УДК. 681.3

Р.Г.Бияшев, Е.В.Горковенко, С.Е.Нысанбаева



АЛГОРИТМЫ ШИФРОВАНИЯ СООБЩЕНИЙ И ФОРМИРОВАНИЯ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ С ЗАДАННОЙ КРИПТОСТОЙКОСТЬЮ

(Институт проблем информатики и управления МОН РК, г. Алма-Ата)

При хранении, передаче и обмене электронной информацией в информационных сетях и системах возникают проблемы обеспечения ее конфиденциальности (защиты от атак), установления аутентификации (подлинности) автора и ее целостности (отсутствия изменений в полученном электронном сообщении). Конфиденциальность может быть обеспечена применением криптографических методов (шифрования). Задачу установления целостности сообщения и подлинности его автора позволяет эффективно решать электронная цифровая подпись (ЭЦП) – относительно короткая дополнительная информация, передаваемая вместе с подписанным текстом.

Существуют различные алгоритмы шифрования сообщений и формирования (создания) электронной цифровой подписи. Государственный стандарт Республики Казахстан (СТ РК 1073-2002) [1] на средства криптографической защиты информации (СКЗИ) распространяется на те средства, которые предназначены для:

- защиты передаваемых или хранимых конфиденциальных данных;
- контроля целостности передаваемых, используемых или хранимых данных или программного обеспечения;
- аутентификации, в том числе отказа от авторства или приписывания авторства одним субъектом другому;
- генерации, формирования, распределения или управления ключами.

В зависимости от степени защиты информации для СКЗИ стандартом устанавливаются 4 уровня безопасности. Каждый уровень определяется конкретным материальным ущербом в зависимости от нарушения защищенности информации путем разглашения, навязывания или несанкционированного изменения конфиденциальных данных. Указаны также общие требования к СКЗИ, в том числе и для каждого уровня безопасности, часть из которых приведена в таблице 1.

Таблица 1.

Уровень безопасности	Ущерб от разглашения, навязывания или несанкционированного изменения информации	Вычислительная сложность алгоритма ВКЗ	Длина ключа алгоритмов, бит		Длина хэш-кода бит	Длина ЭЦП, бит
			Симметричные	Асимметричные		
1	$\leq 10^2$ МРК	$\geq 2^{48}$	≤ 56	≤ 384	≤ 112	≤ 112
2	$\leq 10^4$ МРК	$\geq 2^{96}$	≤ 112	≤ 1536	≤ 160	≤ 160
3	$\leq 10^6$ МРК	$\geq 2^{128}$	≤ 168	≤ 3072	≤ 256	≤ 256
4	$\leq 10^8$ МРК	$\geq 2^{192}$	≤ 256	≤ 8192	≤ 320	≤ 512

МРК - минимальный расчетный показатель, ВКЗ – вскрытие криптографической защиты.

Длина ключа является, безусловно, одним из показателей криптостойкости алгоритмов шифрования сообщений и создания ЭЦП, но не самым лучшим. Правильнее, на наш взгляд, в качестве критерия использовать не длину ключа, а криптостойкость алгоритма.

Известные методы шифрования, схемы формирования ЭЦП и стандарты разработаны для позиционных систем счисления. Существенно повысить криптостойкость алгоритмов шифрования, а также сократить длину хэш-значений и электронной цифровой подписи позволяют нетрадиционные методы криптографии на основе непозиционной полиномиальной системы счисления.

Предлагаются алгоритмы шифрования текста сообщений и формирования электронной цифровой подписи в непозиционной полиномиальной системе, в которой криптостойкость зависит не только от длины ключа, но и от выбранной системы полиномиальных оснований, а также их распределения (порядка следования).

Поскольку шифрование является составной частью формирования ЭЦП, то оба алгоритма целесообразно представить одной блок-схемой. Для этого рассмотрим этапы процессов шифрования сообщения заданной длины и формирования ЭЦП. Предполагаем, что электронное сообщение и ЭЦП имеют соответственно длины N и N_1 бит, причем N_1 намного меньше N, а база данных (БД) неприводимых многочленов содержит все неприводимые полиномы с двоичными коэффициентами степени не выше N.

Процедура шифрования сообщения заданной длины N состоит из двух этапов:

1. выбор системы полиномиальных оснований и порядка их следования;
2. генерация гаммы с использованием ГПСЧ.

Эти два этапа описывают выбор одной (или одного варианта) системы оснований. Суть их состоит в следующем.

1. Пусть $p_1(x), p_2(x),..., p_S(x)$, $1 \le S \le N$, неприводимые многочлены с двоичными коэффициентами, используемые в качестве основного (рабочего) диапазона. Тогда сообщение длиной N можно интерпретировать как последовательность

остатков $a_1(x), a_2(x), ..., a_S(x)$ от деления некоторого многочлена *F(x)* на рабочие основания $p_1(x), p_2(x), ..., p_S(x)$ соответственно.

2. Ключевая последовательность длиной *N* бит также интерпретируется как последовательность остатков $b_1(x), b_2(x), ..., b_S(x)$, но от деления некоторого другого многочлена *G(x)* по тем же рабочим основаниям системы. Тогда в качестве криптограммы $w_1(x), w_2(x), ..., w_S(x)$ может рассматриваться некоторая функция *H(F(x),G(x))* , операции которой, в соответствии с операциями непозиционной системы счисления, выполняются параллельно по модулям полиномов, выбранных в качестве оснований системы.

Для процесса шифрования информации полным ключом, кроме многочлена *G(x)*, является и конкретный набор оснований, выбранных из всего множества неприводимых многочленов степени не выше *N*.

Общее число всех возможных и отличающихся друг от друга вариантов выбора систем оснований определяет криптостойкость алгоритма шифрования.

Пусть n_1 - число неприводимых многочленов с двоичными коэффициентами степени m_1. 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 [2]. 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 *N*) для записи полных систем вычетов по модулям этих оснований необходимо N бит.

Тогда процедура выбора системы рабочих оснований сводится к нахождению коэффициентов в уравнении

$$k_1 p^{m_1}(x) + k_2 p^{m_2}(x) + \ldots + k_S p^{m_S}(x) = N, \qquad (1)$$

(где $0 \le k_i \le n_i$, $p^{m_j}(x)$ - многочлен степени m_j, $1 \le m_j \le S$, $k = k_1 + k_2 + \ldots + k_S$), определяющем количество k неприводимых многочленов из БД различных степеней, которые можно выбрать в качестве оснований системы, запись вычетов по которым покрывает длину заданного сообщения *N*.

С ростом порядка неприводимых многочленов с двоичными коэффициентами их количество стремительно растет (таблица 2), в связи с чем очевиден широкий выбор решений уравнения (1).

Таблица 2.

Степень неприводимых многочленов	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	…
Количество неприводимых многочленов	1	1	2	3	6	9	18	30	56	120	240	488	972	1938	3876	7749	…
Количество бит, покрываемых неприводим. многочленами	1	2	6	12	30	54	126	240	504	1200	2640	5856	12636	27132	58140	123984	…

Для определения криптостойкости зашифрованного сообщения нужно найти число способов отбора оснований. Число различных комбинаций выбора оснований для какой-либо одной степени определяется k_i-сочетаниями из всех n_i неприводимых многочленов степени m_i. В непозиционных системах счисления существенен и порядок расположения оснований, поэтому число систем из *k* выбранных оснований будет равно

$$Z_1 = (k_1 + k_2 + \ldots + k_s)!\, C_{n_1}^{k_1} C_{n_2}^{k_2} \ldots C_{n_S}^{k_S}, \qquad (2)$$

Тогда все варианты шифрования (выбор систем оснований и гаммы, распределение оснований) определится соотношением

$$2^N \sum_{k_1, k_2, \ldots k_S} (k_1 + k_2 + \ldots + k_s)!\, C_{n_1}^{k_1} C_{n_2}^{k_2} \ldots C_{n_S}^{k_S}, \qquad (3)$$

в котором суммирование распространено на всевозможные комбинации целых положительных чисел $k_1, k_2, ..., k_S$, удовлетворяющих равенству (1), т.е. на все выборы систем оснований из числа неприводимых полиномов с двоичными коэффициентами степени $\leq N$.

Обратная величина выражения (3) определяет криптостойкость шифрования сообщения длины N:

$$p_{kr} = \frac{1}{2^N \sum\limits_{k_1, k_2, ..., k_s} (k_1 + k_2 + ... + k_S)! C_{n_1}^{k_1} C_{n_2}^{k_2} ... C_{n_S}^{k_S}}, \qquad (4)$$

Для длины сообщения в 256 байт можно, например, выбрать 80 многочленов 16-й степени, 60 многочленов 12 степени и 6 многочленов 8-й степени, т.е. всего 146 многочленов. В этом случае криптостойкость определяется выражением

$$p_{kr} = \frac{1}{2^{2048} 146! C_{7749}^{80} C_{488}^{60} C_{30}^{6}} \approx \frac{1}{10^{1146}},$$

что значительно меньше любой разумной величины, которая может быть задана в реальных условиях для системы шифрования.

Процедура формирования ЭЦП включает в себя три этапа:

1. восстановление функции $F(x)$: выбор системы полиномиальных оснований для сообщения длины N;
2. хэширование (сжатие) сообщения длины N до длины N_1 путем вычисления вычетов $F(x)$ по избыточным основаниям;
3. шифрование хэш-значения: выбор системы полиномиальных оснований и их размещения, генерация гаммы с использованием ГПСЧ.

Рассмотрим подробнее содержание перечисленных этапов.

1. Этот этап полностью совпадает по содержанию, а поэтому и по обозначениям, с первым этапом процедуры шифрования. Определение (восстановление) многочлена $F(x)$ производится по формуле

$$F(x) = \sum_{i=1}^{S} a_i(x) B_i(x), \quad \text{где}$$

$$B_i(x) = \frac{\prod_{i=1}^{S} p_i(x)}{p_i(x)} M_i(x) \equiv 1 (\mathrm{mod}\, p_i(x)),$$

значения многочленов M_i (x) выбираются для выполнения сравнения [3].

2. Хэширование сообщения производится расширением на избыточные основания $p_{S+1}(x), p_{S+2}(x),..., p_{S+U}(x)$, $1 \le U \le N_1$, выбранные произвольно из всех неприводимых многочленов степени, не превышающей N_1. Эта система оснований формируется независимо от выбора оснований $p_1(x), p_2(x),..., p_S(x)$, но среди U избыточных оснований могут быть и совпадающие с некоторыми из рабочих. Вычеты $a_{S+1}(x), a_{S+2}(x),..., a_{S+U}(x)$ от деления восстановленного многочлена *F(x)* на дополнительные основания $p_{S+1}(x), p_{S+2}(x),..., p_{S+U}(x)$ определяют длину хэш-значения N_1. Как видно, этот пункт повторяет первый этап шифрования.

3. Завершающим этапом создания ЭЦП является шифрование хэш-значения. Описание шифрования приводится в других обозначениях, так как и на этом этапе формирование системы полиномиальных оснований происходит независимо от выбора рабочих оснований.

3.1. Выбирается система оснований $r_1(x), r_2(x),..., r_W(x)$, $1 \le W \le N_1$, из числа неприводимых многочленов с двоичными коэффициентами степени не выше N_1. В состав оснований $r_1(x), r_2(x),..., r_W(x)$ могут попасть некоторые многочлены как из рабочих оснований $p_1(x), p_2(x),..., p_S(x)$, так и из избыточных $p_{S+1}(x), p_{S+2}(x),..., p_{S+U}(x)$. Хэш-значение длины N_1 интерпретируется как последовательность остатков $g_1(x), g_2(x),..., g_W(x)$ от деления некоторого многочлена $F_1(x)$ на выбранные основания $r_1(x), r_2(x),..., r_W(x)$ соответственно.

3.2. Ключевая последовательность генерируется с длиной N_1 и

интерпретируется как последовательность остатков $h_1(x),h_2(x),...,h_W(x)$ от деления некоторого полинома $G_1(x)$ на те же основания $r_1(x),r_2(x),...,r_W(x)$. Тогда полученная в результате шифрования криптограмма $l_1(x), l_2(x),..., l_W(x)$ может быть представлена как некоторая функция $H_1(F_1(x),G_1(x))$.

С учетом перечисленных этапов все варианты формирования ЭЦП будут описываться выражением

$$2^{N_1} \sum_{k_1,k_2,...k_S} ((k_1+k_2+...+k_s)!\ C_{n_1}^{k_1}\ C_{n_2}^{k_2}\ ...\ C_{n_S}^{k_S} \times$$

$$\times \sum_{t_1,t_2,...t_U} (t_1+t_2+...+t_U)!\ C_{d_1}^{t_1}\ C_{d_2}^{t_2}\ ...\ C_{d_U}^{t_U}) \times$$

$$\times \sum_{v,v_2,...,v_W} (v_1+v_2+...+v_W)!\ C_{l_1}^{v_1}\ C_{l_2}^{v_2}\ ...\ C_{l_W}^{v_W}), \quad (5)$$

В формуле (5) суммирование:

– $\sum_{t_1,t_2,...t_U}$ распространено на всевозможные комбинации целых положительных чисел $t_1,t_2,...,t_U$, удовлетворяющих равенству (аналогу формулы (1))

$$t_1 p^{a_1}(x) + t_2 p^{a_2}(x) + ... + t_U p^{a_U}(x) = N_1,$$

где $a_1,a_2,...,a_U$ и $d_1,d_2,...,d_U$ - соответственно степени и число неприводимых многочленов, используемых при выборе избыточных оснований, $0 \le t_i \le d_i$, $p^{a_j}(x)$ - многочлен степени a_j, $1 \le a_j \le U$, $t = t_1 + t_2 + ... + t_U$ - число избыточных оснований системы, запись вычетов по которым покрывает хэш-значение длины N_1;

– $\sum_{v,v_2,...,v_W}$ производится по всевозможным комбинациям целых

положительных чисел $v_1, v_2, ..., v_W$, определяемых из равенства

$$v_1 r^{b_1}(x) + v_2 r^{b_2}(x) + ... + v_W r^{b_W}(x) = N_1,$$

где $b_1, b_2, ..., b_W$ и $l_1, l_2, ..., l_W$ - степени и число неприводимых многочленов соответственно, используемых при выборе оснований $r_1(x), r_2(x), ..., r_W(x)$, $0 \le v_i \le l_i$, $r^{b_j}(x)$ - многочлен степени b_j, $1 \le b_j \le W$, $v = v_1 + v_2 + ... + v_W$ - система оснований системы, запись вычетов по которым покрывает шифруемое хэш-значение длины N_1.

Криптостойкость формирования ЭЦП определяется обратной величиной (5)

$$p_{sig} = \frac{1}{2^{N_1} \sum\limits_{k_1, k_2, ..., k_s} ((Z_1 \sum\limits_{t_1, t_2, ..., t_U} Z_2) \sum\limits_{v_1, v_2, ..., v_W} Z_3)}, \qquad (6)$$

где $Z_2 = (t_1 + t_2 + ... + t_U)! \, C_{d_1}^{t_1} \, C_{d_2}^{t_2} \, ... \, C_{d_U}^{t_U}$, $Z_3 = (v_1 + v_2 + ... + v_W)! \, C_{l_1}^{v_1} \, C_{l_2}^{v_2} \, ... \, C_{l_W}^{v_W}$.

Выражение (6) показывает возможность формирования ЭЦП существенно меньшей длины, чем указано в СТ РК, при сохранении, а при необходимости и увеличения ее надежности.

На рис. 1 приводится блок-схема реализации описанных процедур шифрования сообщений и формирования ЭЦП с заданной криптостойкостью $P_{зад}$. Выбор системы оснований реализуют блоки 3-7. Процедура шифрования сообщения задается переменной Kr и блоками 8, 12-15, 20, 21, а формирования ЭЦП – переменной Sig и блоками 8-21. При создании ЭЦП в процедуре шифрования хэш-значений учтена также возможность применения как использованных при вычислении хэш-значений избыточных оснований, так и выбираемых через блок 3 других оснований (переменная Sigkr, блоки 15-19).

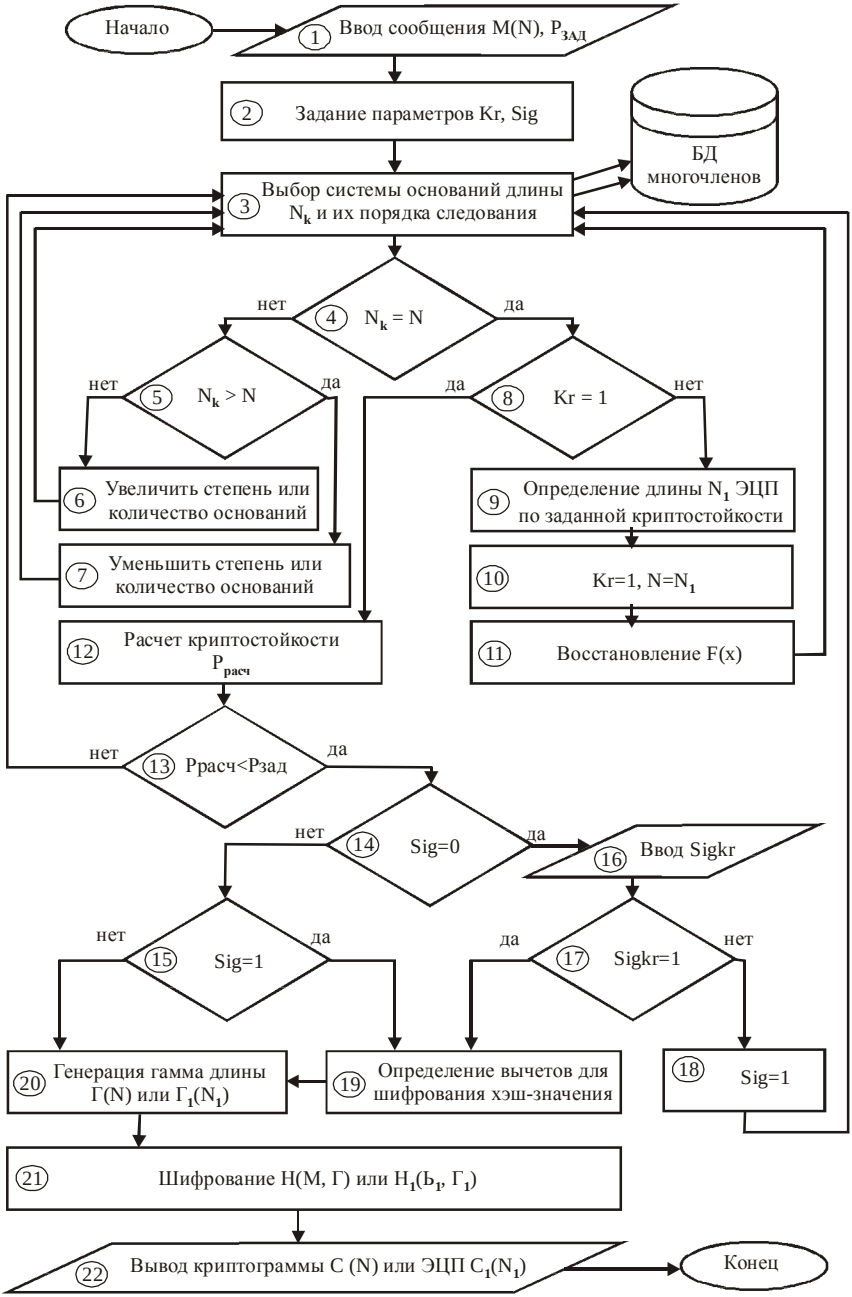

Рис. 1. Блок-схема шифрования сообщений и формирования ЭЦП

Литература

1. СТ РК 1073-2002 «Средства криптографической защиты информации» / Общие технические требования. - Астана: Госстандарт РК, 2002.
2. Гр. К. Моисил. Алгебраическая теория дискретных автоматических устройств. - М: Издательство иностранной литературы, 1963.
3. Акушский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. – М.: Советское радио, 1968.