Сказуемое «поддерживают» позволяет выполнить преобразование этого правила в эквивалентное правило импликацию с 12 конъюнкциям в антецеденте.

Литература

1 Нуртазин А.Т., Хисамиев З.Г. Синтаксическое и семантическое представление текстов // Труды XI междунар. школы-семинара «Проблемы оптимизации сложных систем». – Чолпон-Ата, 2015. – Ч. II. – С.494-497.

2 Nurtazin A., Khisamiev Z. Automatic extraction of corollaries from semantic structure of text // Open engineering: Special Issue on “Mathematical modeling in applied sciences” . – 2016.

3 Нуртазин А.Т., Хисамиев З.Г. Автоматическое извлечение следствий из семантической структуры текста // Матер. междунар. науч. конф. «Информатика и математика», посв. 25-летию Независимости Республики Казахстан и 25-летию Института информационных и вычислительных технологий. – Алматы, 2016. – Ч. II. – С.75 – 83.

4 Конституция Республики Казахстан //http://www.akorda.kz/ru/official_documents/ constitution : 14.10.2016.

АЛГОРИТМ ШИФРОВАНИЯ НА БАЗЕ КИТАЙСКОЙ ТЕОРЕМЫ ОБ ОСТАТКАХ

Нысанбаева С.Е., Капалова Н.А., Дюсенбаев Д.С., Дузбаев Т.Т.
e-mail: *sultasha1@mail.ru, kapalova@ipic.kz, dimash_dds@mail.ru, talgat.duzbaev@mail.ru*

Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аннотация. *В данной работе рассматривается алгоритм шифрования, разработанный на основе китайской теоремы об остатках и* непозиционной полиномиальной системе счисления (*НПСС). В этом алгоритме блок открытого текста длины N бит в процессе преобразовании в НПСС не интерпретируется как последовательность остатков, а представляется в виде остатков от деления на рабочие основания НПСС.*

Пусть $p_1(x), p_2(x), \dots, p_s(x)$ – неприводимые многочлены с двоичными коэффициентами, используемые в качестве рабочего диапазона, т.е. они являются рабочими основаниями НПСС. Это означает, что многочлен $P(x) = p_1(x) \cdot p_2(x) \cdots p_s(x)$ степени $m = \sum_{i=1}^{s} m_i$ определяет основной рабочий диапазон НПСС. В НПСС любой многочлен степени меньше m может быть единственным образом представлен в виде его вычетов по модулям рабочих оснований $p_1(x), p_2(x), \dots, p_s(x)$ соответственно [1-4].

Описание алгоритма шифрования. Блок открытого сообщения длины N бит представляется в НПСС как некоторый многочлен $T(x)$ с двоичными коэффициентами.

Тогда в НПСС этот многочлен $T(x)$ может быть представлен в непозиционном виде, т.е. в виде последовательности остатков или вычетов, которые получаются при делении этого многочлена $T(x)$ на рабочие основания $p_1(x), p_2(x), \dots, p_s(x)$. По правилам системы счисления в остаточных классах получение вычетов осуществляется следующим образом:

$$T(x) \equiv \alpha_i(x)\big(mod\ p_i(x)\big), \text{ где } i=1,2,\dots,S. \quad (1)$$

Тогда, $T(x)$ в непозиционном виде записывается как $\mathrm{T}(x) = \big(\alpha_1(x), \alpha_2(x), \dots, \alpha_S(x)\big)$.

Восстановление многочлена (1) в позиционном виде производится по следующей формуле:

$$F(x) = \sum_{i=1}^{S} \alpha_i(x)\, B_i(x), \quad \text{где } B_i(x) = \frac{P_S(x)}{p_i(x)} M_i(x) \equiv 1\big(mod\ p_i(x)\big). \quad (2)$$

Для проведения этих вычислений необходимо определить базисы $B_i(x)$ в НПСС по формуле (2). Для этого нужно вычислить многочлены:

$$\delta_i(x) \equiv \frac{P_S(x)}{p_i(x)}\big(mod\ p_i(x)\big) \quad (3)$$

и инверсные к ним полиномы: $\delta_i^{-1}(x)$: $\delta_i^{-1}(x)\delta_i(x) \equiv 1\big(mod\ p_i(x)\big)$.

Тогда базисы находятся по формуле:

$$B_i(x) = \delta_i^{-1}(x)\frac{P_S(x)}{p_i(x)}, \quad (4)$$

которые также являются секретными параметрами алгоритма.

Используемая ключевая последовательность длины *N* бит в НПСС интерпретируется как последовательность остатков $(\beta_1(x), \beta_2(x), \dots, \beta_s(x))$, полученных при делении некоторого многочлена *G(x)* на рабочие основания $p_1(x), p_2(x), \dots, p_s(x)$:

$$G(x) = (\beta_1(x), \beta_2(x), \dots, \beta_s(x)),$$

где $G(x) \equiv \beta_i(x)(mod\big(p_i(x)\big), i = \overline{1,S}$. Остатки $(\beta_1(x), \beta_2(x), \dots, \beta_s(x))$ выбираются таким образом, что первым l_1 битам ключа ставятся в соответствие двоичные коэффициенты остатка $\beta_1(x)$, следующим l_2 битам – двоичные коэффициенты остатка $\beta_2(x)$ и так далее, последним l_S двоичным разрядам ставятся в соответствие двоичные коэффициенты вычета $\beta_S(x)$.

По известному ключу *G*(*x*) для каждого значения $\beta_i(x)$ производится вычисление обратного (или инверсного) многочлена ${\beta_i}^{-1}(x)$ из условия выполнения следующего сравнения:

$$\beta_i(x) \times {\beta_i}^{-1}(x) \equiv 1\big(mod\ p_i(x)\big), i = \overline{1,S}.$$

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

Далее производится зашифрование блока открытого текста. Шифртекст $H(x)$ получается в результате выполнения некоторой функции $H(x) = (F(x), G(x), P(x))$:

$$H(x) \equiv \omega_i(x)\big(mod\ p_i(x)\big), \text{ где } i=1,2,\ldots,S$$

или

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

Шифрование производится по следующей формуле:

$$\alpha_i(x)\beta_i(x) \equiv \omega_i(x)\big(mod\ p_i(x)\big)$$

или

$$T(x) \otimes G(x) \equiv H(x)(\ mod\ P(x)),$$

где $T(x) = \big(\alpha_1(x), \alpha_2(x), \ldots, \alpha_s(x)\big)$ - открытый текст, $G(x) = \big(\beta_1(x), \beta_2(x), \ldots, \beta_s(x)\big)$ – ключ, $P(x) = \big(p_1(x), p_2(x), \ldots, p_s(x)\big)$ – рабочие основания.

Перевод шифртекста $H(x)$ в позиционный вид производится по формуле:

$$H(x) = \sum_{i=1}^{S} \omega_i(x)\, B_i(x)(\ modP(x)). \quad (5)$$

Расшифрование шифртекста осуществляется по следующему выражению:

$$\omega_i(x)\beta_1^{-1}(x) \equiv \alpha_i(x)(mod\ p_i(x)) \quad ; \quad (6)$$

$$H(x) \otimes G^{-1}(x) \equiv F(x)(\ mod\ P(x)) \quad ; \quad (7)$$

где $F(x) = \big(\alpha_1(x), \alpha_2(x), \ldots, \alpha_S(x)\big)$,

$G^{-1}(x) = (\beta_1^{-1}(x), \beta_2^{-1}(x), \ldots, \beta_S^{-1}(x)) -$ инверсный ключ,

$P(x) = \big(p_1(x), p_2(x), \ldots, p_S(x)\big)$ – рабочий основания,

$H(x) = \big(\omega_1(x), \omega_2(x), \ldots, \omega_S(x)\big)$ – шифртекст.

Представление результата расшифрования в позиционном виде производится по формуле:

$$T(x) = \sum_{i=1}^{S} \alpha_i(x)\, B_i(x)(\ modP(x)), \quad (8)$$

где $T(x)$ – расшифрованный (открытый) текст.

Программная реализация рассмотренного алгоритма выполнена на языке программирования C# с использованием интерфейса программирования в приложении Windows Forms (рисунок 1).

При выполнении алгоритмов шифрования/дешифрования файл считывается с диалогового окна программы. При нажатии кнопки «Шифрование»/«Дешифрование» начинается процесс шифрования или дешифрования сответственно. При шифровании для записи полученного шифртекста создаётся файл с названием шифрируемого файла, но с расширением «.crypt» в том каталоге, который был выбран пользователем. Если же файл уже существует, то он заменяется текущим шифртекстом по умолчанию в той же папке, где хранится и сама программа. Принципиальная схема работы программной реализации приведена на рисунке 2.

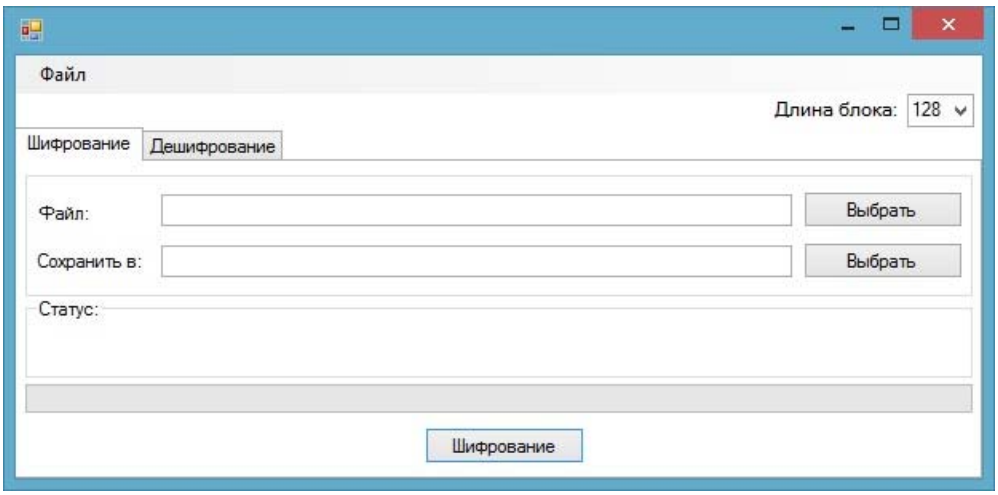

Рис. 1 - Пользовательский интерфейс программы

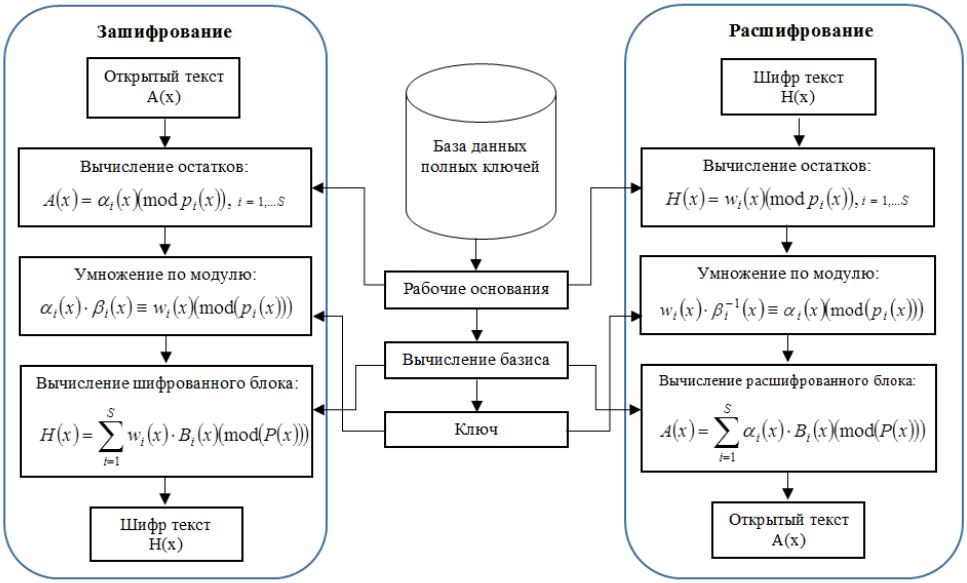

Рис. 2 – Принципиальная схема алгоритма шифрования на базе китайской теоремы об остатках

Рассмотрим примеры шифрования для одного блока открытого файла, демонстрирующие проявление «лавинного эффекта» у рассмотренного алгоритма**.**

Пример 1. При изменении одного бита в конце открытого текста при одном и том же ключе шифртексты, полученные для исходного и измененного открытого блока, полностью отличаются друг от друга.

Набор ключей:
100100000100101 110011110000110 11110101101110 1010101001100 100110110111001
101010011100000 10110100010100 10111100

Открытий текст:	**Шифртекст:**
50726f6772616d6d6572637368617270	D31FDA7909205AC93813A4D9EDB3E54E
50726f6772616d6d6572637368617271	951748E6E9CC911DE27A3F07F45DD6FE

Пример 2. При изменении одного бита в середине открытого текста при одном и том же ключе шифртексты, полученные для исходного и измененного открытого блока, полностью отличаются друг от друга.

Открытий текст:	**Шифртекст:**
50726f6772616d6d6572637368617270	D31FDA7909205AC93813A4D9EDB3E54E
50726f6772616d6c6572637368617270	E4CCABF3DDDC39ADA6E7C4EBA1A89192

Пример 3. При изменении одного бита в конце открытого текста и ключа шифртексты, полученные для исходного и измененного открытого блока, полностью отличаются друг от друга.

Набор ключей:
100100000100101 110011110000110 11110101101110 1010101001100 100110110111001
101010011100000 10110100010100 10111000

Открытий текст:	**Шифртекст:**
50726f6772616d6d6572637368617270	1B80ACE699830754C5DBD7E90B5EC57F
50726f6772616d6d6572637368617271	493C69376852233AC93A0D43950AF586

Заключение

Предлагаемый алгоритм шифрования при сравнении с разработанным ранее алгоритмом шифрования на базе НПСС [3] имеет следующие преимущества: алгоритм удовлетворяет требованиям по «лавинному эффекту» или статистическому криптоанализу.

Вместе с тем имеются и недостатки. В процессе шифрованиия и дешифрования при выполнении операции деления полиномов снижается производительность (эффективность) работы программы. Так как в самом алгоритме изначально заложено возможность распараллеливания по рабочим основаниям НПСС, то это позволяет избавиться от этого недостатка. Это и будет являться предметом дальнейших исследований по надежности и эффективности рассмотренного алгоритма шифрования на основе китайской теоремы об остатках.

Литература

1. Бияшев Р. Г. Разработка и исследование методов сквозного повышения достоверности в системах обмена данными распределенных АСУ: дисс. докт. тех. наук: 05.13.06: защищена 09.10.1985: утв. 28.03.1986. - М., 1985.
2. Амербаев В.М., Бияшев, Р.Г., Нысанбаева С.Е. Применение непозиционных систем счисления при криптографической защите // Изв. Нац. акад. наук Республики Казахстан.– Сер. физ.-мат.– Алматы:Гылым, 2005. - № 3. – С. 84-89.
3. R. Biyashev, M. Kalimoldayev, S. Nyssanbayeva, N. Kapalova, R. Khakimov. Program Modeling of the Cryptography Algorithms on Basis of Polynomial Modular Arithmetic / The 5th International Conference on Society and Information Technologies (ICSIT 2014, march 4-7, 2014- Orlando, Florida, USE) – IIIS. pp. 49-54
4. Бияшев Р.Г., Нысанбаева С. Е., Капалова Н.А. Секретные ключи для непозиционных криптосистем. Разработка, исследование и применение. – LAB LAMBERT Academic Publishing, 2014, с. 126.

РЕАЛИЗАЦИЯ АЛГОРИТМА КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ

Нысанбаева С. Е., Кабылханов А. Б.
e-mail: *sultasha1@mail.ru, faircisco@gmail.ru*

Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аннотация. *В данной работе приводится описание разработанной компьютерной программы для криптографического алгоритма, разработанного на основе режима стандарта шифрования США «Режим сцепления блоков по шифртексту», сети Фейстеля и системы шифрования на базе НПСС. Данная программа является реализацией ранее полученных теоретических результатов при разработке указанного выше криптоалгоритма.*

В Институте информационных и вычислительных технологий (ИИВТ) Министерства образования и науки Республики Казахстан выполняются работы по созданию, исследованию и реализации криптографических алгоритмов защиты хранимой и передаваемой информации. Эти алгоритмы разрабатываются с использованием непозиционных полиномиальных систем счисления (НПСС).

Одним из основных примеров при разработке блочных алгоритмов криптографического преобразования является многократная, состоящая из нескольких циклов (раундов), обработка одного блока открытого текста. На каждом цикле данные подвергаются специальному преобразованию при участии вспомогательного ключа, полученного из заданного секретного ключа. Примером такого криптографического преобразования является сеть Фейстеля [1]. Выбор числа циклов определяется требованиями по криптостойкости и эффективности реализации блочного шифра. Как правило, чем больше циклов, тем выше криптостойкость, но ниже эффективность реализации блочного шифра [1].