Для того чтобы получить кандидата на r, надо округлить $\frac{d}{q}$ до ближайшего числа, кратного $\frac{1}{p-1}$, затем разделить по модулю $p-1$ на $\frac{(p-1)c-\{(p-1)c\}_q}{q}$. Сложность этого алгоритма оценивается как $O(n^3)$. В то же время лучший классический алгоритм для дискретного логарифма имеет сверхполиномиальную сложность.

Заметим также, что существует[6] вариант алгоритма Шора для группы точек эллиптической кривой над полем GF(p), обладающий сложностью $O(n^3)$, а также высказывается гипотеза, что аналогичный алгоритм существует и для эллиптических кривых над другими полями.

Несмотря на большие успехи, которых достигла криптология, необходимо отметить, что появление действующих образцов квантовых компьютеров приведет к тому, что многие криптосистемы, прежде всего асимметричные, станут нестойкими, что приведет к невозможности использования асимметричных криптосистем и, следовательно, к невозможности безопасного предоставления многих услуг, в том числе интернет-банкинга и электронной торговли. Перестанут быть безопасными электронные подписи и схемы распределения ключей. Из этого следует, что уже сейчас необходимо разрабатывать новые асимметричные криптоалгоритмы.

Симметричные алгоритмы шифрования останутся стойкими, но эффективная длина ключа таких алгоритмов уменьшится в 2 раза. Этот эффект следует учитывать при построении систем обработки информации уже сейчас.

---

[1] ***Hankerson D.R., Vanstone S.A. и Menezes A.J.*** Guide to elliptic curve cryptography. New York: Springer, 2003. Vol. XX.

[2] ***Ключарев П.Г.*** Основы квантовых вычислений и квантовой криптографии // Вестник МГТУ им. Н.Э. Баумана. 2006. № 2. С. 36–46. (Сер. Приборостроение).

[3] ***Grover L.K.*** Quantum Mechanics Help in Searching for a Needle in a Hay-stack // Phys. Rev. Lett. 1997. № 78 (2). С. 325–328.

[4] ***Shor P.*** Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 1994.

[5] ***Pomerance C.*** A Tale of Two Sieves // Not. Amer. Math. Soc. 1996. № 43.

[6] ***Proos J.A.*** Shor's discrete logarithm quantum algorithm for elliptic curves. Waterloo: Faculty of Mathematics University of Waterloo, 2003.

УДК 004.056.53

ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ В СЕТИ

Н.Д. Хынг, А.В. Кизим

Безопасность передачи информации в сети является одной из важных задач современной и будущей информационной технологии. В статье авторы предложили метод шифрования данных, способ передачи мультимедиа-информации в сети с обеспечением безопасности, а также алгоритм повышения надежности обмена информацией.

В связи с все возрастающим влиянием Интернета проблема защиты информации с каждым годом становится актуальнее. Вопросами защиты информации являются: предот-

вращение хищения информации, обеспечение целостности данных, аутентификация и др. При проектировании и реализации сетевых приложений необходимо повысить их безопасность, скорость работы и оптимизировать затраты. Для этого предложен алгоритм шифрования данных, способ передачи мультимедиа-информации и метод повышения надежности обмена информацией.

Алгоритм замены для блочного шифрования с закрытым ключом

При организации передачи информации встают вопросы стойкости и скорости реализации алгоритмов шифрования данных. В этом разделе мы предлагаем вариант их решения.

Любой тип данных можно преобразовать к типу данных, построенному на множестве слов по 8 бит. Для шифрования используется ключ. Ключ состоит из комбинации не меньше 8 слов, пусть ключом является $p_1p_2p_3p_4p_5...p_n$, где n – длина ключа. Каждый символ открытого текста заменятся символом, отстоящим от него правее, чем p_i символов. Это означает, что код каждого символа складывается с соответствующим кодом пароля. В результате получаем новый текст. Далее мы работаем с преобразованным текстом.

Разбиваем открытый текст на блоки длиной 8 слов (64 бит). Если длина открытого текста не кратна 8, то получим еще множество избыточных последних символов *w* (меньше 8 слов). Пусть каждый блок состоит из 8 слов $a_0a_1a_2a_3a_4a_5a_6a_7$.

Сформируем целочисленный массив b[8] следующим образом:

$$b[i]=(\sum_{i=0,i\neq j}^{n} p[i]-p[j]) \bmod 8, \qquad (1)$$

где p[i] – значение кода i-ой символа ключа.

Из этого массива выберем множество O, которое состоит из 8 различных чисел:

$$O=\{ c_0, c_1, c_2, c_3, c_4, c_5, c_6, c_7 \} \qquad (2)$$

где c_i – это порядок значения b[i] в сравнении с другими значениями b[j] (j=0..7, j≠i) по направлению возрастания, $0\leq c_i\leq 7$, $c_i\neq c_j$ для $\forall$ i≠j.

Из этого множества мы заменяем положения слова блока текста $a_0a_1a_2a_3a_4a_5a_6a_7$ по порядку множества O.

Открытый текст не обязательно имеет длину, кратную 8 (множество *w* состоит от одного до семи символов). Реализация последних избыточных символов вызывает проблемы для нескольких существующих алгоритмов, потому что в случае недостаточной степени защиты их реализации степень угрозы взлома возрастает. Для указанного алгоритма можно решить эту проблему путем шифрования по битам последних избыточных символов открытого текста.

Выполнение алгоритма представлено в виде блока-схемы на рис. 1. Ход дешифрования обратен шифрованию. В этом алгоритме не используется сложение по модулю 2 (исключение или), поэтому аналитически труднее дешифровать при отсутствии ключа. Предположительно алгоритм имеет хорошую стойкость, более высокую скорость при сравнении с алгоритмами DES, ГОСТ, поэтому удобен для шифрования данных при общении в сети.

Способ передачи мультимедиа-информации в сети

Видео- и аудиообщение являются одними из важных сервисов в современных сетевых приложениях. Рассмотрим процесс шифрования видеоданных, построенный на базе алгоритма, описанного в первом разделе.

Развитие Интернета, особенно развитие цифровой техники, вызывает быстрое развитие приложений Интернета, которые передают информацию в сети в виде чисел, т.е. данные обозначены в виде цепочки бинарных чисел (0/1), передаваемых по сети. Видеоизображение и другие виды информации можно передать на любое расстояние по цифровым каналам связи. При наличии компьютера и камеры, подключенных к Интернету, с помощью программного обеспечения можно передать изображение в любую точку мира.

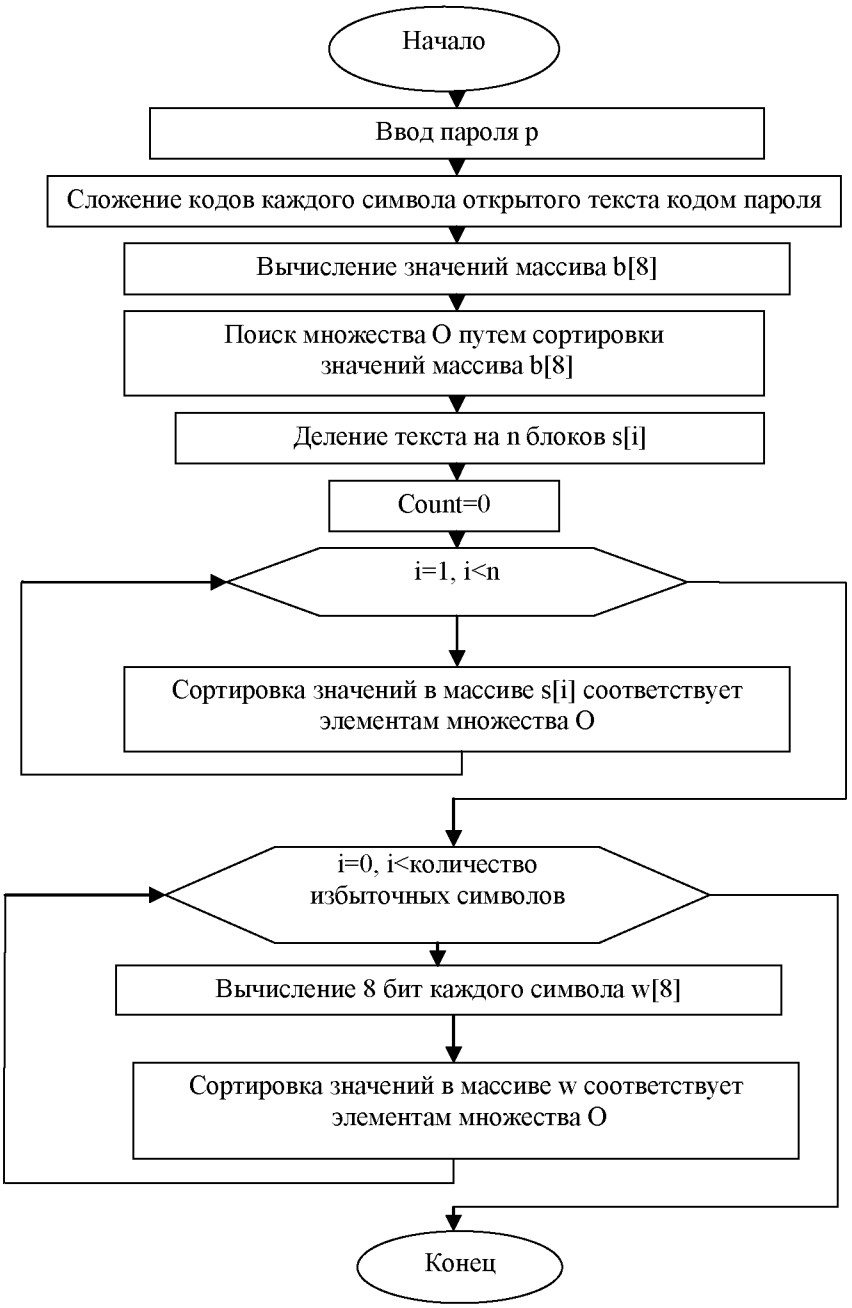

Рис. 1. Блок-схема алгоритма замены блочного шифрования

Рассмотрим процесс обмена видео в сети с точки зрения программиста. У каждого программиста имеется метод обработки информации, соответствующий своей цели. Операционная система Window и другие поддерживают функции для доступа, получения и изменения параметров камеры. Для использования этих функций необходимо подключить в приложение библиотеку, например Vfw.h. С помощью ее функций можно получить поток данных изображения в виде структуры LPVIDEOHDR. Для обеспечения безопасности необходимо шифровать эти данные перед отправлением и расшифровывать их после получения. С целью повышения стойкости и скорости реализации шифрования данных можно использовать такой алгоритм, который описан в первом разделе.

Видеоданные имеют большой размер, поэтому если передавать их без дополнительной обработки, то это уменьшает скорость передачи и повышает затраты. Поэтому необхо-

димо сжимать данные перед передачей в сети. Существует много алгоритмов сжатия данных. В рамках этой статьи опишем алгоритм сжатия данных для видеоконференции. Обычно 2 последовательные карты изображений, полученные из камеры, мало изменяются. Рассмотрим следующий пример. Пусть массив точек цветов карт обозначен в виде двухмерной матрицы (табл. 1).

Таблица 1

Матрица точек цветов двух карт

0	5	8	7	9	6	7	2
3	9	6	8	3	5	5	3
4	6	9	5	8	9	0	9
8	5	5	3	6	2	3	5
1	4	2	1	5	1	0	8

0	5	8	7	9	6	7	2
3	9	6	8	4	5	5	3
4	6	9	4	8	4	0	9
8	5	5	3	5	2	3	5
1	4	2	1	5	1	0	8

Исходя из этого, таблица отличий между первой и второй картами такова (табл. 2).

Таблица 2

Матрица точек цветов двух карт

0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	0
0	0	-1	0	-1	0	0	0
0	0	0	-1	0	0	0	0
0	0	0	0	0	0	0	0

Пусть первая карта отправлена. Теперь вместо отправки полной второй карты отправим разницу двух карт. При получении приемник сравнивает отличие с первой картой и восстанавливает вторую карту. Таким образом, уменьшается объем передачи.

Мы рассмотрели метод обработки информации видеоконференции и обеспечения ее безопасности при общении в незащищенной сети. Аналогично можно организовать обработку аудиоинформации. Далее рассмотрим алгоритм повышения надежности передачи информации.

Алгоритм повышения надежности передачи информации

Для передачи важной информации нужно обеспечить не только высокий уровень безопасности, но и надежности передачи информации.

Согласно RFC 793 протокол TCP должен восстанавливать данные в случае их повреждения, потери, дублирования или доставки с нарушением порядка[1]. С другой стороны, согласно RFC 768 протокол UDP не гарантирует доставки сообщений и не предотвращает появления дубликатов. Приложения, требующие гарантированной доставки потоков данных, должны использовать протокол TCP[2]. Но протокол TCP не обеспечивает абсолютно надежной передачи информации. При передаче данных необходимо разбивать файл на фрагменты согласно формату кадра используемого протокола и затем передавать каждый отдельный фрагмент. При этом если потеряется хотя бы один фрагмент, это вызовет отказ файла. Возможное решение этой проблемы состоит в следующем.

Для предотвращения потери информации организуем цикл отправления каждого пакета. Цикл заканчивается тогда, когда приходит ответ от получателя о благополучной доставке. К каждому пакету будет добавлен идентификационный номер. Аналогично для получения. Получателю приходит пакет с идентификацией, начало сравнивается с идентификатором предыдущего пакета. Если они равны, то пакет уже получен ранее и не сохраняется. Если они не равны, то информация из этого пакета добавляется в файл и отправитель изве-

щается, что получен пакет с этим идентификатором. Для объяснения алгоритма представлена блок-схема отправления файла (рис. 2).

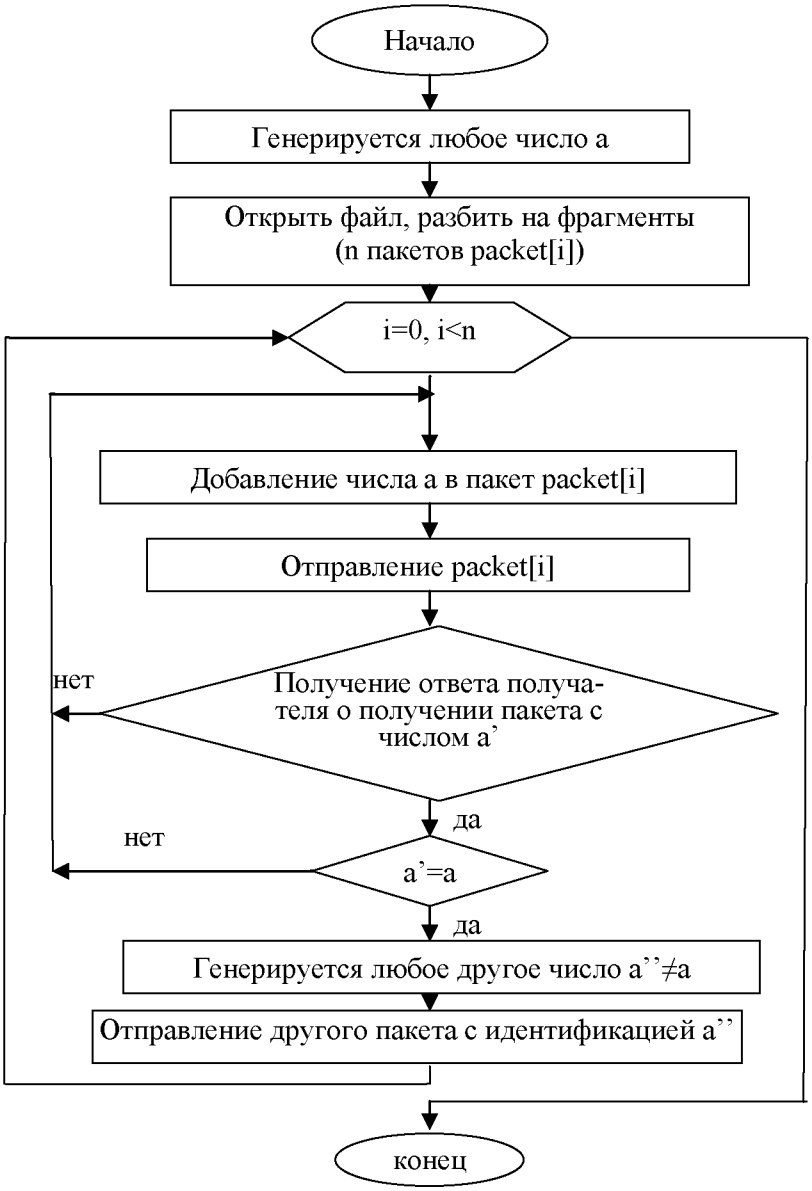

Рис. 2. Блок-схема для повышения надежности передачи файла

О свойствах алгоритма можно предположить, что он обладает такими достоинствами, как высокая вероятность получения неискаженных данных и достаточно высокая скорость передачи (по сравнению с алгоритмом хеширования). Недостатки заключаются в снижении скорости работы при сбоях в передаче информации и необходимости повторений фрагментов.

[1] Протокол управления передачей. Программная спецификация протокола DARPA INTERNET // http://www.protocols.ru/files/RFC/rfc793.pdf

[2] ***Postel J.*** Transmission Control Protocol / Information Sciences Institute. 1980, january. http://www.lissyara.su