5. *Скубілін М.Д. Спірідонов О.Б., Чєрєдничєнко Д.І.* Спосіб утримування інформації у недоступному для невизначеного кола осіб стані. Патент UA 33278, G06F 13/00, G09C 1/00, H04L 9/00, 2001.02.15.

6. *Skubilin M.D., Pismenov A.V.* Teghekatzrrlthlan kgvoghviknan edavnak. Патент AM 973, G01F 13/00, G09C 1/00, H04L 9/00, б. 2, 2001.06.10.

7. *Skubilin M.D., Kasimov F.C., Spiridonov O.B., Regimov R.M.* Melumatin programli kodlaşdirma – dekodlaşdirma űsulu. Patent AZ 20010140, G06F 13/00, G09C 1/00, H04L 9/00, 2001.10.02.

8. *Скубилин М.Д., Божич В.И., Спиридонов О.Б.* Способ защиты информации от несанкционированного доступа и устройство для его осуществления //Патэнт BY 5605, G06F 13/00, G09C 1/00, 2003.12.30.

Р. Г. Бияшев, С. Е. Нысанбаева
Казахстан, г. Алматы, Институт проблем информатики и управления

МОДЕЛИРОВАНИЕ ГЕНЕРАЦИИ КЛЮЧЕЙ В НЕПОЗИЦИОННОЙ ПОЛИНОМИАЛЬНОЙ СИСТЕМЕ СЧИСЛЕНИЯ

Использование непозиционных полиномиальных систем счисления (систем счисления в остаточных классах с полиномиальными основаниями или модулярной арифметики) при создании симметричных криптосистем позволяет существенно повысить их надежность, критерием которой является криптостойкость самого алгоритма шифрования. В непозиционной полиномиальной системе счисления (НПСС) основаниями служат неприводимые многочлены над полем $GF(2)$. В этой системе существенно повышается также криптостойкость алгоритма формирования электронной цифровой подписи (ЭЦП), при этом возможно значительное сокращение длины хэш-значения и подписи [1-3].

В работе представлена модель процедуры генерации ключевых последовательностей для алгоритмов зашифрования и расшифрования электронного сообщения заданной длины *N* бит (далее – сообщения) при хранении и передаче электронной информации и формирования ЭЦП в НПСС на базе нетрадиционного криптографического метода шифрования [4].

В связи с тем, что построение нетрадиционных алгоритмов и методов шифрования и формирования ЭЦП основано на выборе системы полиномиальных оснований, была создана база данных неприводимых многочленов, содержащая их общее число для каждой из степеней от 1 до 22. Пополнение базы данных неприводимыми многочленами последующих степеней производится по мере необходимости в полиномах более высокой степени.

Алгоритм шифрования начинается с формирования системы полиномиальных оснований. Пусть основаниями выбраны неприводимые многочлены с двоичными коэффициентами $p_1(x), p_2(x),..., p_S(x)$ соответственно степени $m_1, m_2,..., m_S$, называемые также рабочими основаниями. Многочлен $P(x) = p_1(x)p_2(x)...p_S(x)$ степени $m = \sum_{i=1}^{S} m_i$ является основным рабочим диапазоном НПСС. В этой системе любой многочлен, степени меньшей *m*, имеет единственное представление в виде его вычетов по модулям рабочих оснований соответственно. Все основания системы должны быть различными: соблюдение этого необходимо для выполнения китайской теоремы об остатках, даже если основания выбираются из неприводимых многочленов одной степени.

Сообщение в НПСС интерпретируется как последовательность остатков $\alpha_1(x),\alpha_2(x),...,\alpha_S(x)$ от деления некоторого неизвестного многочлена $F(x)$ (напомним, что его степень должна быть меньше m) на основания $p_1(x), p_2(x),..., p_S(x)$ соответственно:

$$F(x) = (\alpha_1(x),\alpha_2(x),...,\alpha_S(x)). \quad (1)$$

Расположение выбранных оснований определяется всеми возможными их перестановками.

Непозиционное представление (1) многочлена $F(x)$ является единственным. Позиционное же представление $F(x)$ восстанавливается по его непозиционному виду (1) [5]:

$$F(x) = \sum_{i=1}^{S} \alpha_i(x) P_i(x), \text{ где } P_i(x) = \frac{P(x)}{p_i(x)}. \quad (2)$$

В выражении (1) 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 $\alpha_S(x)$.

Затем генерируется ключевая гамма длиной N битов, которая 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:

$$G(x) = (\beta_1(x), \beta_2(x),..., \beta_S(x)). \quad (3)$$

Полученная в результате нетрадиционного шифрования криптограмма в виде последовательности вычетов $\omega_1(x),\omega_2(x),...,\omega_S(x)$ рассматривается как некоторая функция $H(F(x),G(x))$, операции которой, в соответствии с операциями непозиционной системы счисления, выполняются параллельно по модулям оснований системы. В итоге имеем криптограмму в виде

$$H(x) = (\omega_1(x),\omega_2(x),...,\omega_S(x)). \quad (4)$$

Как видно из вышеизложенного, алгоритм шифрования характеризуется полным ключом, включающим не только гамму $G(x)$ длиной N битов, но и выбранную систему полиномиальных оснований с учетом порядка их распределения. Криптостойкость алгоритма шифрования определяется всеми возможными и отличающимися друг от друга вариантами выбора систем оснований и генерируемых ключевых гамм [2,3].

Выбор системы оснований степени от m_i до m_S из базы данных неприводимых многочленов степени не выше N ограничен условием, которое описывается выражением

$$k_1 p^{m_1}(x) + k_2 p^{m_2}(x) + ... + k_S p^{m_S}(x) = N \cdot \quad (5)$$

Уравнение (5) определяет неизвестные коэффициенты k_i, означающие число выбираемых в качестве оснований неприводимых полиномов степени m_i, $0 \le k_i \le n_i$, n_i - множество всех неприводимых многочленов степени m_i, $p^{m_i}(x)$ - многочлен степени m_i, $1 \le m_i \le m_S \le N$, $S = k_1 + k_2 + ... + k_S$ - количество всех выбранных оснований.

Полные системы вычетов по модулям многочленов степени m_i содержат все многочлены с двоичными коэффициентами степени не выше $m_i - 1$, для записи которых необходимо m_i битов [6]. Уравнение (5) определяет то количество выбранных S оснований, вычеты по которым покрывают длину заданного сообщения N. При $m_S = N$ для записи полных систем вычетов по модулям этих оснований необходимо N битов.

С увеличением степени неприводимых многочленов их количество быстро растет. В табл. 1 эти полиномы приведены только до 12 -й степени включительно, для 16-й степени число неприводимых многочленов равно 7749, а для 20-й – 122673). Поэтому уравнение (1) имеет широкий спектр решений.

Таблица 1

Таблица неприводимых полиномов над полем $GF(2)$

Степень полиномов	1	2	3	4	5	6	7	8	9	10	11	12
Количество полиномов	1	1	2	3	6	9	18	30	56	120	240	488

Рассмотрим используемый при компьютерной реализации алгоритма шифрования нетрадиционный криптографический метод [4].

Криптограмма сообщения $H(x) = (\omega_1(x), \omega_2(x), ..., \omega_S(x))$ получается в результате умножения многочленов (2) и (3) в соответствии со свойствами сравнений по двойному модулю

$$F(x)G(x) \equiv H(x) (\mathrm{mod}\, P(x)) .$$

Тогда элементы последовательности вычетов $\omega_1(x), \omega_2(x), ..., \omega_S(x)$ являются наименьшими остатками от деления произведений $\alpha_i(x)\beta_i(x)$ на соответственные основания $p_i(x)$:

$$\alpha_i(x)\beta_i(x) \equiv \omega_i(x) (\mathrm{mod}\ p_i(x)), \ i=1,2,...S. \quad (6)$$

В двоичном виде криптограмма $H(x)$ будет выглядеть следующим образом: двоичным коэффициентам остатка $\omega_1(x)$ ставятся в соответствие первые l_1 битов криптограммы $H(x)$, двоичным коэффициентам остатка $\omega_2(x)$ ставятся в соответствие следующие l_2 битов криптограммы и так далее, двоичным коэффициентам последнего вычета $\omega_S(x)$ ставятся в соответствие последние l_S двоичных разрядов криптограммы.

Расшифрование криптограммы $H(x)$ по известному ключу $G(x)$ состоит в вычислении для каждого значения $\beta_i(x)$, как следует из (6), обратного (инверсного) многочлена $\beta_i^{-1}(x)$ из условия выполнения следующего сравнения:

$$\beta_i(x)\beta_i^{-1}(x) \equiv 1(\mathrm{mod}\ p_i(x)),\ i=1,2,\ldots S. \quad (7)$$

В результате получится многочлен $G^{-1}(x) = (\beta_1^{-1}(x), \beta_2^{-1}(x),..., \beta_S^{-1}(x))$, инверсный к многочлену $G(x)$.

Тогда исходное сообщение в соответствии с (6) и (7) восстанавливается по сравнению с

$$F(x) \equiv G^{-1}(x)H(x)(\mathrm{mod}\,P(x)). \quad (8)$$

Через вычеты выражение (8) запишется в виде следующих сравнений:

$$\alpha_i(x) \equiv \beta_i^{-1}(x)\omega_i(x)(\mathrm{mod}\ p_i(x)),\ i=1,2,\ldots S. \quad (9)$$

Таким образом получена модель алгоритма шифрования электронного сообщения заданной длины N битов в непозиционной полиномиальной системе счисления.

Полным ключом в этой модели является выбранная система полиномиальных оснований $p_1(x), p_2(x),..., p_S(x)$, полученный некоторым генератором псевдослучайных чисел ключ $G(x) = (\beta_1(x), \beta_2(x),..., \beta_S(x))$ и инверсный к нему ключ $G^{-1}(x) = (\beta_1^{-1}(x), \beta_2^{-1}(x),..., \beta_S^{-1}(x))$, вычисляемый в соответствии с выражением (8) или (9).

При компьютерной реализации рассмотренной модели шифрования для генерации и хранения полных ключей разработана программа, которая реализует все этапы создания полного ключа (будем называть его далее просто ключом) в указанном выше порядке генерации ключевых последовательностей. Полученный ключ хранится в базе данных. Возможен просмотр записей сохраненных ключей в базе данных, доступ к которой осуществляется через пароль.

Перед выбором системы оснований $p_1(x), p_2(x),..., p_S(x)$ задается их общее число S. Затем вводится количество оснований k_i для каждой конкретной степени оснований m_i, $i=1,2,\ldots S.$, определяемых из уравнения (5). После завершения формирования системы оснований осуществляется проверка на соответствие общего количества выбранных оснований $k_1 + k_2 + ... + k_S$ заданным S и уравнению (5), то есть выбранная система рабочих оснований должна покрывать шифруемое сообщение длиной N битов.

Генерация псевдослучайной гаммы для шифрования $G(x) = (\beta_1(x), \beta_2(x),..., \beta_S(x))$ производится с использованием выбранных рабочих оснований $p_1(x), p_2(x),..., p_S(x)$. Многочлены $\beta_i(x)$ находятся как результат сложения вычетов $P_i(x)$ соответственно по модулям $p_i(x)$, $i=1,2,\ldots S.$ с некоторым многочленом степени $m_i - 1$.

Затем из сравнений (7) определяется для расшифрования ключевая последовательность $G^{-1}(x) = (\beta_1^{-1}(x), \beta_2^{-1}(x),..., \beta_S^{-1}(x))$.

Сгенерированный ключ (полный) сохраняется в базе данных. Таким образом могут быть получены и записаны в базу данных ключи различной длины.

При выполнении процедур шифрования и создания ЭЦП номер записи ключа в базе данных задается по алгоритму, который псевдослучайным образом генерирует этот номер по времени и дате выбора ключа.

Приведенная модель шифрования используется в алгоритме формирования в непозиционной полиномиальной системе счисления ЭЦП длиной N_1 битов. Длина подписи N_1 может быть значительно меньше длины подписываемого электронного сообщения длиной N битов. Создание ЭЦП реализуется при помощи процедур хэширования и шифрования: хэш-функция сжимает подписываемое сообщение до длины N_1, а затем полученное хэш-значение шифруется [2].

Алгоритм формирования ЭЦП включает в себя три последовательных этапа:

- восстановление функции $F(x)$ по выбранной системе рабочих полиномиальных оснований $p_1(x), p_2(x),..., p_S(x)$ для сообщения длиной N;

- хэширование сообщения длины N до длины N_1 путем вычисления вычетов $F(x)$ по избыточным (дополнительным или контрольным) основаниям $p_{S+1}(x), p_{S+2}(x),..., p_{S+U}(x)$;

- шифрование хэш-значения: выбор системы полиномиальных оснований и их размещения, генерация ключевой гаммы длины N_1.

Первый этап совпадает с первой половиной процедуры шифрования. Восстановление многочлена $F(x)$ производится по формуле (2).

Хэширование сообщения происходит расширением системы рабочих оснований на избыточные основания $p_{S+1}(x), p_{S+2}(x),..., p_{S+U}(x)$, которые выбираются произвольно из всех неприводимых многочленов степени, не превышающей N_1, где U – это количество всех избыточных оснований. Система дополнительных оснований формируется независимо от выбора рабочих оснований $p_1(x), p_2(x),..., p_S(x)$, но среди U избыточных оснований могут быть и совпадающие с некоторыми из них. Вычеты $\alpha_{S+1}(x), \alpha_{S+2}(x),..., \alpha_{S+U}(x)$ 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 этап формирования ЭЦП также повторяет первую часть шифрования.

На этапе шифрования полученного хэш-значения выбирается система оснований $r_1(x), r_2(x),..., r_W(x)$ из числа неприводимых многочленов с двоичными коэффициентами степени не выше N_1 независимо от выбора рабочих и дополнительных многочленов, но в состав этих оснований могут войти некоторые как из рабочих оснований, так и из избыточных. В соответствии с алгоритмом шифрования хэш-значение интерпретируется как последовательность остатков $\gamma_1(x), \gamma_2(x),..., \gamma_W(x)$ от деления некоторого многочлена $F_1(x)$ на выбранные основания $r_1(x), r_2(x),..., r_W(x)$ соответственно.

Затем генерируется ключевая последовательность длиной N_1, которая интерпретируется как последовательность остатков $\eta_1(x), \eta_2(x),..., \eta_W(x)$ 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 $\lambda_1(x), \lambda_2(x),..., \lambda_W(x)$ может быть представлена как некоторая функция $H_1(F_1(x), G_1(x))$.

Полным ключом в представленном алгоритме формирования цифровой подписи кроме многочлена $G_1(x)$ являются и конкретные наборы оснований

(рабочих, дополнительных и для шифрования хэш-значения) на каждом из 3-х этапов формирования ЭЦП.

В программной реализации для шифрования хэш-значения применен описанный выше нетрадиционный метод [4]. Тогда для этой модели формирования ЭЦП необходим ее полный ключ, состоящий из следующих ключевых гамм каждого этапа:

- системы рабочих оснований $p_1(x), p_2(x),..., p_S(x)$ степени не выше N и порядка их расположения;
- системы избыточных оснований $p_{S+1}(x), p_{S+2}(x),..., p_{S+U}(x)$ степени не выше N_1 и порядка их расположения;
- ключевой последовательности псевдослучайных чисел $G_1(x) = \eta_1(x), \eta_2(x),..., \eta_W(x)$ и обратной к ней гаммы $G_1^{-1}(x) = \eta_1^{-1}(x), \eta_2^{-1}(x),..., \eta_W^{-1}(x)$, системы оснований $r_1(x), r_2(x),..., r_W(x)$ для шифрования хэш-значения с учетом порядка их следования.

При подписывании сообщения ключи каждого этапа алгоритма формирования ЭЦП выбираются из созданной базы полных ключей для шифрования сообщения. Номер записи ключа в базе данных выбирается так же, как при шифровании.

Компьютерная программа генерации и хранения ключей в базе данных является основой разработки комплекса программ по криптографической защите информации при ее хранении и передаче.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Акушский И.Я., Юдицкий Д.И.* Машинная арифметика в остаточных классах. – М.: Советское радио, 1968. – 439 с.

2. *Амербаев В. М., Бияшев Р. Г., Нысанбаева С. Е.* Применение непозиционных систем счисления при криптографической защите информации // Известия Национальной академии наук Республики Казахстан. Сер. физ.-мат. наук. – 2005.. – № 3. – С. 84–89.

3. *Бияшев Р.Г., Нысанбаева С.Е.* Влияние состава полиномиальных оснований непозиционной системы счисления на надежность шифрования // Материалы VIII Международной научно-практической конференции «Информационная безопасность», – Таганрог, Изд-во ТРТУ, 3-7 июля 2006, – С. 66–69.

4. *Нысанбаев Р.К.* Криптографический метод на основе полиномиальных оснований // Вестник Министерства науки и высшего образования и Национальной академии наук Республики Казахстан – Алматы: Гылым, 1999. - №5. – С. 63–65

5. *Бияшев Р.Г.* Разработка и исследование методов сквозного повышения достоверности в системах обмена данными распределенных АСУ: Дис... на соискание уч. степ. докт. тех. наук. – М., 1985. – 328 с.

6. *Моисил Гр. К.* Алгебраическая теория дискретных автоматических устройств. – М.: Издательство иностранной литературы, 1963. – 680 с.

A. G. Chefranov

Russia , Taganrog, Taganrog Institute of Technology, Southern Federal University, and North Cyprus, Gazimagusa, Eastern Mediterranean University

ONE-TIME PASSWORD SCHEME WITH INFINITE AUTHENTICATIONS NUMBER

Authentication of clients to servers is an important problem that has been solved in a number of ways (see, for example, [1, 2]). One time password (OTP) schemes such as [3, 4, 5] address the problem in assumption of not secure channels of communication between clients and servers, and possible compromise of passwords on the server side.