KOKAND UNIVERSITY HERALD SCIENTIFIC E-JOURNAL
QO'QON UNIVERSITETI XABARNOMASI
KOKAND UNIVERSITY HERALD
ВЕСТНИК КОКАНДСКОГО УНИВЕРСИТЕТА
ISSN: 2181-1695 OAK: 01-08/1819/6 www.herald.kokanduni.uz

НОВЫЕ ПОДХОДЫ К ЗАЩИТЕ И ПЕРЕДАЧЕ ДАННЫХ: КОМБИНИРОВАНИЕ ШИФРОВАНИЯ И СЖАТИЯ

Ш.Ш.Ахмадалиев,
старший преподаватель кафедры цифровых технологий и математики,
Кокандский университет,
e-mail: mr.shahobiddin@gmail.com

MAQOLA HAQIDA

Qabul qilindi: 24-iyun 2025-yil
Tasdiqlandi: 26-iyun 2025-yil
Jurnal soni: 15
Maqola raqami: 28
DOI: https://doi.org/10.54613/ku.v15i.1208

KALIT SO'ZLAR/ КЛЮЧЕВЫЕ СЛОВА/ KEYWORDS

шифрование, сжатие информации, защита данных, надежная передача, комбинированные алгоритмы, информационная безопасность, оптимизация алгоритмов.

АННОТАЦИЯ

Статья исследует, как можно грамотно сочетать алгоритмы шифрования и сжатия данных, чтобы надежно защищать информацию и эффективно её передавать. Мы рассмотрели разные способы интеграции этих методов: от последовательного подхода, где сначала сжимаем, а потом шифруем, до параллельных схем, где процессы идут одновременно. Каждый метод оценивался с точки зрения скорости работы, устойчивости к атакам и экономии объема данных. Особое внимание уделили новым схемам, которые учитывают ограничения вычислительных ресурсов - например, для устройств с низкой мощностью. Предложенные решения не только ускоряют обработку, но и делают данные менее уязвимыми к взлому, минимизируя объем передаваемой информации. Итоги исследований показывают: такие комбинированные подходы заметно повышают надежность и производительность систем защиты данных, особенно в условиях жестких требований к ресурсам. Это шаг вперед для безопасной и быстрой передачи информации.

Введение. С ростом объемов цифровой информации и числа кибератак защита данных и их надежная передача выходят на первый план. Шифрование помогает сохранить секретность, целостность и подлинность информации, а сжатие уменьшает её объем, разгружая каналы связи и ускоряя обмен данными. Но использование этих методов по отдельности не всегда дает идеальный баланс между безопасностью, скоростью и экономией ресурсов.

Объединение шифрования и сжатия открывает новые горизонты для создания систем, которые одновременно защищают данные и сокращают затраты на их передачу. Это особенно важно для устройств с ограниченными возможностями, таких как смартфоны, гаджеты Интернета вещей или облачные сервисы. В этой статье мы разбираем, как интегрировать эти алгоритмы, взвешиваем их плюсы и минусы, а также предлагаем свежие подходы, которые обеспечивают надежность и эффективность. Цель — найти универсальные решения, которые подойдут для самых разных задач по защите и передаче данных.

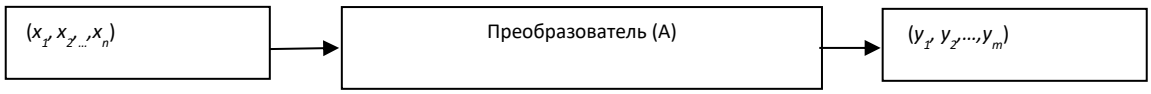
В эпоху бурного развития технологий и коммуникационных систем защита информации и её надежная передача по открытым каналам связи волнуют не только специалистов, но и обычных пользователей. Это особенно важно, когда речь идет о данных, имеющих общественную или государственную значимость.

Для отправки некритичной информации по незащищенным каналам часто применяют помехоустойчивые методы кодирования, которые помогают исправлять ошибки при передаче. А для обработки сигналов с широким спектром используют коды сжатия [1-3], которые делают передачу более эффективной. Когда же нужно обеспечить секретность данных в публичных сетях, на помощь приходят алгоритмы шифрования [4-6].

Все эти подходы — помехоустойчивое кодирование, сжатие и шифрование — основаны на преобразовании исходных данных. Они дополняют друг друга, и их совместное использование открывает новые возможности для надежной защиты информации, как при её хранении, так и при передаче по сетям. Разработка таких универсальных решений — одна из ключевых задач современных информационных технологий.

В этой статье мы сосредоточимся на создании комбинированных методов шифрования и сжатия данных, а также на их применении для защиты информации в сетях. Коммуникационные системы — это сложные структуры, где множество каналов взаимодействуют, передавая данные от источника к получателю. Чтобы управлять потоками информации, обеспечивать их безопасность и решать другие задачи, нужны точные математические модели. Именно они позволяют находить эффективные и надежные способы защиты, хранения и передачи данных.

Методология. Для анализа процессов в информационно-коммуникационных системах часто используют модели «вход-выход».



Они представляют собой системы линейных уравнений с неизменными коэффициентами:

$$A_{m\times n}x_{n\times 1} = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix} = y_{m\times 1},$$

где входной блок данных $x_{n\times 1} = (x_1, \ldots, x_n)$ преобразуется через прямоугольную матрицу $A_{m\times n}$ в выходной блок $y_{m\times 1} = (y_1, \ldots, y_m)$.

В статье [7] описан способ восстановления элементов матрицы $A_{m\times n}$ по известным входным данным $x^{(k)} = (x_1^{(k)}, \ldots, x_n^{(k)})$ и соответствующим выходным данным $y^{(k)} = (y_1^{(k)}, \ldots, y_m^{(k)})$. Эти методы находят применение в шифровании, расшифровке, сжатии данных и других задачах современных коммуникационных систем.

Способы защиты информации, использующие секретный ключ для шифрования и расшифровки, называют криптографическими. Алгоритмы шифрования бывают двух видов: симметричные и асимметричные. В симметричных системах знание ключа шифрования k_e позволяет легко вычислить ключ расшифровки k_d. Примеры таких алгоритмов — DES, AES, ГОСТ 28147-89.

В асимметричных системах, работающих с открытым ключом, знание ключа шифрования k_e не дает возможности определить ключ расшифровки k_d. Пара ключей (k_e, k_d) создается для каждого пользователя сети с неким секретом, который позволяет по k_e

вычислить k_d. Без этого секрета задача становится крайне сложной или неразрешимой с текущими технологиями. Примеры асимметричных алгоритмов — RSA, Эль-Гамаля и Мак-Элиса.

Алгоритм RSA основан на трудности разложения большого нечетного числа n на простые множители p и q. Ключи генерируются по правилу: $ed \equiv 1 \mod \phi(n)$, где $\phi(n)$ — функция Эйлера, известная только центру генерации ключей. Зная $\phi(n)$ и выбрав e, можно легко найти d. Без знания $\phi(n)$ вычислить d по e практически невозможно — злоумышленнику нужно разложить n на p и q, чтобы определить $\phi(n) = (p-1)(q-1)$.

Алгоритм Эль-Гамаля опирается на сложность вычисления дискретного логарифма в конечном поле. Для уравнения $y = a^x \mod p$, где известны y, a и большое простое число p, найти $x = (\log_a y)(\mod p)$ без перебора значений практически невозможно, так как $\log_a y$ не всегда целое число.

Алгоритм Мак-Элиса основан на трудности решения систем линейных уравнений высокого порядка в конечном поле. Нужно найти целочисленные решения из множества чисел, не превышающих характеристику поля, что требует значительных вычислительных усилий.

Подробности об асимметричных алгоритмах можно найти в работах [4–9].

Результаты. Вернемся к теории матриц и их приложениям в решении задач информационно-коммуникационных технологии. Пусть $A_{m\times n}$ –прямоугольная матрица, имеющая m –строк и n – столбцов, и $m \neq n$. Такая матрица не имеет обратную матрицу, так как понятие обратной матрицы определено для квадратичных матриц. Преобразование вектора $x_{n\times 1}$ на вектор $y_{m\times 1}$ прямоугольной матрицей $A_{m\times n}$, т.е. $y_{m\times 1} = A_{m\times n}x_{n\times 1}$ является необратимым. Но для того, чтобы найти $x_{n\times 1}$ обе части последнего равенства применим прямоугольное матричное преобразование $B_{n\times m}$, т.е.

$$B_{n\times m}y_{m\times 1} = B_{n\times m}A_{m\times n}x_{n\times 1} = P_{n\times n}x_{n\times 1}, \quad (1)$$

чтобы квадратная матрица $P_{n\times n}$ была обратимой. Если определитель квадратной матрицы $P_{n\times n}$ отличен нуля, т.е. $|P_{n\times n}| \neq 0$, то матрица $P_{n\times n}$ обратима. Тогда обе части равенства (1) применяя обратную матрицу $P^{-1}_{n\times n}$ имеем:

$$P^{-1}_{n\times n}B_{n\times m}A_{m\times n}x_{n\times 1} = P^{-1}_{n\times n}P_{n\times n}x_{n\times 1} = x_{n\times 1}.$$

Используя свойство необратимости прямоугольных матриц, но обратимости их комбинации с некоторой соответствующей матрицей будем разрабатывать алгоритм генерации пары ключей ($k_ш$, $k_р$), причем знание $k_ш$, не позволит вычислить $k_р$.

Рассмотрим преобразование

$$B_{k\times m}A_{m\times n}x_{n\times 1} = z_{k\times 1}, \quad (2)$$

где матрица $A_{m\times n}$ и вектор $z_{k\times 1}$ известны, матрица $B_{k\times m}$ и вектор $x_{n\times 1}$ неизвестны, кроме того, $k \neq m$, $k \neq n$, $m \neq n$. При этих условиях, нет возможности найти вектор $X_{n\times 1}$, кроме подбора элементов матрицы $C_{n\times k}$ так чтобы матрица $C_{n\times k}B_{k\times m}A_{m\times n} = P_{n\times n}$ была обратимой ($k \geq m \geq n$). При больших размерах матриц и отсутствие ограничения значениям элементов матриц кроме их целостности совокупность значений элементов образуют бесконечное (счетное) множество, что обеспечить бесконечность процесса полного перебора элементов $C_{n\times k}$. Обратная матрица $P^{-1}_{n\times n}$ позволяет найти вектора $X_{n\times 1}$, применив преобразование $C_{n\times k}$ на обе части равенства (2), т. е.

$$P^{-1}_{n\times n}\, C_{n\times k}\, B_{k\times m}\, A_{m\times n}\, x_{n\times 1} = P^{-1}_{n\times n}\, C_{n\times k}\, z_{k\times 1} \text{ или } x_{n\times 1} = P^{-1}_{n\times n}\, C_{n\times k}\, z_{k\times 1}.$$

Теперь, если полагать значения элементы матрицы $A_{m\times n}$ ключом алгоритма шифрования прямоугольным матричным преобразованием, а значения элементы матрицы $P^{-1}_{n\times n}$ ключом алгоритма расшифрования, значения элементы матрицы $B_{k\times m}$ лазейкой, неизвестной пользователям сети телекоммуникации (известной только ответственному лицу центра распределения ключей (ЦРК)), то известность значения элементы матрицы $A_{m\times n}$ не позволяет вычислять значения элементы матрицы $P^{-1}_{n\times n}$, для того, чтобы раскрыть шифртекст, полученный каждого блока открытого текста $x_{n\times 1}$ преобразованием $B_{k\times m}\, A_{m\times n}\, x_{n\times 1} = z_{k\times 1}$.

Таким образом, генерированную по вышеприведенному правилу пару ($A_{m\times n}$, $P^{-1}_{n\times n}$) матриц $A_{m\times n}$ и $P^{-1}_{n\times n}$ с известными значениями элементов принимая как открытый и секретный ключи определим:

1. Алгоритм шифрования: $B_{k\times m}\, A_{m\times n}\, x_{n\times 1} = z_{k\times 1}$;

2. Алгоритм расшифрования: $P^{-1}_{n\times n}\, C_{n\times k}\, z_{k\times 1} = x_{n\times 1}$;

где

$X_{n\times 1}$ -блоки открытого текста *M*,

$z_{k\times 1}$ -блоки шифртекста *C*,

$A_{m\times n}$ -открытый ключ пользователя,

$P^{-1}_{n\times n}$ -закрытый ключ пользователя,

$B_{k\times m}$ и $C_{n\times k}$ -ключи лазейки известные только ЦРК, который генерирует и распределяет, а

также управляет совокупность ключей в середе пользователей.

Главный недостаток упомянутой криптосистемы кроется в использовании матриц-лазейек e и d в алгоритмах шифрования и расшифровки. В процессе шифрования задействуется матрица e, а при расшифровке — матрица d. Такая структура создает уязвимость: если эти матрицы хранятся на носителях в сети, злоумышленник может их перехватить и, используя открытый ключ, восстановить секретный. Это противоречит основным принципам построения безопасных асимметричных криптосистем. К тому же, шифрование заметно увеличивает объем данных, что делает хранение и передачу информации менее эффективными.

Чтобы устранить эти проблемы, мы разрабатываем комбинированные алгоритмы шифрования и сжатия, основанные на прямоугольных матрицах в конечных полях целых чисел. Такие методы позволяют защищать данные при их хранении и передаче в информационно-коммуникационных сетях, избегая указанных недостатков и соответствуя принципам асимметричных криптосистем. Сочетание этих подходов помогает создавать более надежные и эффективные решения для современных задач защиты информации.

Пусть матрицы:

$$A_{m\times n} = \begin{pmatrix} a_{11} & a_{12}\ldots a_{1n} \\ a_{21} & a_{22}\ldots a_{2n} \\ \ldots\ldots & \ldots\ldots\ldots \\ a_{m1} & a_{m2}\ldots a_{mn} \end{pmatrix}, B_{n\times m} = \begin{pmatrix} b_{11} & b_{12}\ldots b_{1m} \\ b_{21} & b_{22}\ldots b_{2m} \\ \ldots\ldots & \ldots\ldots\ldots \\ b_{n1} & b_{n2}\ldots a_{nm} \end{pmatrix}, E_{n\times n} = \begin{pmatrix} e_{11} & e_{12}\ldots e_{1n} \\ e_{21} & e_{22}\ldots e_{2n} \\ \ldots\ldots & \ldots\ldots\ldots \\ e_{n1} & e_{n2}\ldots e_{nn} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ 0 & 1 & 0 & \ldots & 0 \\ \ldots\ldots & \ldots\ldots & \ldots & & \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix},$$

$$B_{n\times m}\cdot A_{m\times n}=\begin{pmatrix} b_{11} & b_{12}\ldots b_{1m}\\ b_{21} & b_{22}\ldots b_{2m}\\ \ldots\ldots\ldots & \ldots\ldots\ldots\\ b_{n1} & b_{n2}\ldots a_{nm}\end{pmatrix}\times\begin{pmatrix} a_{11} & a_{12}\ldots a_{1n}\\ a_{21} & a_{22}\ldots a_{2n}\\ \ldots\ldots\ldots & \ldots\ldots\ldots\\ a_{m1} & a_{m2}\ldots a_{mn}\end{pmatrix}=\begin{pmatrix} c_{11} & c_{12}\ldots c_{1n}\\ c_{21} & c_{22}\ldots c_{2n}\\ \ldots\ldots\ldots & \ldots\ldots\ldots\\ c_{n1} & c_{n2}\ldots c_{nn}\end{pmatrix}=C_{n\times n}$$

где $n \neq m$, элементы a_{ij} и b_{ij} произвольные.

Если $m \prec n$, то преобразование $A_{m\times n}x_{n\times 1}\ mod\ 2^r = y_{m\times 1}$, блок открытой информации $x_{n\times 1}$ длиной n, сжимает на блок $y_{m\times 1}$ меньшей длины m, где r -количество разрядов в битах представления значении каждого элемента x_i блока открытой информации $x_{n\times 1} = (x_1, x_2, \ldots, x_n)$, т.е. элементы x_i, $i = 1,2,\ldots,n$, могут быть представятся в восьми разрядах –байтах ($r = 3$ и $2^r = 8$), в шестнадцати или тридцати двух разрядах – словах ($r = 4 и 2^4 = 16$ или $r = 5 и 2^5 = 32$). Целесообразным является принимать значения параметров m и n, выражающие размера прямоугольной матрицы $A_{m\times n}$, определить кратным двум: $m = 2^d$ и $n = 2^l$, $d \prec l, d = 1,2,\ldots;\ \ l = 2,3,\ldots\ldots$ Зная блок $y_{m\times 1}$ и преобразования $A_{m\times n}$, можно восстановить блок $x_{n\times 1}$. Для этого вычисляется прямоугольная матрица $B_{n\times m}$, удовлетворяющая равенству $B_{n\times m} \times A_{m\times n} = E_{n\times n}\ mod\ 2^r$. Тогда имеет место цепочка равенств:

$B_{n\times m}y_{m\times 1}\ mod\ 2^r = B_{n\times m}A_{m\times n}x_{n\times 1}\ mod\ 2^r = E_{n\times n}x_{n\times 1}\ mod\ 2^r = x_{n\times 1}$.

Как видно, что знание матричного преобразования $A_{m\times n}$, позволяет вычислить преобразование $B_{n\times m}$, которое дает возможность однозначного нахождения блок $x_{n\times 1}$. Следовательно, такой подход позволяет сжатие информации, причем кратное применение данного правила сжимает любую информацию большой длины кратной на *n*, на блок информации длиной m. Обратно, сжатую информацию длиной m, зная количество кратности применения преобразования $A_{m\times n}$, можно разжать на исходную информацию кратной на *n*.

Для хранения и обмена электронных документальных информаций в информационно-коммуникационных сетях значения размеров m и n можно выбрать как удобно пользователям. Так как электронные документальные информации, восприятия которых не зависит от временных факторов и прямых передачи по каналу связи, перед хранением в носителях или перед отправлением в сети связи позволяет предварительную обработку с применением программного обеспечения предлагаемого алгоритма в приложении.

Для хранения голосовых информации и информации видео изображения, учитывая свойства их формата воспроизведения, которые выражаются в цифровых блоках, значения размеров m и nможно выбрать как удобно самому пользователю. Но для прямых передачи голосовых информации и информации видео изображения значения размеров m и n, приходится выбрать с учетом расчета пропускной способности канала связи, которая зависит составляющих технических средств. Самим практичным выбором являются $m = 2$ и $n = 4$ (или $n = 8$) целю обеспечения высокой скорости и эффективной аппаратно-технической или аппаратно-программной реализации предложенного алгоритма сжатия.

Использование изложенного алгоритма с матрицами $A_{m\times n}$ и $B_{n\times m}$, известными только доверяющими друг другу сторонами для хранения и передачи конфиденциальной информации в информационно-коммуникационной сети, дает *комбинирование алгоритмов шифрования и сжатия информации* в одном. При этом, если значения элементов a_{ij} матрицы $A_{m\times n}$, представление в десятичной системе исчислении, в общем должны содержит не меньше 42 (сорока трех) цифра. Тогда, со стороны злоумышленника, для того чтобы восстановит неизвестных значения a_{ij}, требуется перебирать $10^{43} > 2^{128}$ вариантов, которого не возможно осуществить с использованием достижений современной науки и вычислительной техники. Такой алгоритм *комбинирование алгоритмов шифрования и сжатия информации* в одном, представляет собой симметричную криптосистему защиты информации.

1. Правило (алгоритм) обеспечения конфиденциальности : $A_{m\times n}x_{n\times 1}\ mod\ 2^r = y_{m\times 1}$.

2. Правило (алгоритм) обеспечения распознавания: $B_{n\times m}y_{m\times 1}\ mod\ 2^r = x_{n\times 1}$; так, как $B_{n\times m}y_{m\times 1}\ mod\ 2^r = B_{n\times m}A_{m\times n}x_{n\times 1}\ mod\ 2^r = E_{n\times n}x_{n\times 1}\ mod\ 2^r = x_{n\times 1}$.

Обсуждение. Предложенный метод комбинирования алгоритмов шифрования и сжатия информации с использованием прямоугольных матриц на конечном поле целых чисел решает проблему увеличения объема шифрованной информации, характерную для ранее описанных асимметричных криптосистем. Основным недостатком асимметричных систем, описанных ранее, является присутствие ключей-лазейки $B_{k\times m}$ и $C_{n\times k}$, которые могут быть перехвачены криптоаналитиком, что нарушает принципы создания асимметричных криптосистем. В предложенном методе таких лазеек нет, так как матрицы $A_{m\times n}$ и $B_{n\times m}$ известны только доверяющим сторонам, что делает систему симметричной и более устойчивой к атакам.

Разработанный алгоритм позволяет одновременно обеспечивать конфиденциальность и сжатие информации, что особенно важно для приложений, требующих эффективного использования ресурсов, таких как IoT-устройства и мобильные платформы. Выбор размеров *m* и *n* (например, *m* = 2, *n* = 4 или *n* = 8 обеспечивает гибкость и адаптацию к различным типам данных и пропускной способности каналов связи.

Более подробные сведения о приложениях прямоугольных матриц в решениях задач обеспечения конфиденциальности и надежной передачи информации можно найти в работах [8, 9].

Список использованной литературы:

1. Тутевич В.Н. Телемеханика: Учеб. пособие для студентов вузов спец. «Автоматика и телемеханика».- М.: Высш. шк., 1985. – 423 с.

2. Баскаков С.И. Радиотехнические цепи и сигналы: Учебник для вузов по специальности «Радиотехника».-М.: Высш. шк., 1988. -448 с.

3. Бернард Скляр. Цифровая связь. Теоретические основы и практическое применение. – М.: Издательский дом «Вильямс», 2003. -1104 с.

4. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. -М.: Гелиос АРВ, 2002.-480 с.

5. Шнайер Б.. Прикладная криптография. Протоколы, алгоритмы, исходные тексты. М.: ТРИУМФ, 2003. -816 с.

6. Харин Ю.С., Берник В.И., Матвеев Г.В., Агиевич С.В. Математические и компьютерные основы криптологии. –Мн.: Новое знание, 2003. -382 с.

7. Акбаров Д.Е., Ахмадалиев Ш.Ш., Нуриев Ш.З. Математическое моделирование и управление линейно-стационарных объектов в информационных системах //Научно-технический журнал Ферганского политехнического института. - 2002 г., №2 – С. 3-7.

8. Коблиц Н. Курс теории чисел и криптографии. М.: 2001. – 269 с.

9. Коутенхо С. Введение в теорию чисел. Алгоритм RSA. –М.: «ЗАО Предпрятие Постмаркет», 2001. -328 с.