*УДК* 519.330.341 (063)
*ГРНТИ* *81.93.29*

# КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ И АЛГОРИТМЫ ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

**Тукубаев З.Б., Туртаев М.Р.**

*(Университет имени академика А.Куатбекова, г.Шымкент, Казахстан )*

*Мақалада "Электронды Үкімет" құрылысында компьютерлік ақпараттарды қорғау әдістері мен алгоритмдеріне талдау жасалған.*

*В статье делается анализ методов и алгоритмов защиты компьютерной информации при построении "Электроного Правительства"*

Ключевые слова: конфиденциальность, абсолютная криптостойкость шифра, шифрованное сообщение, равновероятная гамма, электронный документооборот, электронная подпись. Коды JEL 81.93.29

Конкретные работы по построению "Электронного Правительства " в Казахстане были начаты 7 января 2003 года; был принят Закон Республики Казахстан об "Электронных документах и об электронной подписи"[1]. Внедрение вышеотмеченных систем в правительственные документообороты и в финансовые сферы (денежные обороты) потребует строгой конфиденциальности циркулирующей информации.

В традиционных системах передачи данных конфиденциальность обеспечивалась различными методами; из них наиболее часто и эффективно используемые методы – метод псевдослучайной перестройки рабочей частоты (FHSS-Frequency Hopping Spread Spectrum) [3].

В RadioEthernet используется этот же метод и метод прямой последовательности (DSSS- Direct Sequence Spread

Spectrum ) [4]. При применении первого рабочий диапазон 2,4 ГГц делится на 79 поддиапазонов. Передатчик и приемник синхронно переключают рабочие частоты с шагом 20 мс…400мс. При применении второго каждый бит информации шифруется последовательностью из 11 символов. Ключ шифровки должен быть известен каждому из сторон.

Современные системы передачи данных интегрального обслуживания принципиально отличаются от традиционных.

Главное отличие современных систем заключается в том, что во всех информационных системах различного назначения (государственные, коммерческие, образовательные, военные и др.) используется единая информационная система интегрального обслуживания, т.е.Интернет. При этом, проблема обеспечения конфиденциальности и информационной безопасности работы при внедрений вышеотмеченных систем становится еще острее, поскольку в системах интегрального обслуживания используются общие канальные и другие ресурсы.

В современных системах конфиденциальность и информационная безопасность обеспечиваются различными методами : правовыми, административными, физическими, информационными ( использование паролей, идентификационных номеров абонентов, ограничение пользователей и др.) и криптографическими методами.

Наиболее эффективным из них является – криптографический метод, который используется в электронном документообороте и в электронной подписи.

Для обеспечения безопасности в компьютерных сетях вводятся стандарты на методы шифрования (государственные, национальные и международные); так в США национальное бюро стандартов в 1977 году приняло стандарт на шифрование данных DES [4, 240] (Data

Encryption Standard), который был успешно использован до 2001 года.

В стандарте предусмотрены были 2 режима работы КАК (Key Auto Key)и СТАК (Cipher Text Auto Key).

В режиме КАК данные шифруются порциями по 64 бита. Ключ также имеет длину 64 бита.

В режиме СТАК система работает в стартстопном режиме и данные шифруются по 8 битов.

В DES последовательно использованы методы замены и перестановок. В настоящее время этот алгоритм считается неоправданно сложным и обладающим невысокой криптостойкостью.

Для оценки криптостойкости введено понятие абсолютной криптостойкости, которая по Шеннону определяется таким образом: "...если шифр получается путем наложения на открытый текст случайной и равновероятной гаммы, то такой шифр является абсолютно стойким "[6].

Однако, применение таких шифров ограничено из-за трудоемкости получения такой гаммы и проблемы хранения и распределения закрытых ключей.

На практике чаще используются комбинированные методы и алгоритмы.

В Росии был принят стандарт шифрования данных ГОСТ 28147-89 [5,120] с учетом мирового опыта и с учетом недостатков стандарта DES.

Этот стандарт предусматривает несколько режимов работы; во всех режимах используются ключ длиной 256 бит, представляемый в виде 8 ми 32 разрядных чисел $X(i): W = X(7)X(6)X(5)...X(2)X(1)X(0)$.

Для дешифрования используется тот же ключ. Режимы замены и подстановки имеет достаточно сложные алгоритмы; Сообщение разбиваются на блоки по 64 бита, а каждый блок Т также разбивается по 32 бита на блоки $A(0), B(0)$.

Алгоритм шифрования имеет вид:

- Для $i = 1,24; j = (i-1) \bmod 8 : A(i) = f(A(i-1)[+]X(j)) \oplus$ $\oplus B(i-1), B(i) = A(i-1).$
- Для $i = 25,31; j = 32 - i : A(i) = f(A(i-1)[+]X(j)) \oplus$ $\oplus B(i-1), B(i) = A(i-1).$
- Для $i = 32 : A(32) = A(31), B(32) = f(A(31)[+]X(0)) \oplus B(31).$

Блок шифровки имеет вид : $T(64) = A(32)B(32).$

Алгоритм в режиме гаммирования с обратной связью имеет вид: $Ш(1) = A(S) \oplus T(1) = Г(1) \oplus T(1), Ш(i) = A(Ш(i-1)) \oplus$ $\oplus T(i) = Г(i) \oplus T(i), i = 1, m,$

где $A(S)$ – синхроблок из 64 битовой последовательности, $Г(i)$ - последовательности гаммы из множества $Г_ш = (Г(1), Г(2), Г(3), ..., Г(m)).$

Последний алгоритм обладает очень высокой крипто - стойкостью.

В коммерческих системах (например, в банковских) для защиты информации используются алгоритмы шифрования с открытым ключом типа RSA.

Этот алгоритм основан на том факте, что разложение на множители произведения двух простых чисел (с учетом производительности современных вычислительных систем) практически невыполнимо.

Криптостойкость такой системы определяется нижней оценкой числа операции для раскрытия шифра и затрачиваемым на это машинным временем.

Такая система используется для работы с удаленными клиентами для обслуживания кредитных карточек.

Алгоритм RSA используется во многих стандартах; например: SSL,S-HHTP,S-MIME,STT,PCT,S/WAN.

Сущность алгоритма RSA заключается в следующем:

Пусть задан $n = p \times q,$ где $p, q -$ различные ( достаточно большие ) простые числа.

Выберем $e$ – простое относительно функции Эйлера - $\varphi(n)$, то существует некоторое целое $d$ такое, что $e \times d = 1(\mathrm{mod}\,\varphi(n))$; при этом, если $p, q -$ достаточно большие простые, то разложение $n -$ практически не осуществимо (на уровне современной вычислительной технологии ).

Практическое использование алгоритма такое; каждый пользователь выбирает два больших простых $(p, q)$ числа, которые генерируются при помощи генератора простых чисел.

Далее, в соответствии с вышеописанным алгоритмом выбирают два простых числа e и d; при этом, полученные совокупности - $(e, n)$ является открытым ключом, а $(d, n)$– закрытым.

Тексты шифруются с помощью открытого ключа, а расшифровка производится только с помощью закрытого ключа.

Криптостойкость системы определяется длиной ключа; например, при длине ключа 50, число операции раскрытия составляет $\sim 1{,}4 \bullet 10^{10}$.

При длине 200, число операции составляет $\sim 1{,}2 \bullet 10^{23}$, что не представляется возможным на уровне современной вычислительной технологии.

Для пользователей рекомендованы следующие модули n: - 768 bit - для частных лиц; 1024 bit – для коммерческой информации; 2024 bit - для особо секретной информации.

По сравнению с DES , для расшифровки RSA потребуется десятки тысяч раз больше времени .

Для цифровой подписи используется алгоритм Эль-Гамаля [7.71-75], который обеспечивает такую же криптостойкость. На основе алгоритма лежит дискретное логарифмирование.

Сущность алгоритма заключается в следующем;

Получатель секретной информации генерирует закрытый ключ - $a$ и подбирает параметры p , q – числа, p - простое, а q - целое; вычислив по алгоритму $y = q^a \bmod p$ , открытый ключ $y$, посылает адресатам (отправителям секретной информации).

Отправитель выбирает случайное число $к$, меньшее $p$ и по известному $y$ для открытого сообщения m вычисляет шифровку $y_{1,}y_2$ по алгоритму : $y_1 = q^k \bmod p$, $y_2 = m \oplus y^k$, которые отправляются получателю.

Получатель по закрытому ключу $a$, восстанавливает сообщение $m$: $m = \left(y_1^a \bmod p\right) \oplus y_2$.

В алгоритме цифровой подписи DSA , разработанный NIST (National Institute of Sytandard and Technology) используется расмотренный алгоритм [5.244].

В России аналогичный алгоритм введен для электронной подписи в ГОСТ Р 34.10 – 94 [7.70-75].

В реальных криптосистемах используются также системы на основе эллиптических уравнений вида:

$$y^2 = x^3 + ax + b \bmod p.$$

Алгоритм Диффи- Хелмана является весьма эффективным, который дает возможность пользователям обменяться ключом [5. 216, 6.335].

В алгоритме используется функция дискретного возведения в степень.

Принцип алгоритма заключается в следующем; пусть задан поле Галуа из P элементов ( P- либо простое, либо простое в любой степени); процесс вычисления логарифмов в таких полях является трудоемкой задачей.

Если $y = \alpha^x, 1 \langle x \langle p - 1$, где $p$ - фиксированный элемент поля $GF(p)$ и если $p$ выбрано правильно, то извлечение логарифма потребует вычислении пропорциональных:

$$L(p) = \exp\{\lambda np \times \lambda n \times \lambda np)^{0,5}\}.$$

Ключ $K_{12}$ вычисляется двумя абонентами; они посылают друг другу сообщения такого типа: $y_1 = \alpha^{x_1}, y_2 = \alpha^{x_2}$, затем каждый из них возводит в степень $x_1, x_2$, полученные по каналу значения $y_1, y_2$ , т.е. $y_1^{x_2}, y_2^{x_1}$.

Таким образом, оба абонента будут иметь обший ключ:

$K_{12} = y_1^{x_2} = \alpha^{x_1 x_2}, k_{12} = y_2^{x_1} = \alpha^{x_2 x_1}$.

Для 1000 битных простых чисел для вычисления в поле Галуа потребуется около $10^{30}$ операции.

Стандарт цифровой подписи DSS (Digital Signature Standard) создан на основе защитного алгоритма хэширования SHA (Sekure Hash Algorithm) [7. 380].

Алгоритм цифровой подписи DSA создан на основе трудности вычисления дискретных логарифмов; наиболее часто используется алгоритм предложенный Эль-Гамалем и Шнорром [7,383].

Три параметра p, q, g открытого ключа являются известными группе пользователей; выбирается 160 -битное простое число q ( простой делитель (p-1)). Далее, выбирается простое число p длиной между 512 и 1024 бит с шагом 64 бит; целое число g выбирается из выражения:

$$g = h^{\frac{(p-1)}{q}} \bmod p \rangle 1, 1 \langle h \langle (p-1).$$

Имея эти числа каждый пользователь генерирует свой личный (секретный) ключ x (случайное или псевдослучайное число, $1 \langle x \langle (q-1)$ ) и открытый ключ y (вычисляется по $y = g^x \bmod p$ ).

Перед каждой подписью генерируется некоторое уникальное целое случайное или псевдослучайное число $k(0 \langle k \langle q-1)$; далее, вычисляются s , r , которые и образуют подпись; при этом , их значения вычисляются по формулам: $r = (g^x \bmod p) \bmod q$ , $s = [k^{-1}(H(M) + xr)] \bmod q$.

При малейшем изменений текста верификация подписи обнаружит “подделку”. Алгоритм верификации таков:

$w = (s')^{-1} \bmod q$; $u_1 = [H(M') \times w] \bmod q$; $u_2 = (r') \times w \bmod q$;

$v = [(g^{u_1} \times y^{u_2}) \bmod p] \bmod q$.

Если $v = r'$ ,то подпись считается подлинной; в противном случае, подделанной.

В алгоритме цифровой подписи применненный в стандарте СТБ-1176.02-99 в качестве метки используются моменты времени подписания документов, что значительно повышает имитостойкость подписи; при этом, даже сам автор не имеет возможность подделки собственной подписи, имея при себе все ключи [8.4-9].

Составленная на основе этого алгоритма лабораторная работа в настоящее время используется в учебном процессе для студентов специальностей Информатика и Сети телекоммуникаций.

Для учебных целей можно использовать комплекс программ “Криптоцентр”[приложение работы 7], который содержит демоверсии криптографических программ для электронной подписи документов, для криптографической шифровки и хранения документов в базах данных и для шифровки перед отправкой данных по каналам связи.

Эти программы не гарантируют высокую криптостойкость.

Лицензионные версии программ обладают высокой криптостойкостью и надежностью; их можно эффективно использовать для скрытной передачи документов в системах телекоммуникации, для скрытного хранения и для электронной подписи документов.

Эти программы могут быть применены при построении Электронного Правительства, а нелицензионные версии могут быть использованы в качестве учебно-методического материала в вузах соотвествующих специальностей.

## *Литература*


1. ЗАКОН РЕСПУБЛИКИ КАЗАХСТАН, *«Об электронных документах и об электронной подписи»,* №371 11 ЗРК, Астана, 3.01.2003.
2. ТУКУБАЕВ З.Б. *Методы и алгоритмы защиты компьютерной информации "Электронного Правительства".* Элект. конф. УБС НИИ ИПУ РАН, www.mtas.ru , 2012
3. ТУКУБАЕВ З.Б. *Моделирование СПДИ с поблочной передачей с накоплением в условиях преднамеренных помех.Тезисы докл. ОНТК "По проблемам распространения радиоволн*", НИИССУ.-М.: 1986 г.
4. МАРТИН ДЖ. *Вычислительные сети и распределенная обработка данных,* - М., Финансы и статистика,1986.
5. ВИЛЬЯМ СТОЛЛИНГС. *Криптография и защита сетей,* изд. дом «Вильямс», - М.-Л.-Киев,2001,-672 с.
6. КЛОД ШЕННОН. *Теория связи в секретных системах*. В кн. «Работы по теории информации и кибернетике».- М.,ИИЛ,1963, -333-369с.
7. МАСЛЕННИКОВ М. *Практическая криптография*, С.-Петербург», БХВ-Петербург», 2003.-464 с.
8. ГОЛИКОВ В.Ф. И ДР. *Криптографическое кодирование информации.* Метод.указания по дисциплине"Криптографическая защита информации в телекоммуникациях".Ч.3 : Электронная цифровая подпись. –Мн.: БГУИР, 2003 г.



**Tukubaev ZuhirxanBeysekovich**, A.Kuatbekov Friendship University, Kazakhstan, Shimkent, Doctor of science, (tukubaev1945@mail.ru).

**Tukubaev Aziz Zuhirxanovich,** Kazakhstan, Almati, Doctor of science.

**Turtaev M.R. (Candidate of Economic Sciences, Professor, Peoples' Friendship University named after Academician A.Kuatbekov)**

**Suleimenovaa B.S. (Master's degree , senior lecturer at the Peoples' Friendship University named after akad.A.Kuatbekova),**

# CRYPTOGRAPHIC METHODS AND ALGORITHMS FOR PROTECTING COMPUTER INFORMATION

*The article analyzes the methods and algorithms of computer information protection in the construction of "Electronic Government"*

Keywords: confidentiality, absolute cryptographic strength of the cipher, encrypted message, equally probable gamma, electronic document flow, electronic signature. Codes JEL 81.93.29