ISSN 1563-0285 • Индекс 75872; 25872

25 жыл
Қазақстан

ӘЛ-ФАРАБИ атындағы ҚАЗАҚ ҰЛТТЫҚ УНИВЕРСИТЕТІ
КАЗАХСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ имени АЛЬ-ФАРАБИ
AL-FARABI KAZAKH NATIONAL UNIVERSITY

ХАБАРШЫ

МАТЕМАТИКА, МЕХАНИКА, ИНФОРМАТИКА СЕРИЯСЫ

ВЕСТНИК

СЕРИЯ МАТЕМАТИКА, МЕХАНИКА, ИНФОРМАТИКА

BULLETIN

MATHEMATICS, MECHANICS, COMPUTER SCIENCE SERIES

3/1(90) 2016

ISSN 1563 – 0285
Индекс 75872; 25872

ӘЛ-ФАРАБИ атындағы ҚАЗАҚ ҰЛТТЫҚ УНИВЕРСИТЕТІ

ҚазҰУ ХАБАРШЫСЫ

Математика, механика, информатика сериясы

Арнайы шығарылым

КАЗАХСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ имени АЛЬ-ФАРАБИ

ВЕСТНИК КазНУ

Серия математика, механика, информатика

Специальный выпуск

AL-FARABI KAZAKH NATIONAL UNIVERSITY

KazNU BULLETIN

Mathematics, Mechanics, Computer Science Series

Special issue

№3/1(90)

Алматы
«Қазақ университеті»
2016

МАЗМҰНЫ - СОДЕРЖАНИЕ

УДК 004.056.5

Калимолдаев М.Н., Кабылханов А.Б., Магзом М.М.*, Нысанбаева С.Е.

Институт информационных и вычислительных технологий КН МОН РК,
Республика Казахстан, г. Алматы
* E-mail: magzomxzn@gmail.com

Построение модели режима для системы шифрования, разработанной на базе модулярной арифметики

В данной работе предлагается алгоритм криптографического преобразования для системы блочного симметричного шифрования, разработанной на базе непозиционной полиномиальной системы счисления (НПСС). Цель создания этой модели режима – повысить уровень статистической безопасности системы шифрования на базе НПСС. При создании алгоритма криптографического преобразования используется модель режима шифра. Эта модель режима разработана с применением сети Фейстеля и режима стандарта шифрования США. Использованный режим - это режим сцепления блоков по шифртексту для блочных алгоритмов шифрования (на языке оригинала: CBC - Cipher block chaining). Данный режим рекомендован НИСТ США (NIST - The National Institute of Standards and Technology). В связи с этим приведены краткие описания сети Фейстеля, режима сцепления блоков по шифртексту, блочного симметричного алгоритма шифрования на базе НПСС. Приведены полученные результаты проведенных исследований: изложена суть разработанной модели режима для системы шифрования на базе НПСС; приведена блок-схема предложенного алгоритма криптографического преобразования. Для указанных результатов будут проведены работы по анализу статистических свойств получаемых криптограмм с использованием графических и оценочных тестов.
Ключевые слова: криптографическая система, алгоритм шифрования, модулярная арифметика, сеть Фейстеля, режимы шифрования.

Kalmoldayev M.N., Kabylkhanov A.B., Magzom M.M., Nyssabayeva S.E.

Construction of the model of application mode for encryption system developed on the basis of modular arithmetic

In this work, we propose an algorithm for cryptographic transformation for the block symmetric encryption system, developed on the basis of nonpositional polynomial notation system (NPNs). The purpose of this mode model is to increase the level of statistical security of the encryption system based on NPNs. During the creation of the algorithm of cryptographic transformation, the model of the cipher mode is used. This mode model was developed using a Feistel network and the mode of US encryption standard. Used mode is the cipher block chaining mode for block encryption algorithms. This mode is recommended by NIST of USA. In this regard brief descriptions of the Feistel network, cipher block chaining mode and block symmetric encryption algorithm based on NPNs are provided. The results of the research is presented: outlined the essence of the developed mode model for the encryption system based on NPNs; a block diagram of the proposed algorithm of the cryptographic transformation is introduced. Work on the analysis of the statistical properties of the resulting cryptograms will be held for these results using graphical and assessment tests.
Key words: cryptosystems, encryption, block cipher, nonpositional polynomial notation, cryptostrength, Feistel network, cipher mode.

Калимолдаев М.Н., Кабылханов А.Б., Магзом М.М., Нысанбаева С.Е.

Модулярлы арифметика негізінде жасалған шифрлау жүйесіне арналған режим моделін құрастыру

Бұл жұмыста позициондық емес полиномиалдық санау жүйелері (ПЕПСЖ) негізінде іске асырылған симметриялық блоктық шифрлау жүйесі алгоритміне арналған криптографиялық түрлендіру алгоритмі ұсынылып отыр. Режим моделінің құрастыру мақсаты - ол ПЕПСЖ негізіндегі шифрлау жүйесінің статистикалық қауіпсіздігінің деңгейін арттыру. Криптографиялық түрлендіру алгоритмін жасау барысында шифрлау режим моделі қолданылады. Бұл режим моделі АҚШ шифрлау стандартының режимі мен Фейстел желісін қолдану арқылы іске асырылған. қолданылған режим - бұл блоктық шифрлау алгоритмдеріне арналған шифрмәтін бойынша блоктардың тұтасу режимі (түпнұсқа тілінде CBC - Cipher block chaining). Бұл режим АҚШ ҰИСТ (NIST - The National Institute of Standards and Technology) ұсынылған. Осыған байланысты: Фейстел желісі, шифртмәтін бойынша блоктардың тұтасу режимі мен ПЕПСЖ негізіндегі блоктық шифрлау жүйесі алгоритміне қысқаша сипаттаулар келтірілген. қарастырылған зерттеулерден алынған нәтижелері келтірілген: ПЕПСЖ негізіндегі шифрлау жүйесіне арналған режим моделін құрастыру негізі сипатталған; ұсынылған криптографиялық түрлендіру алгоритмінің блок-схемасы келтірілген. Көрсетілген нәтижелерге алынған криптограммалардың статистикалық қасиеттеріне бағалық және графикалық тесттер арқылы сынақтамалар өткізіледі.

Түйін сөздер:криптографическлық жүйе, шифрлау алгоритмі, модулярлы арифметика, Фейстель желісі, шифрлау режимдері.

1. Введение

Одним из основных примеров при разработке блочных алгоритмов криптографического преобразования является многократная, состоящая из нескольких циклов, обработка одного блока открытого текста. На каждом цикле данные подвергаются специальному преобразованию при участии вспомогательного ключа, полученного из заданного секретного ключа. Выбор числа циклов определяется требованием криптостойкости и эффективности реализации блочного шифра. Как правило, чем больше циклов, тем выше криптостойкость и ниже эффективность реализации (больше задержка при зашифровании/расшифровании) блочного шифра, и наоборот. Так, например, в случае алгоритма DES для того, чтобы все биты шифртекста зависели от всех битов ключа и всех битов открытого текста, необходимо пять циклов криптографического преобразования. DES с шестнадцатью циклами обладает более высокой криптостойкостью по отношению к ряду криптоаналитических атак [1].

Существуют разные виды построения блочных алгоритмов шифрования. Один из них строятся на основе схемы Фейстеля. К числу таких алгоритмов относятся бывший американский стандарт Data Encryption Standard (DES) и российский стандарт России - ГОСТ 28147-89 [2]. В 1971 г. Хорст Фейстель (Horst Feistel) запатентовал два устройства, реализовавшие различные алгоритмы шифрования, названные затем общим названием «Люцифер» (Lucifer) [3]. Одно из устройств использовало конструкцию, впоследствии названную «сетью Фейстеля» («Feistel cipher», «Feistel network»). Проект «Люцифер» был скорее экспериментальным, но стал базисом для алгоритма стандарта (DES). В 1977 г. DES стал стандартом США для шифрования данных.

В 2002 г. принят новый американский стандарт Advanced Encryption Standard (AES), который относят к нетрадиционным, поскольку при его разработке был использован алгебраический подход.

В данной работе описывается модель режима шифра, которая построена на совместном использовании режима работы стандарта DES «Режим сцепления блоков по шифртексту» и сети Фейстеля. Затем эта модель применяется к системе шифрования, разработанной на базе НПСС. Систему шифрования на базе НПСС можно отнести к системам со специально разработанными алгоритмами, т.е. к нетрадиционным, поскольку он разработан на основе алгебраического подхода с использованием полиномиальных систем счисления в остаточных классах. Нетрадиционные методы и алгоритмы криптографии, построенные на базе НПСС, позволяют существенно повысить надежность алгоритма шифрования. Криптостойкость в этом случае определяется полным ключом, зависящим не только от длины ключа (ключевой последовательности), но и от выбранной системы полиномиальных оснований, а также от количества перестановок оснований в системе. Синонимами НПСС являются системы счисления в остаточных классах с полиномиальными основаниями или модулярная арифметика [4-6].

Описание режима стандарта шифрования DES «Режим сцепления блоков по шифртексту» приводится на основании документа, изданного Американским Национальным Институтом Стандартов и Технологий (НИСТ).

Сеть Фейстеля имеет следующую структуру [3]. Алгоритм шифрования реализуется несколькими раундами (или итерациями). Преобразование в сети Фейстеля на каждом раунде осуществляется следующим образом. Шифруемый блок разбивается на два равные подблока - H_i (верхний, high) и L_i (нижний, low). К нижнему подблоку применяется функция шифрования f с использованием ключевого элемента k_i (части ключа или модификации части ключа). После этого выполняется сложение результата модификации нижнего подблока с верхним подблоком по модулю два. В результате шифруемым блоком для следующего раунда будет объединение подблоков, полученных по формулам

$$H_{(i+1)} = L_i, \tag{1}$$

$$L_{(i+1)} = H_{(i+1)} \oplus f(L_i, H_i). \tag{2}$$

Схема каждого раунда показана на рисунке 1.

Шифрование при помощи данной конструкции легко реализуется как на программном уровне, так и на аппаратном, что обеспечивает широкие возможности применения. На основе сетей Фейстеля разработано большое количество шифров, среди которых: DES, ГОСТ 28147-89, Blowfish, CAST, FEAL, IDEA, Khufu, Twofish и другие.

DES - федеральный стандарт шифрования США в 1977-2001 гг. [1] для использования во всех несекретных правительственных каналах связи (FIPS PUB 46 «Data Encryption Standard»). Несмотря на то, что в настоящий момент федеральным стандартом шифрования США является алгоритм Rijndael (AES - Advanced Encryption Standard), рассмотрение DES позволяет понять основные принципы блочного шифрования [7-8].

DES является классической сетью Фейстеля с двумя ветвями (подблоками). Данные шифруются 64-битными блоками, используя 56-битный ключ. Алгоритм преобразует за несколько раундов 64-битный вход в 64-битный выход. Длина ключа равна 56 битам. Первоначально ключ подается на вход функции перестановки. Затем для каждого из 16 раундов подключ K_i является комбинацией левого циклического сдвига и перестановки. Функция перестановки одна и та же для каждого раунда, но подключи K_i для каждого раунда получаются разные вследствие повторяющегося сдвига битов ключа [1].

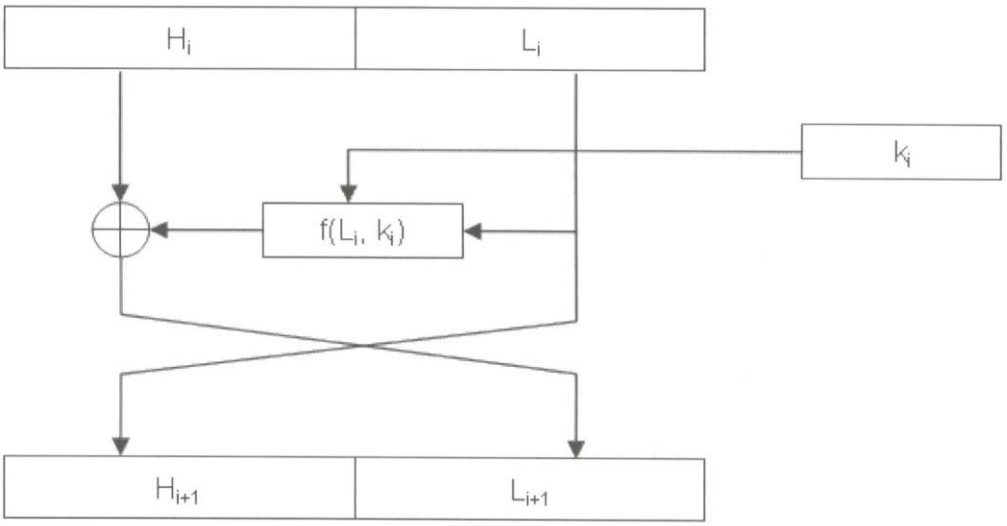

Рисунок 1 – Схема выполнения одного раунда в сети Фейстеля

2. Построение непозиционной полиномиальной системы счисления

Построение непозиционных полиномиальных систем счисления основано на использовании китайской теоремы об остатках, доказанной в I веке китайским математиком Сун Це. Свое развитие они начали после выхода в свет в 1955 году первых работ чешских исследователей - инженера М. Валаха и математика А. Свободы, которые предложили использовать систему остаточных классов для операций над компьютерными числами [9,10].

В 1955 году исследования в этой области были начаты также в СССР и получили широкое развитие благодаря трудам И.Я. Акушского, Д.И. Юдицкого, В.М. Амербаева [11]. Эта идея привлекла внимание ученых и в других странах. В результате возникло новое научное направление - модулярная арифметика. Одним из направлений развития модулярной арифметики являются работы Р.Г. Бияшева по созданию, анализу и использованию НПСС для разработки самокорректирующихся кодов, применяемых для обнаружения и исправления ошибок [6]. Им были обоснованы основные положения алгебры НПСС, которые использованы при разработке симметричной блочной системы шифрования.

2. Модель нетрадиционного алгоритма шифрования

Суть нетрадиционного алгоритма шифрования электронного сообщения заданной длины N состоит в следующем.

Вначале формируется НПСС. Пусть основаниями НПСС выбраны неприводимые многочлены с двоичными коэффициентами

$$p_1(x), p_2(x), ..., p_S(x). \tag{3}$$

степени $m_1(x), m_2(x), ..., m_s(x)$ соответственно. С учетом всех возможных их перестановок (расположений) эти полиномы образуют систему оснований НПСС. Основания

(3) задают основной (рабочий) диапазон НПСС, который определяется многочленом $P(x) = p_1(x)p_2(x) \cdots p_S(x)$ степени $m = \sum_{i=1}^{s} m_i$. В данной системе оснований любой многочлен, степень которого меньше m, имеет единственное представление в виде его остатков (вычетов) по модулям рабочих оснований $p_1(x), p_2(x), ..., p_S(x)$ соответственно.

Тогда сообщение длины N бит можно интерпретировать как последовательность остатков $\alpha_1(x), \alpha_2(x), ..., \alpha_S(x)$ от деления некоторого многочлена $F(x)$ на основания $p_1(x), p_2(x), ..., p_S(x)$ соответственно:

$$F(x) = (\alpha_1(x), \alpha_2(x), ..., \alpha_S(x)), \tag{4}$$

где $F(x) \equiv \alpha_i(x)(mod\ p_i(x)), i = \overline{1, \mathrm{S}}$. Запись $F(x)$ в виде (4) - это позиционное представления многочлена $F(x)$.

В выражении (4) остатки $\alpha_1(x), \alpha_2(x), ..., \alpha_S(x)$ выбираются таким образом, что первым l_1 битам сообщения ставятся в соответствие двоичные коэффициенты остатка $\alpha_1(x)$, следующим l_2 битам - двоичные коэффициенты остатка $\alpha_2(x)$ и так далее, последним l_s двоичным разрядам ставятся в соответствие двоичные коэффициенты вычета $\alpha_S(x)$.

Восстановление позиционного представления $F(x)$ производится по его непозиционному виду (4). В случае хранения, передачи и обработки информации оно осуществляется по следующей формуле:

$$F(x) = \sum_{i=1}^{S} \alpha_i(x) B_i(x), B_i(x) = \frac{\prod_{i=1}^{S} p_i(x)}{p_i(x)} M_i(x) \equiv 1(mod p_i(x)), \tag{5}$$

где $i = \overline{1, \mathrm{S}}$ и значения многочленов $M_i(x)$ выбираются для выполнения указанного в формуле сравнения.

Затем производится генерация ключевой (псевдослучайной) последовательности. Используемая ключевая последовательность длины N бит также интерпретируется как последовательность остатков $\beta_1(x), \beta_2(x), ..., \beta_S(x)$, но от деления некоторого другого многочлена $G(x)$ по тем же рабочим основаниям системы:

$$G(x) = (\beta_1(x), \beta_2(x), ..., \beta_S(x)), \tag{6}$$

где $G(x) \equiv \beta_i(x)(mod\ p_i(x)), i = \overline{1, \mathrm{S}}$.

Тогда в качестве криптограммы (шифртекста) $\omega_1(x), \omega_2(x), ..., \omega_S(x)$ может рассматриваться некоторая функция $H(F(x), G(x))$:

$$H(x) = (\omega_1(x), \omega_2(x), ..., \omega_S(x)), \tag{7}$$

где $H(x) \equiv \omega_i(x)(mod\ p_i(x)), i = \overline{1, \mathrm{S}}$.

В соответствии с операциями непозиционной системы счисления операции в функциях $F(x), G(x), H(x)$ могут выполняться параллельно по модулям полиномов $p_1(x), p_2(x), ...$, выбранных в качестве оснований НПСС.

Секретность нетрадиционного шифрования сообщения заданной длины N определяется не только многочленом (ключом) $G(x)$, но конкретным набором оснований, выбранных из всего множества неприводимых многочленов степени не выше N. Эти секретные составляющие (3) и (7) назвали полным секретным ключом.

Конкретная система оснований НПСС находится он следующим образом.

Пусть n_1 - число неприводимых многочленов с двоичными коэффициентами степени m_1. Тогда полные системы вычетов по модулям этих многочленов содержат все многочлены с двоичными коэффициентами степени не выше $m_1 - 1$, для записи которых используется m_1 бит. Пусть соответственно n_2 - число неприводимых многочленов с двоичными коэффициентами степени m_2, n_3 - число неприводимых многочленов с двоичными коэффициентами степени m_3 и т.д., n_S - число неприводимых многочленов степени m_S. При $S = N$ (степень оснований равна значению N) для записи полных систем вычетов по модулям этих оснований необходимо N бит.

Тогда процедура выбора всех систем рабочих оснований степени от m_1 до m_S сводится к нахождению всевозможных решений алгебраического уравнения

$$k_1 m_1 + k_2 m_2 + ... + k_S m_S = N \tag{8}$$

где $0 \le k_i \le n_i$ - неизвестные коэффициенты, один конкретный набор которых является одним из решений (8) и задает одну систему рабочих оснований; n_i - количество всех неприводимых многочленов степени m_i, $1 \le m_i \le N$, k_i- число выбранных неприводимых многочленов степени m_i, $S = k_1 + k_2 + .. + k_s$ - число выбранных оснований. Уравнение (5) определяет то количество S оснований, вычеты по которым покрывают длину N заданного сообщения. Полные системы вычетов по модулям многочленов степени m_i включают в себя все полиномы степени не выше $m_i - 1$, поэтому для их записи потребуется m_i бит. Выбираются же эти S оснований из общего количества всех неприводимых многочленов различных степеней, но не выше N. Все выбираемые основания должны отличаться друг от друга, даже если они являются неприводимыми полиномами одной степени, поскольку теория НПСС построена на выполнении китайской теоремы об остатках.

3. Моделирование режима шифрования

При шифровании исходного текста произвольной длины блочные шифры используются в различных криптографических режимах. Криптографический режим определяет подробности реализации алгоритма шифрования для различных применений и является методом использования блочного алгоритма шифрования, позволяющий преобразовать последовательность блоков в открытых данных в последовательность блоков зашифрованных данных [12-15].

В 1980 г. в США был принят также стандарт, который определил режимы работы алгоритма DES. Этот стандарт уточнял подробности реализации DES для различных применений (или применения DES в различных приложениях) [1]. Эти режимы обеспечивают требуемые свойства блочных шифрованных текстов, такие как контроль за распространением ошибок, случайность - должна быть скрыта структура открытого текста.

В режиме шифрования CBC (Cipher Block Chaining) происходит «сцепливание» всех блоков сообщения по шифртексту (рисунок 2). При зашифровании первого блока исходного текста в этом «Режиме сцепления блоков по шифртексту» используется специальный входной блок - «вектор инициализации». Вектор инициализации должен быть случайным и в каждом сеансе шифрования быть новой. В процессе шифрования тогда все блоки открытого текста оказываются связанными, а входные данные, поступающие на вход функции шифрования, уже зависят не только от текущего блока шифруемого открытого текста. По этой причине повторяющиеся блоки последовательности в шифрованном тексте не встречаются, а одно и тоже открытое сообщение в разных сеансах шифрования будет переходить в разные шифртексты. При расшифровании если внести искажения в зашифрованный блок, то после расшифрования искаженными окажутся два блока открытых данных - соответствующий и следующий за ним, причем искажения в первом случае будут носить тот же характер, что и в режиме гаммирования, а во втором случае - как в режиме простой замены.

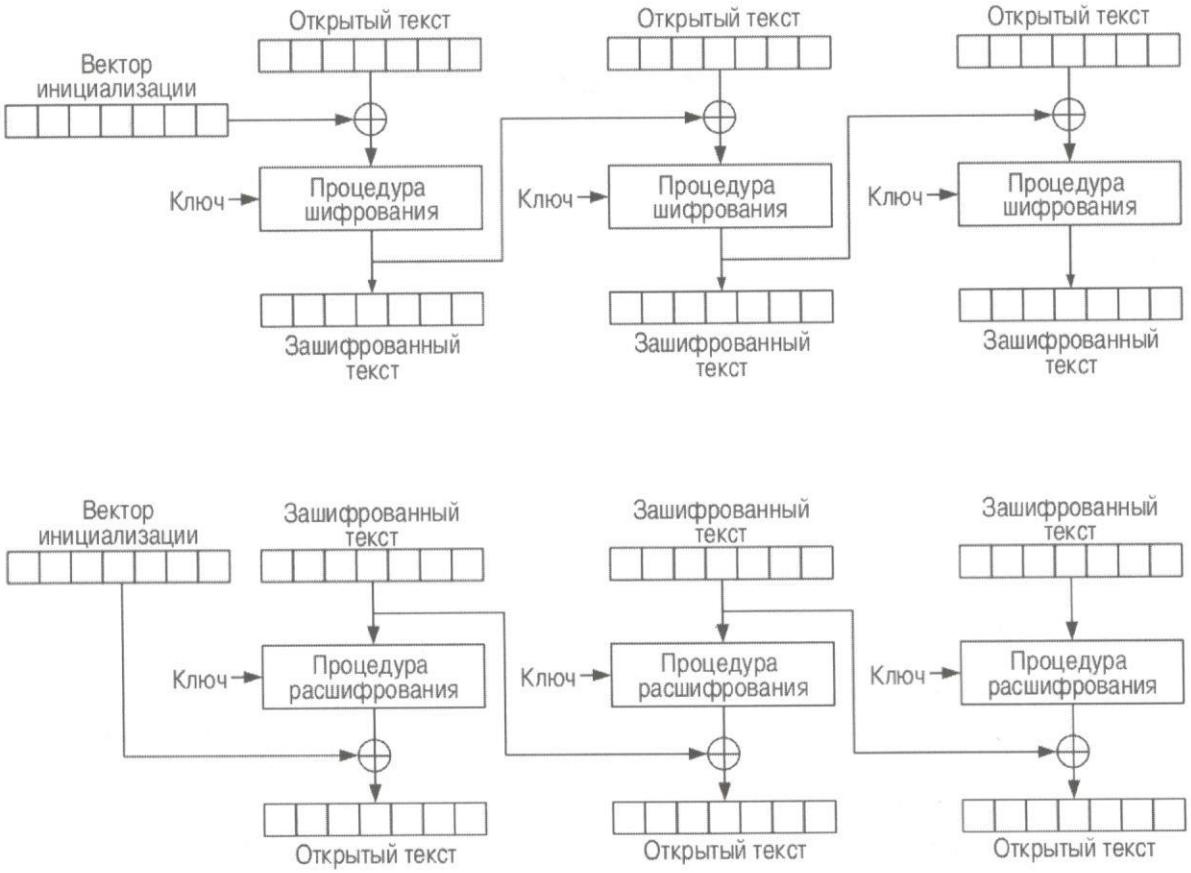

Рисунок 2 – Режим сцепления блоков по шифртексту: а) алгоритм зашифрования, б) алгоритм расшифрования

Как видно из рисунка в алгоритме шифрования на вход функции шифрования $CIPH_K$ (на рисунке 2,а – Процедура шифрования) каждый раз подаётся результат суммиро-

вания по модулю 2 открытых данных очередного блока сообщения и выходных данных функции $CIPH_K$ для предыдущего блока. Поскольку выходные данные функции $CIPH_K$ для очередного блока идут прямо на выход алгоритма CBC, то есть являются шифртекстом этого блока и одновременно поступают на вход этой же функции для зашифрования последующего блока, то происходит сцепление блоков по шифртексту. Первый блок открытых данных суммируется с вектором инициализации (9). Этот вектор инициализации становится известен как отправителю, так и получателю в самом начале сеанса связи (поэтому зачастую его называют просто синхропосылкой). Расшифрование происходит (12), соответственно, в обратном порядке - сначала к шифртексту применяют функцию расшифрования $CIPH_K^{-1}$ (на рисунке 2,б – Процедура расшифрования), а затем суммируют с предыдущим блоком шифртекста для получения на выходе алгоритма очередного блока открытого текста. Первый блок открытого текста, опять же, восстанавливается с помощью вектора инициализации(11).

Таким образом весь алгоритм может быть выражен в виде уравнений следующим образом:

$$C_1 = CIPH_K(P_1 \oplus IV) \tag{9}$$

$$C_j = CIPH_K(P_j \oplus C_j) \tag{10}$$

$$P_K = CIPH_K^{-1}(C_1) \oplus IV \tag{11}$$

$$P_K = CIPH_K^{-1}(C_1) \oplus C_{j-1} \tag{12}$$

В уравнениях приняты следующие обозначения:
IV - вектор инициализации;
P_j - очередной, j -ый блок открытого текста;
C_j - очередной, j -ый блок шифртекста.

В режиме CBC при зашифровании каждая итерация алгоритма зависит от результата предыдущей итерации, то зашифрование сообщения не поддаётся расспараллеливанию. Однако в режиме расшифрования, когда весь шифртекст уже получен, функции $CIPH_K^{-1}$ вполне можно исполнять параллельно и независимо для всех блоков сообщения. Это даёт значительный выигрыш по времени. В этом режиме стоит остановиться ещё на одной детали. Дело в том, что последний блок шифртекста, который получается на выходе алгоритма режима CBC зависит как от ключа блочного шифра и вектора инициализации.

Поскольку алгоритм шифрования представляет собой множество обратимых преобразований электронного сообщения с целью его защиты от несанкционированного прочтения. Переход от открытого текста к шифртексту называется зашифрованием, а обратный переход - расшифрованием или дешифрованием [4]. Необходимым условием выполнения прямого, так и обратного криптографического преобразования является наличие секретного ключа. В связи с этим был предложен алгоритм криптографического преобразования, суть которого состоит в применении разработанной модели режима шифра к алгоритму шифрования на базе НПСС (рисунок 3).

Сообщение разбивается на блоки одинакового размера из n бит. При необходимости последний блок дополняется до длины n.

Для шифрования одного блока открытого сообщения P выполняются следующие действия.

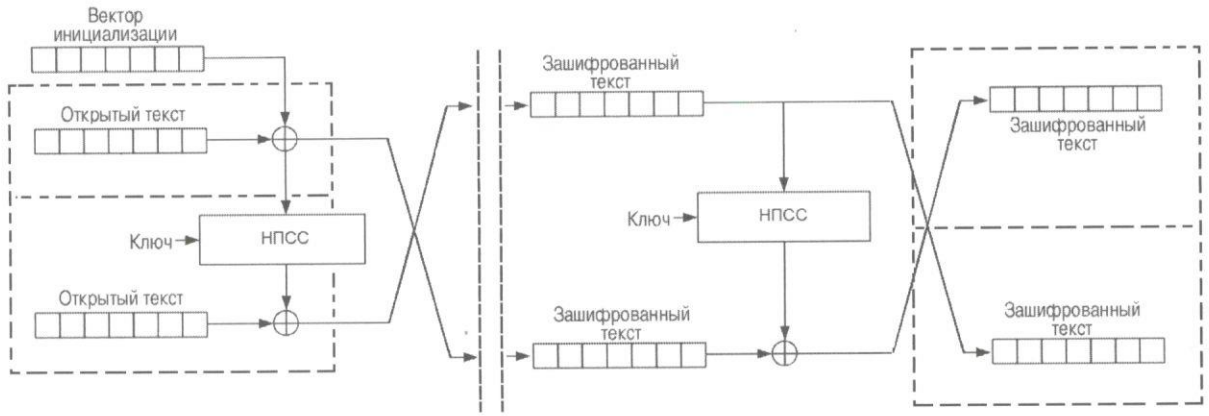

Рисунок 3 – Модель криптографического преобразования одного блока, полученная при комбинировании режима стандарта шифрования США «Режим сцепление блоков по шифртексту» и сети Фейстеля для алгоритма шифрования на базе НПСС

1. Выбранный блок делится на два подблока одинакового размера - «верхний» (U_0) и «нижний» (D_0); 2. Для «верхнего подблока» (U_0) производится сложение по модулю с «вектором инициализации» (IV). Вектор инициализации – псевдослучайная последовательность, размер (длина) (IV) равна размеру блока ($n/2$). «Верхний подблок» (U_0) изменяется функцией шифрования E_k с использованием ключа k.

$$x = E_k(U_0, k). \tag{13}$$

3. Результат складывается по модулю 2 («$\oplus$», «хог») с «нижним подблоком» (D_0):

$$x = x \oplus D_0 \tag{14}$$

4. Результат будет использован в следущем раунде в роли «верхнего подблока» (U_1):

$$U_1 = x. \tag{15}$$

5. «Верхний подблок» (U_0) текущего раунда будет использован в следующем раунде в роли «нижнего подблока» (D_1):

$$D_1 = U_0. \tag{16}$$

Здесь использованы следующие обозначения:

i - номер блока;

k - ключ;

IV - вектор инициализации (синхропосылка);

U_0 - верхний подблок сообщения (открытый текст);

D_0 - нижний подблок сообщения (открытый текст);

x - зашифрованный блок (шифртекст), полученный на предыдущем шаге шифрования;

E_k - функция, выполняющая блочное шифрование.

Перечисленные операции выполняются $N-1$ раз, где N - количество раундов в выбранном алгоритме шифрования.

4. Заключение

Цель полученной модели режима – улучшение статистических характеристик системы шифрования, разработанной на базе непозиционных полиномиальных систем счисления. В связи с этим планируется следующие работы:

- программная реализация предложенного алгоритма криптографического преобразования;

- анализ статистических свойств получаемых криптограмм с использованием графических и оценочных тестов.

Работа выполнена при поддержке программно-целевого финансирования научно-технических программ и проектов Комитетом науки МОН РК №0128/ПЦФ.

Литература

[1] FIPS 46-3. Data Encryption Standard (DES). – 1977. – 27 p.

[2] ГОСТ 28147-89. Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – 1989. – 28 с.

[3] Feistel H. Cryptography and Computer Privacy // Scientific American – 1973. – pp. 15-23

[4] Акушский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. – 1968. – 439 с.

[5] Бияшев Р.Г Разработка и исследование методов сквозного повышения достоверности в системах обмена данными распределенных АСУ. – 1985. – 328 с.

[6] Нысанбаева С. Е. Разработка и исследование криптографических систем на базе непозиционных полиномиальных систем счисления. – 2009. – 240 с.

[7] FIPS PUB 197. Advanced Encryption Standard (AES). – 2002. – 51 p.

[8] FIPS 46-3. Data Encryption Standard (DES). – 1977. – 27 p.

[9] Cvoboda A., Valach M. Operatorve obvody // Stroje na Zpracovani Informaci – 1955. – 122 p.

[10] Свобода А. Развитие вычислительной техники в Чехословакии. Системы счисления в остаточных классах. // Кибернетический сб. – 1963. – с. 115-149

[11] Амербаев В.М., Бияшев Р.Г. Интерполяция и коды, исправляющие ошибки // Теория кодирования и информационное моделирование. – 197. – с. 51-64

[12] Recommendation for Block Cipher Modes of Operation // Recommendation for Block Cipher Modes of Operation. – 2001. – 10 p.

[13] Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тесты на языке Си. – 2003. – 816 с.

[14] Фороузан Б.А. Криптография и безопасность сетей: Учебное пособие. – 2010. – 784 с.

[15] Панасенко С.В. Алгоритмы шифрования. Специальный справочник. – 2013. – 576 с.

References

[1] FIPS 46-3. Data Encryption Standard (DES). – 1977. – 27 p.

[2] GOST 28147-89. Sistema obrabotki informacii. Zashita kriptogaficheskaya. Algoritm kriptogaficheskogo preobrazovanya. – 1989. – 28 p.

[3] Feistel H. Cryptography and Computer Privacy // Scientific American – 1973. – pp. 15-23

[4] Akushski I.Ya., Yidickii D.I. Mashinnaya arifmetika v ostatochnih klassah. – 1968. – 439 p.

[5] Biyashev R.G Razrabotka i issledovanie metodov skvoznogo povisheniya dostovernosti v sistemah obmena dannimi raspredelennih ASY. – 1985. – 328 p.

[6] Nisanbayeva S. E. Razrabotka i issledovanie kriptograficheskih sistem na baze nepozicionnih polinomialnih sistem schisleniya. – 2009. – 240 p.

[7] FIPS PUB 197. Advanced Encryption Standard (AES). – 2002. – 51 p.

[8] FIPS 46-3. Data Encryption Standard (DES). – 1977. – 27 p.

[9] Cvoboda A., Valach M. Operatorve obvody // Stroje na Zpracovani Informaci – 1955. – 122 p.

[10] Svoboda A. Razvitie vichislitelnoi tehniki v Chehoslovakii. Sistemi schisleniya v ostatochnih klassah. // Kiberneticheski sb. – 1963. – p. 115-149

[11] Amerbayev V.M., Biyashev R.G. Interpolyaciya i kodi, ispravlyauchie oshibki // Teoriya kodirovaniya i informacionnoe modelirovanie. – 197. – p. 51-64

[12] Recommendation for Block Cipher Modes of Operation // Recommendation for Block Cipher Modes of Operation. – 2001. – 10 p.

[13] Shnaier B. Prikladnaya kriptografiya. Protokoli, algoritmi, ishodnie testi na yazike Si. – 2003. – 816 p.

[14] Foroyzan B.A. Kriptografiya i bezopasnost setei: Ychebnoe posobie. – 2010. – 784 p.

[15] Panasenko S.V. Algoritmi shifrovaniya. Specialni spravochnik. – 2013. – 576 p.