только блоки по j разрядов могут быть зашифрованы и дешифрованы. Блоки другой длины должны быть дополнены до j-разрядного предела. Тем не менее, в большинстве применений j следует выбирать равным размеру символа и набивка не потребуется.

А.3.4 Распространение ошибки

В режиме CFB ошибки в любом j-разрядном элементе шифротекста будут влиять на дешифрование следующего шифротекста до тех пор, пока биты в ошибке будут сдвигаться без сохранения выдвигаемых разрядов входного блока режима CFB. Первый подверженный влиянию j-разрядный элемент открытого текста будет искажен именно в тех местах, где в шифротексте имеется ошибка. При предположении, что шифр обладает свойством, при котором изменение одного бита открытого текста вызывает в среднем 50 %-е изменение в шифротексте, в последующем дешифрованном открытом тексте каждый разряд будет

иметь среднюю ошибку порядка 50 % до тех пор, пока все ошибки будут сдвигаться без сохранения выдвигаемых разрядов входного блока.

А.3.5 Границы блока

Если j-разрядные границы утеряны между шифрованием и дешифрованием (например, обусловлены ошибкой разряда), криптографическая синхронизация будет восстановлена до n разрядов после того, как восстановятся j-разрядные границы. Если блок из j разрядов утерян, синхронизация будет восстановлена автоматически после обработки n разрядов.

А.4 Свойства режима работы с обратной связью по выходу (OFB)

А.4.1 Условия применения

Режим OFB порождает тождественный шифротекст всякий раз, когда шифруется тождественный открытый текст с использованием тождественных ключа и запускающей переменной. Кроме того, в режиме OFB порождается тождественный поток ключей, когда используются тождественные ключ и *SV*. Следовательно, из соображений секретности специальная *SV* должна быть использована только один раз для заданного ключа.

А.4.2 Свойства

Свойства режима OFB:

a) отсутствие связанности делает режим OFB более уязвимым к специальным атакам;

b) использование различных значений *SV*, порождая различные потоки ключей, препятствует шифрованию тождественного открытого текста в тождественный шифротекст;

c) обе процедуры шифрования и дешифрования в режиме OFB используют формулу шифрования алгоритма;

d) режим OFB не зависит от открытого текста при генерации потока ключей, используемых для сложения по модулю 2 к открытому тексту;

e) выбор малого значения j будет требовать больше циклов на единицу открытого текста из-за алгоритма шифрования и, таким образом, вызовет большие непроизводительные издержки процесса.

А.4.3 Требования к набивке

Только блоки по j разрядов могут быть зашифрованы и дешифрованы. Блоки другой длины должны быть дополнены до j-разрядного предела. Тем не менее, в большинстве применений j следует выбирать равным размеру символа и набивка не потребуется.

А.4.4 Распространение ошибки

Режим OFB не расширяет ошибки шифротекста на выходе результирующего открытого текста. Каждый бит в ошибке шифротекста вызывает только один бит, который будет ошибочным в дешифрованном открытом тексте.

А.4.5 Границы блока

Режим OFB не является самосинхронизирующимся. Если две операции шифрования и дешифрования выходят из синхронизации, система нуждается в приведении в исходное состояние (реинициализации). Такая потеря синхронизации может быть (если $j>1$) из-за потери правильных границ блоков по j разрядов (например, обусловлена ошибкой разряда).

Каждое восстановление исходного состояния должно использовать значение *SV*, отличное от значений *SV*, использованных до этого с тождественным ключом. Основанием для этого является то, что для тождественных параметров всякий раз должен порождаться идентичный поток разрядов. Указанные условия делают режим OFB уязвимым к «известной атаке открытого текста».

ПРИЛОЖЕНИЕ В

(информационное)

ИНФОРМАЦИЯ О ПАТЕНТАХ

В процессе подготовки международного стандарта ИСО/МЭК 10116 была собрана информация о патентах, от которых может зависеть применение данного стандарта. Было выявлено, что такие патенты принадлежат корпорациям IBM и UNISYS.

Однако Международная организация по стандартизации — ISO (International Organization for Standardization) не может дать авторитетной или исчерпывающей информации об очевидности, обоснованности или области распространения патентов или подобных прав.

Владельцы патентов приняли положение, по которому в оговоренные периоды лицензии будут допускать предоставление права применения данного международного стандарта при условии, что те, кто желает получить лицензии, согласны отвечать взаимностью.

Дополнительная информация имеется в распоряжении фирм:

Director of Commercial Relations
International Business Machines Corporation (IBM)
2000 Purchase Street
PURCHASE, N. Y. 10577

Director, Industry Relations
UNISYS
PO Box 500
Blue Bell, PA 19424
U. S. A.

ПРИЛОЖЕНИЕ С

(информационное)

ПРИМЕРЫ ДЛЯ РЕЖИМОВ РАБОТЫ

С.1 Общие сведения

В этом приложении приведены примеры для шифрования и дешифрования передаваемых блоков информации с использованием режимов работы, установленных в настоящем стандарте. Используемые параметры:

a) алгоритм шифрования — алгоритм шифрования данных (DEA — Data Encryption Algoritm). Значение n — 64;

b) криптографический ключ — 0123456789ABCDEF;

c) запускающая переменная — 1234567890ABCDEF;

d) открытый текст — 7-битный код ASCII (американский стандартный код для обмена информацией) для слов «Now is the time for all» (в шестнадцатеричном представлении 4E6F772069732074 68652074696D6520 666F72206C6C20). Для режима CFB открытый текст — 7-битный код ASCII для слова «Now» (в шестнадцатеричном представлении 4E6F77).

С.2 Режим ECB

Примеры шифрования и дешифрования в режиме ECB даны в таблицах С.1 и С.2 соответственно.

Таблица С.1 — **Режим ECB, шифрование**

i	Открытый текст P_i	Входной блок алгоритма	Выходной блок алгоритма	Шифротекст C_i
1	4E6F772069732074	4E6F772069732074	3FA40E8A984D4815	3FA40E8A984D4815
2	68652074696D6520	68652074696D6520	6A271787AB8883F9	6A271787AB8883F9
3	666F7220616C6C20	666F7220616C6C20	893D51EC4B563B53	893D51EC48563B53

Таблица С.2 — **Режим ECB, дешифрование**

i	Шифротекст P_i	Входной блок алгоритма	Выходной блок алгоритма	Открытый текст C_i
1	3FA40E8A984D4815	3FA40E8A984D4815	4E6F772069732074	4E6F772069732074
2	6A271787AB8883F9	6A271787AB8883F9	68652074696D6520	68652074696D6520
3	893D51EC48563B53	893D51EC4B563B53	666F7220616C6C20	666F7220616C6C20

С.3 Режим CBC

Примеры шифрования и дешифрования в режиме CBC даны в таблицах С.3 и С.4 соответственно.

Таблица С.3 — **Режим CBC, шифрование**

i	Открытый текст P_i	Входной блок алгоритма	Выходной блок алгоритма	Шифротекст C_i
1	4E6F772069732074	5C5B2158F9D8ED9B	E5C7CDDE872BF27C	E5C7CDDE872BF27C
2	68652074696D6520	8DA2EDAAEE46975C	43E934008C389C0F	43E934008C389C0F
3	666F7220616C6C20	25864620ED54F02F	683788499A7C05F6	683788499A7C05F6

Таблица С.4 — **Режим CBC, дешифрование**

i	Шифротекст P_i	Входной блок алгоритма	Выходной блок алгоритма	Открытый текст C_i
1	E5C7CDDE872BF27C	E5C7CDDE872BF27C	5C5B2158F9D8ED9B	4E6F772069732074
2	43E934008C389C0F	43E934008C389C0F	8DA2EDAAEE46975C	68652074696D6520
3	683788499A7C05F6	683788499A7C05F6	25864620ED54F02F	666F7220616C6C20

С.4 Режим CFB

Примеры шифрования и дешифрования в режиме CFB даны в таблицах С.5 и С.6 соответственно. Для этих примеров выбраны параметры $j=k=8$; k разрядов обратной связи показаны наклонным (курсивным) шрифтом.

Таблица С.5 — **Режим CFB, шифрование**

i	Открытый текст P_i	Входной блок алгоритма	Выходной блок алгоритма	Шифротекст C_i
1	4E	1234567880ABCDEF	BD661569AE874E25	F3
2	6E	34567890ABCDEF*F3*	7039546F9A0F6330	1F
3	**77**	567890ABCDEFF3*1F*	AD1B78B0BB371BE7	DA

Таблица С.6 — **Режим CFB, дешифрование**

i	Шифротекст P_i	Входной блок алгоритма	Выходной блок алгоритма	Открытый текст C_i
1	F3	1234567890ABCDEF	BD661569AE874E25	4E
2	1F	34567890ABCDEF*F3*	7039546F9A0F6330	6E
3	DA	567890ABCDEFF3*1F*	AD1B78B0BB371BE7	77

С.5 Режим OFB

Примеры шифрования и дешифрования в режиме OFB даны в таблицах С.7 и С.8 соответственно. Для этих примеров выбран параметр $j=64$.

Таблица С.7 — **Режим OFB, шифрование**

i	Открытый текст P_i	Входной блок алгоритма	Выходной блок алгоритма	Шифротекст C_i
1	4E6F772069732074	1234567890ABCDEF	BD661569AE874E25	F3096249C7F46E51
2	68652074696D6520	BD661569AE874E25	5D976A504786581F	35F24A242EEB3D3F
3	666F7220616C6C20	5D976A504786581F	5B0229C3443694E3	3D6D5BE3255AF8C3

Таблица С.8 — **Режим OFB, дешифрование**

i	Шифротекст P_i	Входной блок алгоритма	Выходной блок алгоритма	Открытый текст C_i
1	F3096249C7F46E51	1234567890ABCDEF	BD661569AE874E25	4E6F772069732074
2	35F24A242EEB3D3F	BD661569AE874E25	5D976A504786581F	68652074696D6520
3	3D6D5BE3255AF8C3	5D976A504786581F	5B0229C3443694E3	666F7220616C6C20

УДК 681.33:006.354 П85

Ключевые слова: информационная технология, режим работы, алгоритм *n*-разрядного блочного шифрования, алгоритм шифрования, защита передачи данных, хранение данных, подтверждение подлинности, режим работы с обратной связью, режим работы с обратной связью по выходу, открытый текст, шифротекст, связывание блоков, запускающая переменная, криптографическая синхронизация

ОКСТУ 4002

Редактор *Л. В. Афанасенко*
Технический редактор *О. Н. Никитина*
Корректор *Т. А. Васильева*

Сдано в наб. 04.02.94. Подп. в печ. 06.04.94. Усл. п. л. 1,40. Усл. кр.-отт 1,40. Уч.-изд. л. 1,20. Тир. 411 экз. С 1167.

Ордена «Знак Почета» Издательство стандартов, 107076, Москва, Колодезный пер., 14.
Калужская типография стандартов, ул. Московская, 256. Зак. 296