16. Большанин Г.А., Большанина Л.Ю. Использование теории восьмиполюсников для анализа передачи электрической энергии // Там же. С. 132-136.

17. Большанин Г.А., Большанина Л.Ю. Определение вторичных параметров однородного участка трехпроводной линии электропередачи методом восьмиполюсника // Современные технологии. Системный анализ. Моделирование. 2013. № 2 (38). С. 232-237.

18. Большанин Г.А., Большанина Л.Ю. Определение первичных параметров однородного участка трехпроводной линии электропередачи методом восьмиполюсника // Воздушные линии. 2013. № 2 (11). С. 8-14.

19. Большанин Г.А., Большанина Л.Ю. Восьмиполюсники как элементы трехфазной трехпроводной линии электропередачи // Главный энергетик. 2013. № 5. С. 19-25.

References

1. Bolshanin G.A. Ten R.V., Plotnikov M.P. Load matching with an electric network for improving electric energy quality // Trudy Bratskogo gosudarstvennogo universiteta. Ser. Estestvennye i inzhenernye nauki. 2008. No. 2. P. 92-95.

2. Bolshanin G. A. Features of transportation of electric energy on three-wire power lines // Trudy Bratskogo gosudarstvennogo universiteta. Ser. Estestvennye i inzhenernye nauki. 2010. Vol. 2. P. 64-68.

3. Kozlov V.A., Bolshanin G.A. Matched operating mode of homogeneous three-wire high-voltage line as a means of increasing the working reliability of hydroelectric power station // Bratskaja GES: istorija stroitelstva, opyt ekspluatacii, perspektivy: Tr. Vseros. nauch.-prakt. konf. Bratsk, 2011. P. 77-81.

4. Bolshanin G.A, Bolshanina L.Yu., Maryasova E.G. Electric power line as an object of systems analysis // Materialy VII Miedzynarodowej naukowi-praktycznei konferencje konferencji «Perspektywiczne opracowania sa nauka I technikami – 2011» Vol. 55. Techniczne nauki.: Przemysl. Nauka I studia. P. 103-105.

5. Bolshanin G.A. Bolshanina L.Yu. Features of electric energy distribution on three-wire power line // Sovremennye tehnologii. Sistemnyj analiz. Modelirovanie. 2010. No. 4 (28). P. 197-204.

6. Bolshanin G.A. Distribution of electric energy on sections of electrical power systems: monograph. 2 vol. Bratsk: BrGU, 2006. 807 p.

7. Bolshanin G.A., Bolshanina L.Yu. Three-wire high voltage line parameters. Method of eight-terminal circuit. Bratsk: Izd-vo BrGU, 2012. 259 p.

8. Bolshanin, G.A., Bolshanina L.Yu. Distribution of electric energy of the lowered quality on a three-phase three-wire main power line. // Vestn. Izhev. gos. tehn. un-ta. 2008. № 3 (39). P. 130-134.

9. Bolshanin G.A. Bolshanina L.Yu. Maryasova E.G. Features of electric energy distribution on multiwire power lines // Trudy Bratskogo gosudarstvennogo universiteta. Ser. Estestvennye i inzhenernye nauki. 2011. Vol. 2. P. 38-43.

10. Bolshanin G.A. Distribution of electric energy of the lowered quality on sections of electrical power system // Trudy Bratskogo gosudarstvennogo universiteta. Ser. Estestvennye i inzhenernye nauki. 2006. Vol. 2. P. 129-140.

11. Bolshanin G.A., Bolshanina L.Yu. Three-wire high voltage line parameters. Method of eight-terminal circuit. Bratsk: Izd-vo BrGU, 2012. 259 p.

12. Bolshanin G.A., Bolshanina L.Yu. Determination of coefficients of eight-terminal circuit replacing three-wire high voltage line // Mezdunarodnyj naucno-issledovatelskij zurnal. 2012. No. 6 (6). P. 38-41.

13. Bolshanin G.A., Bolshanina L.Yu. Dedetermination of coefficients of eight-terminal circuit replacing three-phase three-wire power line // Elektrotehnicheskie kompleksy i sistemy upravlenija. 2013. № 1 (29). 2013. P. 41-46.

14. Bolshanin G.A. Bolshanina L.Yu. Three-wire power line elements in the multiterminal circuit theory // Materiály IX mezinárodní vědecko-praktická konference «Moderni vymoženosti věda – 2013» – Díl 76. Technické vědy: Praha. Publishing House «Education and Science» s.r.o. P. 24-28.

15. Bolshanin G.A., Bolshanina L.Yu. Way of determination of eight-terminal circuit coefficients replacing a three-phase three-wire power line // Trudy Bratskogo gosudarstvennogo universiteta. Ser. Estestvennye i inzhenernye nauki. 2012. Vol. 3. P. 136-145.

16. Bolshanin G.A., Bolshanina L.Yu. Use of eight-terminal circuit theory for analyzing electric energy transfer // Trudy Bratskogo gosudarstvennogo universiteta. Ser. Estestvennye i inzhenernye nauki. 2012. Vol. 3. P. 132-136.

17. Bolshanin G.A., Bolshanina L.Yu.. Determination of secondary parameters of a homogeneous section of a three-wire power line by using the method of eight-terminal circuit. // Sovremennye tehnologii. Sistemnyj analiz. Modelirovanie. 2013. No. 2 (38). P. 232-237.

18. Bolshanin G.A., Bolshanina L.Yu. Determination of primary parameters of a homogeneous section of a three-wire power line by using the method of eight-terminal circuit. // Vozdushnye linii. 2013. № 2 (11). P. 8-14.

19. Bolshanin G.A,. Bolshanina L.Yu. Eight-terminal circuits as elements of a three-phase three-wire power line // Glavnyj energetik. 2013. № 5. P. 19-25.

УДК 003.26; 004.056

IT-технологии в вопросах обеспечения информационной безопасности предприятий

М.Ю. Иванов

Братский государственный университет, Макаренко 40, Братск, Россия
nis@brstu.ru
Статья получена 16.12.2013, принята 17.02.2014

Представлены результаты исследований базовых математических и алгоритмических аспектов симметричных и асимметричных криптографических преобразований на примере шифров RC4 и Эль-Гамаля, а также выработки и проверки электронной цифровой подписи. Рассмотрен спектр интересов субъектов информационных отношений с привязкой к категориям информационной безопасности. Проанализированы достоинства и недостатки симметричных и асимметричных методов криптографии. Приведены фрагменты кода, описывающего глобальные переменные, массив данных, заполнение массива и функцию, реализующую шифрование байта исходной информации с помощью шифра RC4. Предложен эффективный криптоалгоритм, надежность которого обусловлена сложностью вычислений дискретных логарифмов, с описанием процесса шифрования и дешифрования текста, генерации пары ключей, вычисления открытого ключа и формирования цифровой подписи с последующей ее верификацией. Показана возможность автоматизированного шифрования текстовых данных на основе дискретного логарифмирования и формирования электронной цифровой подписи, являющейся эффективным средством подтверждения подлинности и авторства информации в электронной форме.

Ключевые слова: информационная безопасность, шифрование, симметричные и асимметричные криптографические системы, электронная цифровая подпись, программное обеспечение.

IT-technologies in enterprise information security matters

M.Y. Ivanov

Bratsk State University, 40 Makarenko St., Bratsk, Russia
nis@brstu.ru
Received 16.12.2013, accepted 17.02.2014

The research results for basic mathematical and algorithmic aspects of symmetric and asymmetric cryptographic transformations in terms of RC4 cipher and ElGamal encryption system, as well as development and verification of electronic digital signature have been shown in the article. The spectrum of the interests of the subjects of information relations with reference to information security categories has been examined. The advantages and disadvantages of symmetric and asymmetric cryptographic methods have been analyzed. There have been given code fragments representing the global variables, data array, data array filling and the function in which the encryption of byte input information is implemented with the help of RC4. An effective cryptoalgorithm has been proposed. Its reliability is caused by complex calculating of discrete logarithms with the description of the text encryption and decryption processes, of key pair generating, public key computing and digital signature creating with its subsequent verification. The possibility of automated encryption of text data based on the discrete logarithm problem, and of creating the digital signature as an effective tool for confirming the information authenticity and authorship in electronic form have been presented.

Keywords: information security, encryption, symmetric and asymmetric cryptographic systems, electronic digital signature, software.

Введение. В настоящее время защита персональных данных является сложной и трудноразрешимой задачей для создателей информационных систем. Существует множество субъектов (независимых от государства юридических лиц), занимающихся автоматизированным сбором, обработкой и хранением информации (в частности, социально-экономического характера), вследствие чего процессы ее копирования, распространения и использования существенно упрощаются.

Наиболее мощным средством обеспечения информационной безопасности является криптографическое преобразование (шифрование) данных. Шифрование занимает центральное место среди программно-технических средств защиты, являясь не только основой реализации многих из них, но и последним, а подчас и единственным методом защиты. Например, только шифрование позволяет обеспечить конфиденциальность данных персональных ЭВМ даже в случае их кражи.

Немаловажным аспектом при обеспечении информационной безопасности предприятий является и автоматизация процесса криптографического преобразования (шифрования) данных, поскольку использование современных информационных технологий [1, 2] способствует повышению эффективности любой сферы деятельности, в том числе и защиты данных.

Теоретические основы криптографии. Известно, что все существующие сегодня методы криптографического преобразования (шифрования) информации подразделяются на симметричные и асимметричные (двухключевые) и имеют, соответственно, свои достоинства и недостатки.

Так, симметричные системы лучше изучены, представлены в большом количестве специализированной литературы, отличаются меньшей длиной ключа (при вполне сопоставимой с асимметричным шифрованием стойкости), более простыми операциями по преобразованию данных, что позволяет в случае необходимости легко модифицировать криптоалгоритм и снизить длительность процесса шифрования информации.

В качестве недостатка симметричных методов шифрования можно отметить сложность обмена и управления ключами. После каждой передачи зашифрованного сообщения ключ необходимо обновлять, для чего требуется дополнительный защищенный канал связи.

Использование асимметричных методов шифрования предполагает более надежную защиту информации, при этом пару ключей можно не обновлять значительное время и нет необходимости передавать получателю сообщения один из ключей. Вместе с тем, для реализации асимметричных криптоалгоритмов нужны ключи значительно большей длины (ключ длиной 512 битов обеспечивает аналогичную защиту информации, как и при использовании ключа длиной всего 64 бита при симметричном шифровании), из-за чего снижается скорость шифрования сообщения. Надежность асимметричного шифрования информации нивелируется тем, что сам факт передачи зашифрованного сообщения позволяет установить местонахождение как отправителя, так и получателя.

Таким образом, основным недостатком симметричного шифрования является то, что секретный ключ должен быть известен и отправителю, и получателю. С одной стороны, получатель на основании наличия зашифрованного и расшифрованного сообщения не может доказать, что получил это сообщение от конкретного отправителя, поскольку такое же сообщение он мог сгенерировать самостоятельно. С другой стороны, если стороны не доверяют друг другу, совместная выработка секретных ключей невозможна.

Существенный недостаток асимметричных методов шифрования – их низкое быстродействие (в 3…4 раза медленнее симметричных методов). В связи с этим на практике часто пользуются комбинированными криптосистемами. Например, для решения задачи эффективного шифрования с передачей секретного ключа, использованного отправителем, сообщение сначала симметрично зашифровывают случайным ключом, затем этот ключ зашифровывают открытым асимметрич-

ным ключом получателя, после чего сообщение и ключ отправляются по сети получателю [3].

Следует отметить, что единого, подходящего для всех случаев способа шифрования информации нет, поскольку выбор криптографической системы зависит от особенностей информации, ее ценности и возможностей ее владельцев.

Так, государственные, военные тайны должны храниться десятилетиями, а некоторые (например, биржевые сводки) можно разгласить уже через несколько часов ввиду утраты ими своей актуальности.

Практическая реализация методов криптографии. Наиболее известным симметричным шифром является RC4 (англ. Ron's Code 4, или Rivest's Cipher 4), разработанный в 1987 г. Роном Ривестом для компании RSA Data Security Inc. Шифр RC4 крайне прост в реализации, характеризуется переменной длиной ключа, высокими быстродействием и криптостойкостью. В течение первых семи лет существования этот шифр лицензировался компанией RSA Data Security Inc. только на условиях неразглашения. Однако в 1994 г. RC4 был анонимно опубликован в глобальной сети Интернет, и с тех пор шифр стал доступен для независимого криптоанализа. Тем не менее, до сих пор не известен ни один случай успешной атаки на него.

Шифр RC4 входит в спецификацию стандарта CDPD (сотовая пакетная передача данных), а также в «туннельный» защищенный протокол «точка-точка» PPTP.

Криптопреобразования по алгоритму RC4 могут быть описаны на языке программирования Object Pascal (среда разработки Borland Delphi) следующим образом:

```
procedure RC4Init(key: shortstring);
var
k: array[0..255] of byte;
i, j, t : byte;
begin
rc4i:= 0;
rc4j:= 0;
for i:= 0 to 255 do rc4s[i]:= i;
j:= 0;
t:= length(key);
for i:= 0 to 255 do begin
inc(j);
k[i]:= Byte(key[j]);
if j= t then j:= 0;
end;
j:= 0;
for i:= 0 to 255 do begin
j:= (j + k[i] + rc4s[i]) mod 256;
t:= rc4s[i];
rc4s[i]:= rc4s[j];
rc4s[j]:= t;
end;
end;
```

Данный фрагмент кода описывает глобальные переменные: *rc4i*, *rc4j* типа *byte*, массив *rc4s: array[0..255] of byte* и заполнение массива.

Функция, реализующая шифрование байта исходной информации, следующая:

```
function RC4GetCryptoByte(ch: byte): byte;
var t: byte;
begin
rc4i:= (rc4i + 1) mod 256;
rc4j:= (rc4j + rc4s[rc4i]) mod 256;
t:= rc4s[rc4i];
rc4s[rc4i]:= rc4s[rc4j];
rc4s[rc4j]:= t;
t:= (rc4s[rc4i] + rc4s[rc4j]) mod 256;
RC4GetCryptoByte:= rc4s[t] xor ch;
end;
```

В первой строке кода значение *rc4i* циклически увеличивается на единицу. Если значение стало равным 255, то оно обнуляется. Во второй строке значение счетчика *rc4j* изменяется в зависимости от массива *rc4s*, который, в свою очередь, зависит от ключа. Далее элементы массива с порядковыми номерами *rc4i* и *rc4j* меняются местами. Затем определяется номер элемента, который складывается по модулю 2 (реализация функции XOR) с байтом исходного текста. Шифр RC4 является симметричным, поэтому дешифрование сообщения выполняется аналогично процессу шифрования [4].

Поскольку асимметричное шифрование данных производится достаточно медленно, на практике в криптосистемах используется быстрое и надежное симметричное преобразование информации по схеме с ключом сеанса. А вот сам ключ сеанса шифруется асимметричным криптоалгоритмом с помощью открытого ключа получателя сообщения. Такая система характеризуется всеми положительными свойствами асимметричного шифрования и в то же время очень высоким быстродействием [5].

В отличие от симметричных алгоритмов, в которых процесс дешифрования легко восстанавливается по процедуре шифрования и, наоборот, в схеме криптопреобразования с открытым ключом, зная алгоритм шифрования, вычислить процедуру дешифрования невозможно. Более того, длительность таких вычислений настолько велика, что реализовать их на любых современных ЭВМ также невозможно.

В настоящее время получение и отправка сообщений по компьютерным сетям включает в себя не только пользование услугами электронной почты, но и обмен данными, побуждающими людей к определенным действиям, таким, как передача банковских фондов, автоматизированная продажа акций, авиабилетов, бронирование гостиничных номеров, безналичная оплата услуг и т. д., и т. п. Участники подобного информационного обмена нуждаются в защите от множества злонамеренных действий, к которым можно отнести:

1) отказ (ренегатство) отправителя от переданного им ранее сообщения;

2) фальсификацию (подделку) сообщения получателем;

3) внесение получателем изменений в сообщение;

4) маскировку злоумышленника под другого пользователя.

Эффективным способом решения перечисленных выше проблем является использование электронной цифровой подписи (далее – ЭЦП) (англ. Electronic digital signature).

Назначение ЭЦП заключается в следующем: она должна гарантированно подтвердить подлинность информации, содержащейся в электронном документе, а также неопровержимо доказать третьей стороне (партнеру по бизнесу, аудитору, арбитражному суду), что электронный документ был составлен именно конкретным лицом или по его поручению и именно в том виде, в котором он предъявлен.

ЭЦП, представляющая собой последовательность символов, полученную в результате криптографического преобразования электронного сообщения, добавляется к блоку данных и позволяет получателю проверить источник отправления, целостность данных, а также защититься от подделки. Иначе говоря, ЭЦП используется в качестве аналога собственноручной подписи полномочного лица.

На сегодняшний день целям выработки и проверки ЭЦП служат методы асимметричного шифрования.

Пусть $E(T)$ обозначает результат шифрования текста T с помощью открытого ключа, а $D(T)$ – результат дешифрования текста T, зашифрованного с помощью секретного ключа. Чтобы применить асимметричный метод шифрования для реализации ЭЦП, необходимо выполнить тождество $E(D(T)) = D(E(T)) = T$.

Процедура выработки ЭЦП заключается в шифровании с помощью преобразования D дайджеста $h(T)$ (рис. 1). Проверка ЭЦП может быть реализована по схеме, представленной на рис. 2.

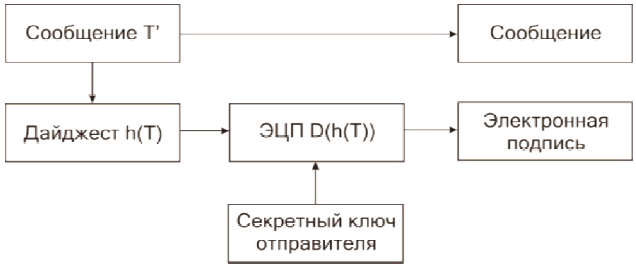

Рис. 1. Выработка электронной цифровой подписи

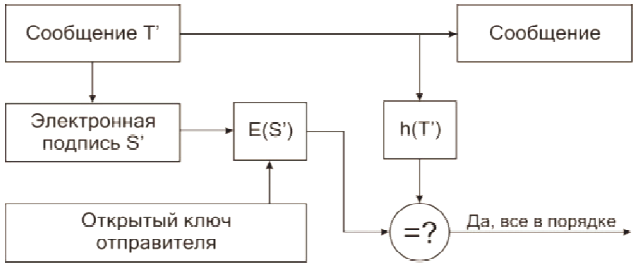

Рис. 2. Проверка электронной цифровой подписи

Из равенства $E(S') = h(T')$ следует, что $S' = D(h(T'))$. Для доказательства достаточно применить к частям равенства преобразование D и отбросить в левой части тождественное преобразование $D(E(T))$. Таким образом, ЭЦП защищает целостность сообщения и удостоверяет личность отправителя.

Одной из причин популярности использования для выработки ЭЦП именно асимметричных алгоритмов шифрования является наличие в них открытого ключа. Свой открытый ключ можно послать любому адресату непосредственно перед отправкой ему подписанного сообщения или, что еще проще, разместить такой ключ в каком-либо информационном ресурсе сети Интернет. Но при этом, однако, возникает вероятность элементарной подмены открытых ключей.

Так, два пользователя создали по паре ключей (секретный и открытый) и обменялись открытыми ключами. Злоумышленник в процессе этого обмена может перехватить один из отправленных открытых ключей (причем, сделать это таким образом, что до получателя ключ так и не дойдет), прочитать фамилию отправителя и создать затем новую пару ключей, записав туда сведения об отправителе. Секретный ключ злоумышленник оставит у себя, а открытый пошлет получателю от имени отправителя. После этого злоумышленник сможет посылать любые письма, а подпись отправителя под его ложными сообщениями получатель будет считать верной до тех пор, пока подлог не станет явным. В электронной коммерции, например, такая ситуация может привести к катастрофическим последствиям. Сегодня наиболее распространенным способом борьбы с подменой открытых ключей является их сертификация.

Генерацию ЭЦП осуществляют с помощью общеизвестных асимметричных криптоалгоритмов (например, Ривеста-Шамира-Адльмана, Эль-Гамаля), специфицированных для стандартов ЭЦП типа DSA (Digital Signature Algorithm).

Тагир Эль-Гамаль в 1984 г. предложил алгоритм цифровой подписи EGSA на основе дискретного логарифмирования. Он позволяет повысить стойкость подписи, например, при ключах длиной 64 байта, приблизительно в 1000 раз (при такой длине ключей обеспечивается уровень стойкости порядка 10^{21}). Отечественный аналог EGSA под названием «Нотариус-1» был разработан в России в 1992 г.

Алгоритм Эль-Гамаля послужил основой для принятия нескольких стандартов ЭЦП, которую невозможно подделать за приемлемое время, в том числе национальных стандартов США и государственных стандартов информационной безопасности Российской Федерации.

Российским аналогом описанных выше алгоритмов является ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма», регламентирующий вычисление дайджеста и реализацию ЭЦП.

Как уже отмечалось, криптостойкость алгоритма Эль-Гамаля обусловлена сложностью вычислений дискретных логарифмов. Поэтому с учетом механизма его реализации можно предложить способ шифрования текстовой информации и выработки ЭЦП.

Так, для генерации пары ключей сначала берется простое число p и два случайных числа g и x, каждое из которых меньше p. Затем вычисляется открытый ключ $y = g^x \bmod p$. Здесь y, g и p – общедоступные ключи, а секретным ключом является x. Для подписи сообщения M выбирается случайное число k, простое по отношению к $p - 1$. После этого вычисляется число $a = g^k \bmod p$. Далее из уравнения $M = (x \cdot a + k \cdot b) \bmod (p - 1)$ находится значение числа b. Электронной подписью для сообщения M будет служить пара чисел a и b. Случайное число k является

секретным. Верификацией подписи служит проверка равенства $y^a \cdot a^b \bmod p = g^M \bmod p$.

Пара чисел a и b представляет собой зашифрованный текст. Следует заметить, что зашифрованный текст имеет размер в два раза больше исходного. Дешифрование сообщения осуществляется по формуле $M = b/a^x \bmod p$.

Описанный алгоритм был реализован с помощью среды программирования Microsoft Visual C++ Standard Edition [6].

Главные формы разработанной программы для ЭВМ представлены на рис. 3 и 4. В окне генерации открытых ключей указывается их длина (поле «Keysize»), поле «Number Base» служит для выбора системы счисления, а поле «Passphrase» – для ввода секретного ключа (рис. 4).

В поле «Message» окна шифрования текстовой информации (рис. 4) указывается сообщение, шифруемое с помощью кнопки «Encrypt». Кнопка «Decrypt» присоединяет к сообщению цифровую подпись.

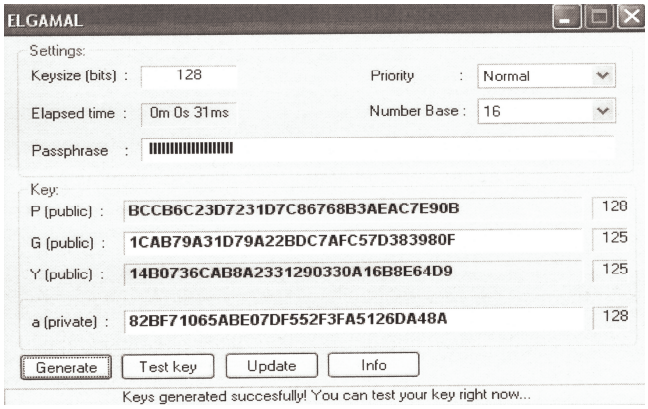

Рис. 3. Окно генерации открытых ключей

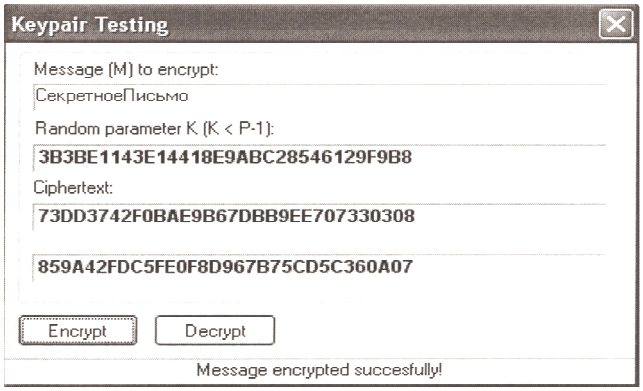

Рис. 4. Окно шифрования текстовой информации

Следует отметить, что процедура подписывания не позволяет вычислять цифровые подписи под новыми сообщениями без знания секретного ключа.

Невозможность восстановления ключа подписывания по ключу проверки и любому количеству подписанных электронных документов гарантируется использованием указанных выше процедур, так что практическое восстановление ключей подписи по ключам проверки требует решения непростой вычислительной задачи.

Таким образом, разработанная программа для ЭВМ для шифрования и формирования ЭЦП является эффективным средством подтверждения подлинности и авторства текстовой информации в электронной форме.

Заключение

В работе рассмотрены теоретические основы симметричных и асимметричных методов криптографии и электронной цифровой подписи. С учетом рекомендаций российских и зарубежных нормативных документов предложен эффективный криптоалгоритм, надежность которого обусловлена сложностью вычислений дискретных логарифмов. Разработана программа для ЭВМ для шифрования текстовых данных, хранящихся на незащищенных носителях или пересылаемых по ненадежным каналам связи, и выработки электронной цифровой подписи.

Литература

1. Иванов М.Ю. Структура и принципы функционирования экспертных систем для оценки деятельности хозяйствующего субъекта // Проблемы социально-экономического развития Сибири. 2012. № 3 (9). С. 18-22.

2. Иванов М.Ю. Экспертные системы для оценки деятельности хозяйствующего субъекта // Там же. С. 23-27.

3. Иванов М.Ю. Шифрование текстовой информации методом возведения целых чисел в большие степени по модулю CipherTextStepMod v. 1.1: программа для ЭВМ. Св. ГР. № 2012613807 Рос. Федерация; зарег. в реестре Федер. службы по интеллектуальной собственности, пат. и товарным знакам 23.04.2012.

4. Иванов М.Ю. Шифрование текстовой информации методом блочных перестановок CipherTextBlock v. 1.1: программа для ЭВМ. Св. ГР. № 2010615864 Рос. Федерация; зарег. в реестре Федер. службы по интеллектуальной собственности, пат. и товарным знакам 08.09.2010.

5. Иванов М.Ю. Шифрование текстовой информации методом замены блоков CiphTextBlock v. 1.1: программа для ЭВМ. Св. ГР. № 2012613808 Рос. Федерация; зарег. в реестре Федер. службы по интеллектуальной собственности, пат. и товарным знакам 23.04.2012.

6. Иванов М.Ю., Ивахтин М.А., Ремизов И.А. Шифрование текстовой информации на основе дискретного логарифмирования CipherText v. 1.1: программа для ЭВМ. Св. ГР. № **2008614025** Рос. Федерация; зарег. в реестре Федер. службы по интеллектуальной собственности, пат. и товарным знакам 25.08.2008.

References

1. Ivanov M.Yu. The structure and principles of expert systems functioning to evaluate economic entity activity // Problemy sotsialno-economicheskogo razvitia Sibiri. 2012. № 3 (9). P. 18-22.

2. Ivanov M.Yu. Expert systems for economic entity activity assessment // Problemy sotsialno-economicheskogo razvitia Sibiri. 2012. № 3 (9). P. 23-27.

3. Ivanov M.Yu. Text information encryption by method of integers involution to a large power, modulo CipherTextStepMod v. 1.1: PC program. Ownership Certificate № 2012613807 Rus. Federation; reg. in Federal Service for Intellectual Property, Patents and Trademarks 23.04.2012.

4. Ivanov M.Yu. Text information encryption by block permutations method CipherTextBlock v. 1.1: PC program. Ownership Certificate № 2010615864 Rus. Federation; reg. in Federal Service for Intellectual Property, Patents and Trademarks 08.09.2010.

5. Ivanov M.Yu. Text information encryption by replacing blocks method CiphTextBlock v. 1.1: PC program. Ownership Certificate № 2012613808 Rus. Federation; reg. in Federal Service for Intellectual Property, Patents and Trademarks 23.04.2012.

6. Ivanov M.Yu., Ivakhtin M.A., Remizov I.A. Text information encryption based on the discrete logarithmization CipherText v. 1.1: PC program. Ownership Certificate № 2008614025 Rus. Federation; reg. in Federal Service for Intellectual Property, Patents and Trademarks 25.08.2008.

УДК 662.613

Оценка эффективности технологий утилизации энергии уходящих газов котлов, включающей теплоту конденсации водяных паров

В.К. Елсуков

Братский государственный университет, ул. Макаренко 40, Братск, Россия
elswk@mail.ru
Статья поступила 16.12.2013, принята 19.02.2014

На основе анализа литературных данных, исследований, проведенных авторам лично и с магистрантами, рассматриваются технологии утилизации энергии уходящих газов котлов, включающей теплоту конденсации водяных паров. Задачами исследований являются определение наиболее эффективных технологий указанной утилизации и уточнение условий их применения. Выделяются следующие проблемы внедрения рассматриваемых технологий: опасность ухудшения санитарно-гигиенического и технологического качества нагреваемой воды в контактных теплообменниках либо приобретение сильных коррозионных свойств конденсатом, выделившимся из газов на поверхностных теплообменниках; сложность и не всегда высокая надежность схем подсушки дымовых газов после теплоутилизатора; различие и сложность методик расчета теплоутилизаторов дымовых газов с конденсацией водяных паров. Предлагаются пути решения указанных проблем. Кратко указываются ошибки в существующих методиках теплового расчета различных теплообменных аппаратов в рассматриваемых технологиях. Показана высокая экономическая эффективность внедрения технологий утилизации энергии уходящих газов, включающей теплоту конденсации водяных паров, на теплоисточниках, работающих как на природном газе, так и на буром угле. Рассмотрены и описаны условия эффективного применения этих технологий. Отмечена необходимость дальнейших исследований по уточнению значений коэффициентов теплопередачи в контактных экономайзерах и поверхностных теплообменниках (при конденсации водяных паров).

Ключевые слова: энергосбережение, технологии, теплоэлектроцентраль (ТЭЦ), котельная, контактный экономайзер, теплообменник поверхностного типа, конденсация водяных паров.

Efficiency assessment of utilization technologies of boiler’s exit gas energy including heat of steam condensation

V.K. Elsukov

Bratsk State University, 40 Makarenko St, Bratsk, Russia
elswk@mail.ru
Received 16.12.2013, accepted 19.02.2014

Utilization technologies of boiler's exit gas energy including heat of steam condensation have been considered using the analysis of the published data and the investigations made by the author of this article personally and in collaboration with Master students. The objectives of the study are the detection of the most effective technologies for the mentioned utilization and the specification of their application conditions. The following problems of implementation of the technologies have been emphasized: the danger of deteriorating sanitary hygienic and technological quality of heated water in contact heat exchangers; acquisition of strong corrosive properties by the condensate released from the surface heat exchangers gas; complexity and not always high reliability of the flue gases drying schemes after the heat recovery; the difference and complexity of calculation methods of flue gas heat recovery with water vapor condensation. The ways to solve these problems have been suggested. The errors of existing methods of various heat exchangers' thermal calculation in these technologies have been shown briefly. High economic efficiency of utilization technologies of energy exit gases including the heat of water vapor condensation on the heat sources operating on both natural gas and lignite has been demonstrated. The conditions of effective application of these technologies have been examined and described. The need for further research to clarify the values of heat transfer coefficients in the contact economizers and surface heat exchangers (in presence of the water vapor condensation) has been highlighted.

Keywords: energy saving, technologies, combined heat-and-power plant, boiler house, contact economizer, surface-type heat exchanger, condensation of water steam.

Введение. Снижение потерь тепла с уходящими газами может быть наиболее значимым энергосберегающим мероприятием на энергоисточниках, использующих органическое топливо. Возможный выигрыш энергии возрастает в разы, если включает в себя теплоту конденсации водяных паров, содержащихся в дымовых газах. Технологии утилизации энергии уходящих газов котлов, включающей теплоту конденсации водяных паров (далее – технологии утилизации тепла уходящих газов с конденсацией водяных паров), предполагают использование теплообменников контактного либо поверхностного типов, в которых температура