РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 542 926**(13) **C1**

(51) МПК
G09C 1/00 (2006.01)
H04L 9/00 (2006.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2014114746/08, 14.04.2014**

(24) Дата начала отсчета срока действия патента:
14.04.2014

Приоритет(ы):
(22) Дата подачи заявки: **14.04.2014**

(45) Опубликовано: **27.02.2015** Бюл. № **6**

(56) Список документов, цитированных в отчете о поиске: **RU 2459276 C1, 20.08.2012. RU 2459367 C2, 20.08.2012. RU 2103828 C1, 27.01.1998. RU 2411666 C1, 10.02.2011. RU 2459275, 20.08.2012. US 2013/0016829 A1, 17.01.2013. US 7831827 B2, 09.11.2010. US 7397916 B2, 08.07.2008**

Адрес для переписки:
197376, Санкт-Петербург, ул. Проф. Попова, 5, СПбГЭТУ, патентный отдел, Ивановой Е.А.

(72) Автор(ы):
Молдовян Александр Андреевич (RU),
Молдовян Дмитрий Николаевич (RU),
Вайчикаускас Мария Александровна (RU)

(73) Патентообладатель(и):
Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Санкт-Петербургский государственный электротехнический университет "ЛЭТИ" им. В.И. Ульянова (Ленина)" (RU)

(54) СПОСОБ ШИФРОВАНИЯ СООБЩЕНИЯ, ПРЕДСТАВЛЕННОГО В ВИДЕ МНОГОРАЗРЯДНОГО ДВОИЧНОГО ЧИСЛА

(57) Реферат:

Способ шифрования блока данных, представленного в виде битовой строки, относится к области электросвязи, а именно к области криптографических устройств и способов. Технический результат - повышение уровня защищенности шифруемой информации. Способ шифрования сообщения, представленного в виде многоразрядного двоичного числа, заключающийся в том, что генерируют секретный ключ (p, q) в виде двух простых многоразрядных двоичных чисел p и q, генерируют открытый ключ в виде многоразрядного двоичного числа n=pq, формируют криптограмму C в зависимости от сообщения M и открытого ключа n и восстанавливают сообщение M из криптограммы C по секретному ключу (p, q), отличающийся тем, что дополнительно генерируют вспомогательное многоразрядное двоичное число R<n, криптограмму C формируют в виде пары (A, B) многоразрядных двоичных чисел A и B в зависимости от сообщения M, открытого ключа n и многоразрядного двоичного числа R, а восстанавливают сообщение M путем решения уравнения $x^2-Ax+B=0 \bmod n$ относительно неизвестного x и вычисления сообщения M из одного из решений указанного уравнения. 3 з.п. ф-лы.

RU 2542926 C1

RU 2542926 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 542 926**(13) **C1**

(51) Int. Cl.
G09C 1/00 (2006.01)
H04L 9/00 (2006.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2014114746/08, 14.04.2014**

(24) Effective date for property rights:
14.04.2014

Priority:
(22) Date of filing: **14.04.2014**

(45) Date of publication: **27.02.2015** Bull. № **6**

Mail address:
197376, Sankt-Peterburg, ul. Prof. Popova, 5, SPbGEhTU, patentnyj otdel, Ivanovoj E.A.

(72) Inventor(s):
Moldovjan Aleksandr Andreevich (RU),
Moldovjan Dmitrij Nikolaevich (RU),
Vajchikauskas Marija Aleksandrovna (RU)

(73) Proprietor(s):
Federal'noe gosudarstvennoe bjudzhetnoe obrazovatel'noe uchrezhdenie vysshego professional'nogo obrazovanija "Sankt-Peterburgskij gosudarstvennyj ehlektrotekhnicheskij universitet "LEhTI" im. V.I. Ul'janova (Lenina)" (RU)

(54) METHOD TO CODE MESSAGE REPRESENTED AS MULTIDIGIT BINARY NUMBER

(57) Abstract:

FIELD: information technologies.

SUBSTANCE: method to code a message represented as a multidigit binary number, which consists in the fact that a secret key is generated (p, q) in the form of two simple multidigit binary numbers p and q, an open key is generated in the form of a multi-digit binary number n=pq, a cryptogram C is generated depending on the message M and open key n, and the message M is recovered from the cryptogram C according to the secret key (p, q), differing by the fact that additionally they generate an auxiliary multidigit binary number R<n, the cryptogram C is formed as a pair (A, B) of multidigit binary numbers A and B depending on the message M, the open key n and the multidigit binary number R, and the message M is recovered by solving the equation x^2-Ax+B=0 mod n relative to the unknown x and calculation of the message M from one of the solutions of the specified equation.

EFFECT: increased level of protection of coded information.

4 cl

RU 2542926 C1

RU 2542926 C1

Изобретение относится к области электросвязи и вычислительной техники, а конкретнее к области информационной безопасности телекоммуникационных систем и, в частности, может быть использовано в криптографических системах, обеспечивающих конфиденциальность сообщений, передаваемых по открытым каналам связи.

Известен способ шифрования путем формирования секретного ключа, генерации ключевого потока в виде последовательности битов, зависящих от секретного ключа, и сложения текущих битов ключевого потока с текущими битами передаваемого сообщения [Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография. С.-Петербург, Лань, 2000. - 218 с.; см. с.88-89]. Недостатком этого способа шифрования является необходимость синхронизации ключевого потока и потока данных.

Также известен способ шифрования, включающий генерацию 56-битового секретного ключа, формирование сообщения M в виде 64-битовой строки, генерацию криптограммы, представляющей собой 64-битовую строку, в зависимости от секретного ключа [Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография. С.-Петербург, Лань, 2000. - 218 с.; см. с.68-73]. При этом генерация криптограммы осуществляется путем разбиения сообщения M на две 32-битовые строки и поочередное преобразование 32-битовых строк в зависимости от секретного ключа. Недостатком этого способа является малый размер секретного ключа, что не обеспечивает криптостойкости, соответствующей современным требованиям.

Толкование терминов, используемых в описании, приведено в Приложении 1

Также известен способ шифрования сообщения M, представленного в виде битовой строки, описанный в патенте США №4424414 [Hellman M.E., Pohlig S.C. Exponentiation Cryptographic Apparatus and Method // U.S. Patent #4,424,414. Jan.3, 1984] и в книге [Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. - М:. Издательство ТРИУМФ, 2002. - 815 с.; см. с.577-578]. Ближайший способ-аналог (прототип) включает следующие действия:

1. Генерируют простое многоразрядное двоичное число (МДЧ) p.

2. Генерируют секретный ключ в в виде двух МДЧ e и d, удовлетворяющих условию $ed \equiv 1 \bmod p-1$

3. Формируют криптограмму в виде МДЧ C по формуле $C=M^e \bmod p$.

4. Восстанавливают сообщение M из криптограммы C по формуле $M=C^d \bmod p$.

Наиболее близким по своей технической сущности к заявленному способу шифрования сообщения M, представленного в виде МДЧ, является известный способ шифрования, включающий генерацию секретного ключа в виде двух больших простых МДЧ p и q, генерацию открытого ключа в виде МДЧ n, формирование криптограммы в виде МДЧ C по формуле $C=M^2 \bmod n$ [Молдовян Н.А. Теоретический минимум и алгоритмы цифровой подписи. - С.-Петербург. Петербург - БХВ, 2010. - 304 с.; см. с.78] и восстановление сообщения M из криптограммы C путем вычисления квадратных корней из криптограммы по модулю n, а именно по формуле $M = \sqrt{C} \bmod n$, из которой вычисляются четыре различных корня, одним из которых является сообщение M. Недостатком этого способа шифрования является то, что данный способ шифрования не обеспечивает достаточной стойкости при шифровании сравнительно коротких сообщений, например сообщений, размер которых не превышает половины размера МДЧ n. Этот недостаток связан с тем, что извлечение квадратных корней из криптограмм, полученных путем возведения коротких сообщений в квадрат, может быть выполнен сравнительно легко без знания разложения МДЧ n на простые

множители p и q, являющиеся элементами секретного ключа.

Задачей заявленного нового технического решения является разработка способа шифрования, в котором устраняется возможности восстановления сообщения из криптограмм, полученных путем шифрования коротких сообщений, без знания разложения МДЧ n на простые множители p и q.

Техническим результатом нового способа шифрования сообщения M, представленного в виде МДЧ, является повышение уровня защищенности информации при шифровании коротких сообщений.

Указанный технический результат достигается тем, что в способе шифрования сообщения M, представленного в виде МДЧ, заключающемся в том, что генерируют секретный ключ (p, q) в виде двух простых многоразрядных двоичных чисел p и q, генерируют открытый ключ в виде многоразрядного двоичного числа n=pq, формируют криптограмму C в зависимости от сообщения M и открытого ключа n и восстанавливают сообщение M из криптограммы C по секретному ключу (p, q),

новым является то, что дополнительно генерируют вспомогательное МДЧ R<n, криптограмму C формируют в виде пары (A, B) многоразрядных двоичных чисел A и B в зависимости от сообщения M, открытого ключа n и МДЧ R, а восстанавливают сообщение M путем решения уравнения x^2-Ax+B=0 mod n относительно неизвестного x и вычисления сообщения M из одного из решений указанного уравнения.

Генерация вспомогательного МДЧ R<n, имеющего разрядность, примерно равную разрядности МДЧ n, устраняет возможность нахождения решений уравнения X^2-Ax+B=0 mod n без знания разложения МДЧ n на простые множители p и q для сообщений M, представленных в виде МДЧ любого размера, включая короткие сообщения, например размером от 1 до 500 бит.

Новым также является то, что криптограмму C формируют в виде пары (A, B) МДЧ A и B, генерируемых по формулам A=(R+n-M-1) mod n и B=R(n-M-1) mod n.

Генерация МДЧ A и B по формулам A=(R+n-M-1) mod n и B=R(n-M-1) mod n обеспечивает то, что уравнение x^2-Ax+B=0 mod n в качестве своих решений имеет МДЧ x_1=R и МДЧ x_2=n-M-1 mod n, и сообщение вычисляется по формуле M=n-x_2-1 mod n.

Новым также является и то, что криптограмму C формируют в виде пары (A, B) МДЧ A и B, генерируемых по формулам A=(2R-M) mod n и B=R(R-M) mod n.

Генерация МДЧ A и B по формулам A=(2R-M) mod n и B=R(R-M) mod n обеспечивает то, что уравнение x^2-Ax+B=0 mod n в качестве своих решений имеет МДЧ x_1=R и МДЧ x_2=R-M mod n и сообщение вычисляется по формуле M=R-x_2 mod n.

Новым является и то, что дополнительно генерируют вспомогательное МДЧ R<n путем генерации вспомогательного сообщения T и вычисления R по формуле R=(n-T) mod n.

Генерация вспомогательного МДЧ R<n путем генерации вспомогательного сообщения T и вычисления R по формуле $R=(n-T)^2$ mod n позволяет осуществить совместное шифрование двух сообщений, которые восстанавливаются из криптограммы C=(A, B) путем решения уравнения x^2-Ax+B=0 mod n относительно неизвестного x и вычисления сообщения M из одного из решений, а сообщения T - из другого решения. Эта возможность реализуется путем генерации МДЧ A и B по формулам A=(R+M) mod n и B=RM mod n. В случае таких значений МДЧ A и B уравнение x^2-Ax+B=0 mod n в качестве

своих решений имеет МДЧ x_1=R и МДЧ x_2=M и сообщение T вычисляется по формуле $T = n - \sqrt{x_1} \bmod n$, а сообщение M - по формуле M=x_2.

Изобретательский замысел заявленного нового технического решения состоит в дополнительной генерации вспомогательного МДЧ R<n достаточно большого размера и формировании криптограммы C в виде пары МДЧ A и B, являющихся коэффициентами уравнения x^2-Ax+B=0 mod n и зависящих как от сообщения M, так и от МДЧ R. Это позволяет восстановить сообщение M путем решения указанного уравнения и вычисления сообщения M из одного из его решений. Зависимость решений от МДЧ R устраняет возможность восстановления сообщений M малого размера без знания разложении числа n. Благодаря указанной новой совокупности существенных признаков достигнут сформулированный изобретательский замысел.

Проведенный анализ уровня техники позволил установить, что в известных источниках информации аналоги, характеризующиеся совокупностью признаков, тождественных всем признакам заявленного технического решения, отсутствуют, что указывает на соответствие заявленного изобретения условию патентоспособности «новизна». Результаты поиска известных решений в данной и смежных областях техники с целью выявления признаков, совпадающих с отличительными от прототипа признаками заявленного объекта, показали, что они не следуют явным образом из уровня техники. Из уровня техники также не выявлена известность влияния предусматриваемых существенными признаками заявленного изобретения преобразований на достижение указанного технического результата. Следовательно, заявленное изобретение соответствует условию патентоспособности «изобретательский уровень».

Корректность заявленного способа шифрования сообщения M, представленного в виде МДЧ, обеспечивается тем, что многочлен второй степени x^2-Ax+B (mod n), корнями которого являются МДЧ x_1 и x_2, может быть представлен в виде произведения $(x-x_1)(x-x_2)$, т.е. имеет место

$$x^2-Ax+B=(x-x_1)(x-x^2)=x^2-(x_1+x_2)x+x_1x_2 \pmod n$$

следовательно, A=(x_1+x_2) mod n и B=$x1x_2$ mod n. Поэтому, если встроить сообщение M и дополнительно генерируемое МДЧ R в корни уравнения x^2-Ax+B=0 mod n таким образом, что из корней x_1 и x_2 легко можно вычислить M и R, то восстановление сообщения M из криптограммы можно выполнить путем решения указанного уравнения и вычисления M из одного из корней. Таким образом, корни x_1 и x_2 вычисляются по значениям M и R, а криптограмма C формируется в виде пары МДЧ (A, B) по формулам A=(x_1+x_2) mod n и B=x_1x_2 mod n. Криптограмма задает такие коэффициенты указанного уравнения второй степени, при которых МДЧ x_1 и x_2 являются решениями этого уравнения. Решение уравнения с коэффициентами, заданными криптограммой, позволит найти МДЧ x_1 и x_2 и вычислить из последних сообщение M и МДЧ R.

Решение уравнения x^2-Ax+B=0 mod n выполняется по секретному ключу (p, q) следующим путем. Решаются следующие два уравнения: x^2-Ax+B=0 mod p и x^2-Ax+B=0 mod q, каждое из которых имеет два корня. Пусть корнями первого уравнения являются следующие два значения:

$$x_{p1}=\frac{A}{2}+\sqrt{\frac{A^2}{4}-B}\bmod p \quad \text{и} \quad x_{p2}=\frac{A}{2}-\sqrt{\frac{A^2}{4}-B}\bmod p,$$

а корнями второго - следующие:

$$x_{q1}=\frac{A}{2}+\sqrt{\frac{A^2}{4}-B}\bmod q \quad \text{и} \quad x_{q2}=\frac{A}{2}-\sqrt{\frac{A^2}{4}-B}\bmod q.$$

Вычислительно эффективные алгоритмы извлечения квадратных корней по простому модулю описаны, например, в книге [Молдовян Н.А. Теоретический минимум и алгоритмы цифровой подписи. - С.-Петербург. Петербург - БХВ, 2010. - 304 с.; см. с.25-29]. Четыре корня X_1, X_2, X_3 и X_4 уравнения x^2-Ax+B=0 mod n находятся как решения следующих четырех систем линейных сравнений

$$\begin{cases} X_1 \equiv x_{p1} \bmod p \\ X_1 \equiv x_{q1} \bmod q \end{cases}; \quad \begin{cases} X_2 \equiv x_{p1} \bmod p \\ X_2 \equiv x_{q2} \bmod q \end{cases}; \quad \begin{cases} X_3 \equiv x_{p2} \bmod p \\ X_3 \equiv x_{q1} \bmod q \end{cases} \quad \text{и}$$

$$\begin{cases} X_4 \equiv x_{p2} \bmod p \\ X_4 \equiv x_{q2} \bmod q \end{cases}.$$

В соответствии с китайской теоремой об остатках [Молдовян Н.А. Теоретический минимум и алгоритмы цифровой подписи. - С.-Петербург. Петербург - БХВ, 2010. - 304 с.; см. с.15-16] решениями этих четырех систем сравнений являются следующие четыре МДЧ:

$X_1=(x_{p1}q(q^{-1} \bmod p)+x_{q1}p(p^{-1} \bmod q))\bmod n;$

$X_2=(x_{p1}q(q^{-1} \bmod p)+x_{q2}p(p^{-1} \bmod q))\bmod n;$

$X_3=(x_{p2}q(q^{-1} \bmod p)+x_{q1}p(p^{-1} \bmod q))\bmod n;$

$X_4=(x_{p2}q(q^{-1} \bmod p)+x_{q2}p(p^{-1} \bmod q))\bmod n.$

По значениям корней X_1, X_2, X_3, и X_4 вычисляются четыре различных МДЧ M_1, M_2, M_3 и M_4, соответственно. При этом одно из МДЧ M_1, M_2, M_3, и M_4, например M_4, соответствует осмысленному сообщению M, представленному в виде МДЧ, т.е. из криптограммы (A, B) восстанавливается сообщение $M=M_4$.

Рассмотрим частные примеры реализации заявленного способа шифрования сообщения M, представленного в виде МДЧ.

Пример 1

Данный пример иллюстрирует реализацию заявленного способа по п.2 формулы изобретения. В данном частном варианте реализации способа выполняются следующие действия:

1. Генерируют секретный ключ (p, q) в виде двух простых 512-разрядных двоичных чисел p и q.

2. Генерируют открытый ключ в виде МДЧ n=pq.

3. Формируют криптограмму C в виде пары (A, B) МДЧ A и B в зависимости от сообщения M и открытого ключа n путем выполнения следующих действий:

3.1. Генерируют вспомогательное МДЧ R<n в виде случайного 1022-разрядного двоичного числа R.

3.2. Генерируют МДЧ A по формуле A=(R+n-M-1) mod n.

3.3. Генерируют МДЧ B по формуле B=R(n-M-1) mod n.

4. Восстанавливают сообщение M из криптограммы C по секретному ключу (p, q) путем выполнения следующих действий:

4.1. Вычисляют четыре решения уравнения второй степени x^2-Ax+B=0 mod n в виде МДЧ X_1, X_2, X_3 и X_4.

4.2. Вычисляют четыре МДЧ M_1, M_2, M_3, и M_4 по формуле

$M_i=(n-X_i-1) \bmod n$, где i=1, 2, 3 и 4.

4.3. Отбрасывают три случайных МДЧ, например МДЧ M_1, M_2 и M_3, и в качестве восстановленного сообщения M берут осмысленное сообщение, представленное МДЧ M_4, т.е. $M=M_4$.

Пример 2

Данный пример иллюстрирует реализацию заявленного способа по п.3 формулы изобретения. В данном частном варианте реализации способа выполняются следующие действия:

1. Генерируют секретный ключ (p, q) в виде двух простых 768-разрядных двоичных чисел p и q.

2. Генерируют открытый ключ в виде МДЧ n=pq.

3. Формируют криптограмму C=(A, B) в виде пары МДЧ A и B в зависимости от сообщения M и открытого ключа n путем выполнения следующих действий:

3.1. Генерируют вспомогательное МДЧ R<n в виде случайного 1534-разрядного двоичного числа R.

3.2. Генерируют МДЧ A по формуле A=(2R-M) mod n.

3.3. Генерируют МДЧ B по формуле B=R(R-M) mod n.

4. Восстанавливают сообщение M из криптограммы C по секретному ключу (p, q) путем выполнения следующих действий:

4.1. Вычисляют четыре решения уравнения второй степени x^2-Ax+B=0 mod n в виде МДЧ X_1, X_2, X_3 и X_4.

4.2. Вычисляют четыре МДЧ M_1, M_2, M_3, и M_4 по формуле

$M=(2X_i-A) \bmod n$, где i=1, 2, 3 и 4.

4.3. Отбрасывают три случайных МДЧ, например МДЧ M_1, M_3, и M_4, и в качестве восстановленного сообщения M берут осмысленное сообщение, представленное МДЧ M_3, т.е. $M=M_4$.

Пример 3

Данный пример иллюстрирует реализацию заявленного способа по п. 4 формулы изобретения. В данном частном варианте реализации способа криптограмма формируется в зависимости от двух независимых сообщений - сообщения M и вспомогательного сообщения T, которые восстанавливаются из криптограммы. В данном примере выполняются следующие действия:

1. Генерируют секретный ключ (p, q) в виде двух простых 1024-разрядных двоичных чисел p и q.

2. Генерируют открытый ключ в виде МДЧ n=pq.

3. Формируют криптограмму C=(A, B) в виде пары МДЧ A и B в зависимости от сообщения M и открытого ключа n путем выполнения следующих действий:

3.1. Генерируют вспомогательное МДЧ R<n в виде случайного 2046-разрядного

двоичного числа R, для чего

3.1.1. Генерируют вспомогательное сообщение T.

3.1.2. Вычисляют МДЧ R по формуле $R=(n-T)^2 \bmod n$.

3.2. Генерируют МДЧ A по формуле $A=(2R-M) \bmod n$.

3.3. Генерируют МДЧ B по формуле $B=R(R-M) \bmod n$.

4. Восстанавливают сообщение M из криптограммы C по секретному ключу (p, q) путем выполнения следующих действий:

4.1. Вычисляют четыре решения уравнения второй степени $x^2-Ax+B=0 \bmod n$ в виде МДЧ X_1, X_2, X_3, и X_4.

4.2. Вычисляют четыре МДЧ M_1, M_2, M_3, и M_4, по формуле

$M_i=(2X_i-A) \bmod n$, где i=1, 2, 3 и 4.

4.3. Отбрасывают три случайных МДЧ, например МДЧ M_1, M_3, и M_4, и в качестве восстановленного сообщения M берут осмысленное сообщение, представленное МДЧ M_3, т.е. $M=M_3$.

5. Восстанавливают вспомогательное сообщение T из криптограммы C по секретному ключу (p, q) путем выполнения следующих действий:

4.1. Вычисляют значение МДЧ $R=(M+A)/2 \bmod n$ 0 mod n.

4.2. Вычисляют четыре МДЧ U_1, U_2, U_3 и U_4, являющихся корнями второй степени из МДЧ R, после чего вычисляют МДЧ T_1, T_2, T_3, и T_4 по следующей формуле

$T_i=n-U_i \bmod n$, где i=1, 2, 3 и 4.

4.3. Отбрасывают три случайных МДЧ, например МДЧ T_1, T_3, и T_4, и в качестве восстановленного вспомогательного сообщения T берут осмысленное сообщение, представленное МДЧ T_2, т.е. $T=T_2$.

Производительность заявленного способа шифрования сообщения M, представленного в виде МДЧ, примерно равна производительности его ближайшего аналога, поскольку вычислительная сложность как первого, так и второго способа примерно равна вычислительной сложности операции извлечения квадратного корня по простому модулю p и операции извлечения квадратного корня по простому модулю q. Для уменьшения вычислительной сложности операции извлечения квадратных корней по простым модулям p и q можно выбирать в качестве секретного ключа МДЧ p и q, которые удовлетворяют условиям $p\equiv 3 \bmod 4$ и $q\equiv 3 \bmod 4$ [Молдовян Н.А. Теоретический минимум и алгоритмы цифровой подписи. - С.-Петербург. Петербург - БХВ, 2010. - 304 с.; см. с.25].

Таким образом, приведенные математические выкладки и конкретные примеры реализации показывают, что заявленный способ шифрования сообщения M, представленного в виде МДЧ, технически реализуем и позволяет достичь сформулированного технического результата.

Заявляемый способ шифрования сообщения M, представленного в виде МДЧ, может быть применен для разработки средств защиты информации, передаваемой по открытым телекоммуникационным каналам, от несанкционированного доступа.

Толкование терминов, используемых в описании изобретения

1. Двоичный цифровой электромагнитный сигнал - последовательность битов в виде нулей и единиц.

2. Параметры двоичного цифрового электромагнитного сигнала: разрядность и порядок следования единичных и нулевых битов.

3. Разрядность двоичного цифрового электромагнитного сигнала - общее число его единичных и нулевых битов, например число 10011 является 5-разрядным.

4. Битовая строка - двоичный цифровой электромагнитный сигнал, представляемый в виде конечной последовательности цифр «0» и «1».

5. Секретный ключ - двоичный цифровой электромагнитный сигнал, используемый для формирования подписи к заданному электронному документу. Секретный ключ представляется, например, в двоичном виде как последовательность цифр «0» и «1».

6. Открытый ключ - битовая строка, параметры которой зависят от секретного ключа. Открытый ключ вычисляется по секретному как значение функции, вычислимой в одну сторону, которая делает практически неосуществимым вычисление секретного ключа по открытому ключу.

7. Многоразрядное двоичное число (МДЧ) - двоичный цифровой электромагнитный сигнал, интерпретируемый как двоичное число и представляемый в виде последовательности цифр «0» и «1».

8. Разрядность МДЧ - это число двоичных разрядов (битов) в записи МДЧ по двоичному основанию.

9. Простое МДЧ - это МДЧ, которое делится только на единицу и на само себя.

10. Взаимно простые МДЧ - это МДЧ, наибольший общий делитель которых равен единице.

11. Сравнимость двух заданных значений по модулю некоторого числа m - это равенство остатков от деления заданных значений на m [Бухштаб А.А. Теория чисел. - М.: Просвещение, 1966. - 384 с.].

12. Сравнение - выражение, состоящее из правой и левой частей, такое, что значение левой части сравнимо со значением правой части по заданному модулю [Бухштаб А.А. Теория чисел. - М.: Просвещение, 1966. - 384 с.].

13. Обратный элемент по модулю n к числу a, являющемуся взаимно простым с n, есть натуральное число, обозначаемое как a^{-1}, для которого выполняется условие $a^{-1}a=1$; для любого числа, являющегося взаимно простым с модулем, существует элемент, обратный этому числу. Известны эффективные алгоритмы вычисления обратных элементов [Романец Ю.В., Тимофеев П.А., Шань-гин В.Ф. Защита информации в компьютерных системах и сетях. - М.: Радио и связь. - с.308-310].

14. Операция возведения числа S в дискретную степень A по модулю n - это операция, выполняемая над конечным множеством натуральных чисел {0, 1, 2, …, n-1}, включающем n чисел, являющихся остатками от деления всевозможных целых чисел на число n; результат выполнения операций сложения, вычитания и умножения по модулю n представляет собой число из этого же множества [Виноградов И.М. Основы теории чисел. - М.: Наука, 1972. - 167 с.];

операция возведения числа S в дискретную степень Z по модулю n определяется как Z-кратное последовательное умножение по модулю n числа S на себя, т.е. в результате этой операции также получается число W, которое меньше или равно числу n-1; даже для очень больших чисел S, Z и n существуют эффективные алгоритмы выполнения операции возведения в дискретную степень по модулю.

12. Сложность операции Oper - количество стандартных элементарных битовых операций (т.е. операций над битами), которые необходимо осуществить для выполнения операции Oper. Чем сложнее операция, тем больше время ее выполнения.

Формула изобретения

1. Способ шифрования сообщения, представленного в виде многоразрядного

двоичного числа, заключающийся в том, что генерируют секретный ключ (p, q) в виде двух простых многоразрядных двоичных чисел p и q, генерируют открытый ключ в виде многоразрядного двоичного числа n=pq, формируют криптограмму C в зависимости от сообщения M и открытого ключа n и восстанавливают сообщение M из криптограммы C по секретному ключу (p, q), отличающийся тем, что дополнительно генерируют вспомогательное многоразрядное двоичное число R<n, криптограмму C формируют в виде пары (A, B) многоразрядных двоичных чисел A и B в зависимости от сообщения M, открытого ключа n и многоразрядного двоичного числа R, а восстанавливают сообщение M путем решения уравнения x^2-Ax+B=0 mod n относительно неизвестного x и вычисления сообщения M из одного из решений указанного уравнения.

2. Способ по п.1, отличающийся тем, что криптограмму C формируют в виде пары (A, B) многоразрядных двоичных чисел A и B, генерируемых по формулам A=(R+n-M-1) mod n и B=R(n-M-1) mod n.

3. Способ по п.1, отличающийся тем, что криптограмму C формируют в виде пары (A, B) многоразрядных двоичных чисел A и B, генерируемых по формулам A=(2R-M) mod n и B=R(R-M) mod n.

4. Способ по п.1, отличающийся тем, что дополнительно генерируют вспомогательное многоразрядное двоичное число R<n путем генерации вспомогательного сообщения T и вычисления R по формуле $R=(n-T)^2$ mod n.