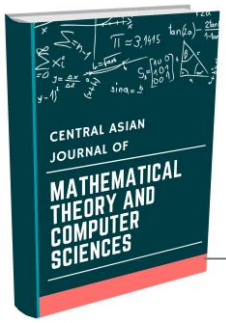

CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES

http://cajmtcs.centralasianstudies.org/index.php/CAJMTCS

Volume: 02 Issue: 11 | Nov 2021 ISSN: 2660-5309

Исследования Вопросов Необходимых Условий Крипто Стойкости Алгоритмов Блочного Шифрования С Симметричным Ключом

Д. Е. Акбаров[1], О. Э.Кушматов[2], Ш.А. Умаров[3], Р. Г. Расулов[4]

[1]*д.физ.-мат. н., Какандский государственный педагогический институт, Каканд, Узбекистан*

[2]*к.физ.-мат. н., Ферганский филиал Ташкентского университета информационных технологий, Фергана, Узбекистан*

[3]*исследователь, Ферганский филиал Ташкентского университета информационных технологий, Фергана, Узбекистан*

[4]*ст. преподаватель, Ферганский политехнический институт, Фергана, Узбекистан*

Аннотатсия:

В статье исследованы особенности критериев стойкости алгоритмов блочного шифрования с симметричным ключом. Выявлены общие свойства моделей классов алгоритмов блочного шифрования с симметричным ключом. На их основе сформулированы соответствующие требования в виде критериев, определяющих необходимые условия криптостойкости. Эти критерии в совокупности сформулированы как утверждение.

ARTICLEINFO

Article history:
Received 30 Sep 2021
Revised form 22 Oct 2021
Accepted 17 Nov 2021

Ключевые слова: классы алгоритмов шифрования, идеально стойких алгоритмов, непрерывный алгоритм шифрования, блочный алгоритм шифрования, критерий, криптостойкость, необходимое условие, математическая модель, преобразование распространения, преобразование перемешивания, коллизия, длина ключа, шифрованное сообщение, микропроцессор.

Введение. При использовании алгоритмов шифрований, для того чтобы частотные характеристики языка, на котором составлено открытое сообщение, не перешли на соответствующее шифрованное сообщение, пользуются алгоритмами многозначной замены. Для достижения такой цели на этапах шифрования изменяют таблицы замены, т.е. возникает необходимость увеличения длины ключа.

Идеально стойкие и непрерывные шифрвания относясь к типу алгоритмов многозначной замены, являются достаточно высокой степени стойкими [1-9, 14-16]. Они, обычно в своей основе, имеют односторонние несложные преобразования, следовательно, по конструкции являются удобными для разработки их аппаратными средствами. Но, идеально стойкие алгоритмы шифрования, с криптографическими достоинствами, имеют недостатки по использованию ключей. Используемый ключ имеет довольно большую длину и к тому же применяется один раз. Кроме того, процесс шифрования, часто осуществляется гаммированием, т. е. элементы ключевого блока или псевдослучайной последовательности с соответствующими элементами шифруемого сообщения преобразуются с некоторой операцией. Часто, с операцией $\oplus$ –XOR, в случае гаммирования на основе битов [3-8], что является поводом для проведения полного перебора блока гаммирования,

относительно коротких криптограмм. Из вышеприведенных фактов следует, что при обеспечении безопасности: ключевой базы при хранении, обмене с ключами по открытому каналу информационно-коммуникационной сети и т.д. отнимают много объема памяти и времени, что является нежелательным.

Исследования на пути предотвращений таких и других, не предвиденных обстоятельств, привело к созданию блочных алгоритмов шифрования с симметричным ключом. Более полную информацию по блочным алгоритмам шифрования с симметричным ключом, можно получить в других литературных источниках [1,2, 7–14].

Постановка задачи. В статье исследуются криптографические особенности критериев стойкости алгоритмов блочного шифрования с симметричным ключом. Выявляются общие криптографические свойства преобразований и конструкции моделей классов алгоритмов блочного шифрования с симметричным ключом. Формулируется утверждение необходимых критериев обеспечивающих условия стойкости.

Решение задачи. В симметричных блочных алгоритмах шифрования процесс шифрования осуществляют отдельными блоками фиксированной длины. Длина исходного ключа должна быть такова, чтобы для нахождения нужного ключа осуществление полного перебора ключей неэффективна экономически, и затратна по времени. В настоящее время этот показатель не меньше 256 символов, исходя из особенностей преобразований, которые выполняются, над какими элементами: битов, двух битов, полубайтов, байтов и др.

Основы симметричных блочных алгоритмов шифрования содержат базовые преобразования со свойствами высокого перемешивания и рассеивания. Эти алгоритмы относятся к типу *стойких алгоритмов шифрования* [17-29]. Базовые преобразования и конструкции блочных алгоритмов шифрования связаны со сложно решаемыми задачами, решения которых требуют глубоких исследований.

Изучения, исследования и наблюдения авторов в области криптографии, позволили решиться сформулировать совокупность необходимых условий стойкости блочных алгоритмов шифрования с симметричным ключом, в виде утверждения.

Утверждение. *Для того чтобы симметричные алгоритмы блочного шифрования были криптостойкими необходимо выполнения следующих условий:*

1) *Алгоритм должен быть открытым, его криптостойкость зависит только от неизвестности и длины ключа, при этом длина должна быть не меньше 256 символов*: $k = k_1 k_2 ... k_N, \quad k_i \in \{0;1\}, N = 32 \times l, \quad l = 8,9, \ldots < \infty$;

2) *Желательно, длина преобразуемого блока была* $2^t, \quad t = 6,7, \ldots < \infty$, *операции применяемые в преобразованиях алгоритма должны соответствовать эффективному использованию в микропроцессорах, микроконтроллерах и компьютерных вычислительных системах;*

3) *Основные базовые преобразования обладают свойствами: эффективного перемешивания и распространения, нелинейности, односторонности, равновесия, регулярности, лавинного эффекта, гибкости относительно корреляции и т.д.;*

4) *Основные базовые преобразования алгоритма симметричного блочного шифрования на основе сети Фейстеля должны обладать свойством односторонности.*

Доказательство. Блочные алгоритмы шифрования с симметричным ключом по конструкции разделяются, в основном, на две группы [1,2,14,17,30,31]: основанные на сети Фейстеля и не основанные на ней. Первый, принятый в 1980 году США стандарт алгоритм блочного шифрования с

симметричным ключом – DES, для использования в коммерческих структурах и принятый в России стандарт ГОСТ 28147-89 основаны на сети Фейстеля. В 2000 году США был принят новый стандарт алгоритма блочного шифрования AES-FIPS 197, взамен морально устаревшего алгоритма DES. Алгоритм AES-FIPS 197 не основан на сети Фейстеля. Его основные базовые преобразования основаны [17, 32]:

1) ***SubBytes*** – по таблице размером 16x16 заданной в алгоритме, заменяются байты шифруемого блока, т.е. осуществляются S –блок преобразования – рассевания;
2) ***ShiftRows*** – по заданной таблице алгоритма, осуществляется циклический сдвиг байтов шифруемого блока;
3) ***MixColumns*** – по матрице заданной в алгоритме, перемешиваются элементы шифруемого блока;
4) ***AddRoundKey –*** сложение по операции $\oplus$ – ***XOR*** ключевого блока раундов с битами шифруемого блока.

Эти преобразования имеют обратные преобразования в случае известных ключей раундов. Характеристики необходимых условий стойкости, приведенных в утверждении, обосновываются тем, что нарушения этих условий отрицательно влияют на стойкость алгоритма.

1. Требование первого условия обеспечивает уверенность в стойкости алгоритма шифрования со стороны пользователей разного рода. Тем самым соблюдается принцип Кирхгофса. Кроме того, выполнение первого требования привлечёт широкий круг криптоаналитиков к анализу алгоритма, и позволяет во время засечь/устранить недостатки в целом.

Символы ключа определяются на основе принципа использования в преобразованиях алгоритма шифрования. При этом длина исходного ключа, в настоящее время, должна быть не меньше 256 символов:

а) если преобразования осуществляются над битами, то длина исходного ключа не меньше 256 битов;

б) если преобразования осуществляются над полубайтами или байтами, то длина исходного ключа не меньше 256 полубайтов или байтов соответственно.

2. Второе требование, что алгоритмы блочного шифрования с симметричным ключом должны содержать преобразования, не сложных вычисляемых операций, что позволит удобно реализовать их в аппаратных средствах [1-17].

В противном случае, т.е. неэффективность операций преобразований алгоритма шифрования в приложениях микропроцессоров, микроконтроллеров, компьютеров и других вычислительных устройств информационной технологии, ограничит их широкое применение. Использование операции табличной замены, таблицей истинности с равномерно распределенными элементами, являются целесообразным. Кроме того, в случае необходимости, для увеличения степени стойкости алгоритма при сохранении свойств базовых преобразований, можно провести их эффективную модификацию.

Длина, преобразуемого блока должна быть кратна, степени два, т.е $2^t, \quad t = 6,7,\ldots < \infty$. В противном случае, могут возникать проблемы связанные не эффективностью криптографических свойств в приложениях, как по увеличению длины ключа и не удобств при аппаратной реализации.

3. Третье требование необходимо для того, чтобы обеспечить стойкость преобразования алгоритма к криптографическим атакам. Если базовые преобразования осуществляются операциями над битами или их объединениями, то не обеспечения эффективного перемешивания и рассевания могут быть

основами моделирования способов криптоатак разного рода, исходя из результатов статистического анализа:

а) Свойства эффективного перемешивания и рассеивания преобразований при входных блоков $\left(x_1^i, x_2^i, \ldots, x_n^i\right),\ i = 0,\ldots,2^{n-1}$ и выходных блоков, где $n \geq m$, проверяются и вследствие определяются равномерным распределением выходных блоков в их таблице истинностей;

б) Независимость совокупности выходных блоков относительно совокупности входных блоков – свойство псевдослучайности обеспечит нелинейность преобразования.

Выполнение условия а) обеспечит свойства преобразований, как: равновесие, регулярность, лавинный эффект, корреляционная иммунность и др.

Если, базовые преобразования не обладают свойствами: криптографической нелинейности, сбалансированности, регулярности, лавинной эффективности, корреляционной иммунности и др., то могут появляться обстоятельства успешных осуществлений линейных и дифференциальных методов крипто атак. Такие обстоятельства увеличат вероятность успешного моделирования некоторых моделей по раскрытую ключей раундов, вследствие исходного ключа или их частей.

Выше перечисленные свойства базовых преобразований, обеспечивающие стойкость, проверяются сравнением попарно разных входных блоков в соответствии попарно разным выходным блокам преобразований. То есть проверяются свойства взаимной однозначности – биективности базовых преобразований. Действительно, для проверки справедливости этого умозаключения осуществляются непосредственные вычисления. На примере рассматриваются преобразование входными и выходными блоками четырьмя битами.

Значит, для удобности, полагается, что $n = m = 4$ и $Y = f(X)_: GF(2)^4 \to GF(2)^4$. Пусть это преобразование обладает свойством биективности. Еще задана таблица истинности обратного биективного преобразования, т.е. определено соответствие: $X = f^{-1}(Y)_: GF(2)^4 \to GF(2)^4$:

Таб.1. Таблица истинности обратного биективного преобразования

$x_1\ x_2\ x_3\ x_4$	$f_1\ f_2\ f_3\ f_4$
0 = 0 0 0 0	0 1 0 0 =4
1 = 0 0 0 1	1 1 1 1 =15
2 = 0 0 1 0	0 0 1 1 =3
3 = 0 0 1 1	0 0 0 0 =0
4 = 0 1 0 0	1 0 0 1 =9
5 = 0 1 0 1	1 1 0 0 =12
6 = 0 1 1 0	1 1 0 1 =13
7 = 0 1 1 1	1 0 1 0 =10
8 = 1 0 0 0	1 0 0 0 =8
9 = 1 0 0 1	0 1 1 1 =7
10 = 1 0 1 0	0 1 1 0 =6
11 = 1 0 1 1	0 0 1 0 =2
12 = 1 1 0 0	0 0 0 1 =1
13 = 1 1 0 1	1 0 1 1 =11
14 = 1 1 1 0	0 1 0 1 =5
15 = 1 1 1 1	1 1 1 0 =14

$f_1\ f_2\ f_3\ f_4$	$x_1\ x_2\ x_3\ x_4$
0 = 0 0 0 0	0 0 1 1 =3
1 = 0 0 0 1	1 1 0 0 =12
2 = 0 0 1 0	1 0 1 1 =11
3 = 0 0 1 1	0 0 1 0 =2
4 = 0 1 0 0	0 0 0 0 =0
5 = 0 1 0 1	1 1 1 0 =14
6 = 0 1 1 0	1 0 1 0 =10
7 = 0 1 1 1	1 0 0 1 =9
8 = 1 0 0 0	1 0 0 0 =8
9 = 1 0 0 1	0 1 0 0 =4
10 = 1 0 1 0	0 1 1 1 =7
11 = 1 0 1 1	1 1 0 1 =13
12 = 1 1 0 0	0 1 0 1 =5
13 = 1 1 0 1	0 1 1 0 =6
14 = 1 1 1 0	1 1 1 1 =15
15 = 1 1 1 1	0 0 0 1 =1

Булевы функции, соответствующие к таблицам истинности отображений $Y = f(X)_: GF(2)^4 \to GF(2)^4$ и $X = f^{-1}(Y)_: GF(2)^4 \to GF(2)^4$, следующие:

а) Булева функция преобразования $Y = f(X)_: GF(2)^4 \to GF(2)^4$ с приведенной таблицей истинности выражаются следующими соотношениями:

$$f_1 = (\overline{x}_1\overline{x}_2\overline{x}_3x_4) \oplus (\overline{x}_1x_2\overline{x}_3\overline{x}_4) \oplus (\overline{x}_1x_2\overline{x}_3x_4) \oplus (\overline{x}_1x_2x_3\overline{x}_4) \oplus$$
$$\oplus (\overline{x}_1x_2x_3x_4) \oplus (x_1\overline{x}_2\overline{x}_3\overline{x}_4) \oplus (x_1x_2\overline{x}_3x_4) \oplus (x_1x_2x_3x_4);$$

$$f_2 = (\overline{x}_1\overline{x}_2\overline{x}_3\overline{x}_4) \oplus (\overline{x}_1\overline{x}_2\overline{x}_3x_4) \oplus (\overline{x}_1x_2\overline{x}_3x_4) \oplus (\overline{x}_1x_2x_3\overline{x}_4) \oplus$$
$$\oplus (x_1\overline{x}_2\overline{x}_3x_4) \oplus (x_1\overline{x}_2x_3\overline{x}_4) \oplus (x_1x_2x_3\overline{x}_4) \oplus (x_1x_2x_3x_4);$$

$$f_3 = (\overline{x}_1\overline{x}_2\overline{x}_3x_4) \oplus (\overline{x}_1\overline{x}_2x_3\overline{x}_4) \oplus (\overline{x}_1x_2x_3x_4) \oplus (x_1\overline{x}_2\overline{x}_3x_4) \oplus$$
$$\oplus (x_1\overline{x}_2x_3\overline{x}_4) \oplus (x_1\overline{x}_2x_3x_4) \oplus (x_1x_2\overline{x}_3x_4) \oplus (x_1x_2x_3x_4);$$

$$f_4 = (\overline{x}_1\overline{x}_2\overline{x}_3x_4) \oplus (\overline{x}_1\overline{x}_2x_3\overline{x}_4) \oplus (\overline{x}_1x_2\overline{x}_3\overline{x}_4) \oplus (\overline{x}_1x_2x_3\overline{x}_4) \oplus$$
$$\oplus (x_1\overline{x}_2\overline{x}_3x_4) \oplus (x_1x_2\overline{x}_3\overline{x}_4) \oplus (x_1x_2\overline{x}_3x_4) \oplus (x_1x_2x_3\overline{x}_4);$$

б) Также булева функция обратного преобразования $X = f^{-1}(Y)_: GF(2)^4 \to GF(2)^4$ с соответствующей таблицей истинности выражается следующими соотношениями:

$$x_1 = (\overline{f}_1\overline{f}_2\overline{f}_3f_4) \oplus (\overline{f}_1\overline{f}_2f_3\overline{f}_4) \oplus (\overline{f}_1f_2\overline{f}_3f_4) \oplus (\overline{f}_1f_2f_3\overline{f}_4) \oplus$$
$$\oplus \overline{f}_1f_2f_3f_4) \oplus (f_1\overline{f}_2\overline{f}_3\overline{f}_4) \oplus (f_1f_2\overline{f}_3f_4) \oplus (f_1f_2f_3\overline{f_4});$$

$$x_2 = (\overline{f}_1\overline{f}_2\overline{f}_3f_4) \oplus (\overline{f}_1f_2\overline{f}_3f_4) \oplus (f_1\overline{f_2}\overline{f}_3f_4) \oplus (f_1\overline{f_2}f_3\overline{f}_4) \oplus$$
$$\oplus (f_1\overline{f}_2f_3f_4) \oplus (f_1f_2\overline{f_3}\overline{f}_4) \oplus (f_1f_2\overline{f_3}f_4) \oplus (f_1f_2f_3\overline{f_4});$$

$$x_3 = (\overline{f}_1\overline{f}_2\overline{f}_3\overline{f}_4) \oplus (\overline{f}_1\overline{f}_2f_3\overline{f}_4) \oplus (\overline{f}_1\overline{f_2}f_3f_4) \oplus (\overline{f}_1f_2\overline{f_3}f_4) \oplus$$
$$\oplus (\overline{f_1}f_2f_3\overline{f}_4) \oplus (f_1\overline{f}_2f_3\overline{f}_4) \oplus (f_1f_2\overline{f_3}f_4) \oplus (f_1f_2f_3\overline{f_4});$$

$$x_4 = (\overline{f}_1\overline{f}_2\overline{f}_3\overline{f}_4) \oplus (\overline{f}_1\overline{f}_2f_3\overline{f}_4) \oplus (\overline{f}_1f_2f_3f_4) \oplus (f_1\overline{f_2}f_3\overline{f}_4) \oplus$$
$$\oplus (f_1\overline{f}_2f_3f_4) \oplus (f_1f_2\overline{f_3}\overline{f}_4) \oplus (f_1f_2f_3\overline{f}_4) \oplus (f_1f_2f_3f_4).$$

На основах этих преобразований, задавая последовательность следующих возможных значений входных блоков:

$$(0)_{10} = (0000)_2 \le x = (x_1, x_2, x_3, x_4) \le (1111)_2 = (15)_{10}$$

образуются соответствующие таблицы, приведенные выше. Исследуя криптографические свойства этих булевых функций и их соответствующих таблиц, можно проверить выполнение третьего и четвертого условий сформулированного утверждения. Подсчитав количество нулей «0» и единиц «1» по столбцам, определяется равенства их количеств, следовательно,:

1) По определению следует выполнение свойства регулярности прямого и обратного преобразований;

2) Так же, исследуя значения этих таблиц, определяется независимость распределений выходных блоков относительно изменений входных блоков, т.е. устанавливается статистическая независимость изменения битов входных блоков относительно выходных;

3) От предыдущих особенностей, непосредственно заключается, что преобразования взаимно-однозначных соответствий обладают свойствами корреляционной иммунности и лавинного эффекта;

4) В выражениях булевых функций f_i , $i = 1,2,3;4;$ определенных таблицей истинности, соответствующих отображений $Y = f(X)_: GF(2)^4 \to GF(2)^4$, осуществив замены $\overline{x_i} = x_i \oplus 1$, $i = 1,2,3;4;$ и упростив полученные выражения получится сумма членов, содержащие конъюнкций переменных x_i, максимальное количество x_i в членах суммы определяет степени нелинейности преобразования;

5) В рассматриваемом преобразовании каждая функция f_i , $i = 1,2,3;$ содержит блок конъюнкции $x_1x_2x_3x_4$, а функция f_4 содержит $x_1x_2x_3\overline{x_4}$. Непосредственными вычислениями и упрошениями можно убедиться, что преобразование с заданной таблицей истинности, является максимально нелинейным;

6) В приведенном примере из свойства сюрективности установлены равномерные распределения выходных блоков и битов столбцов таблицы истинности, статистической независимости изменения битов входных блоков относительно выходных, обеспечат неэффективность криптоатак дифференциального и линейного анализа на шифрованные блоки.

Эти вычисления и их результаты справедливы для любого взаимно- однозначного преобразования: $Y = f(X)_: GF(2)^n \to GF(2)^m$, где $n = m$.

4. Четвертое требование обеспечит свойства стойкости преобразований относительно атак с использованием обратных преобразований алгоритма. В частности, ограничит криптографическую атаку: зная некоторую часть криптограмм, найти ключи раундов, вследствие исходного ключа.

Если базовые преобразования алгоритма не имеют односторонних преобразований, то пользуясь обратными преобразованиями можно моделировать средства, криптографической атаки для раскрытия нужной информации о ключах.

С теоретической точки зрения можно составить таблицу истинности любого преобразования, исходя из возможных входных блоков и соответствующих выходных блоков, на основе многочленов Жегалкина [14,15]. Но процесс много этапного (раундного) блочного шифрования с разными ключами раундов, обеспечит аналогичные свойства многозначной замены с соответствующими базовыми преобразованиями, с практической точки зрения, т.е. значительно усложняет моделирование обратных преобразований.

Стоит отметить, что сохраняя основные базовые преобразования, приведено универсальное правило модернизации алгоритмов блочных шифровании с симметричным ключом конструкции сети Фейстеля, с удлинением исходного ключа [13, 14]. Здесь же предложен новый алгоритм блочного шифрования с симметричным ключом, относящийся к конструкции сети Фейстеля с новыми базовыми преобразованиями.

Кроме, того в работах [12, 14] приведено универсальное правило, сохраняя основные преобразования алгоритма AES-FIPS 197, конструкция которого не основан на сети Фейстеля, его модернизации по удлинению ключа сохранением количество раундов. Здесь же предложен новый алгоритм блочного шифрования с симметричным ключом, который относится к конструкции AES-FIPS 197. Предложенный алгоритм позволяет эффективную модернизации по увеличению стойкости сохраняя базовые преобразования.

Анализ полученных результатов. Результаты, полученные по исследованию необходимых условий стойкости алгоритмов блочного шифрования с симметричным ключом, их обоснованные свойства и характеристики относительно обеспечения стойкости базовых преобразований, математические подходы и модели проверки приведенных необходимых условий, предложенные принципы и средства позволяют исследовать алгоритмы этого класса.

Возникающие отрицательные последствия при нарушении этих необходимых условий криптостойкости опробованы соответствующими примерами.

Заключение.

1. Определены критерии проверки, особенностей криптографической стойкости, моделей алгоритма симметричного блочного шифрования с симметричным ключом.
2. Обоснована криптографическая стойкость конструкции и базовых преобразований алгоритмов основанных на сети Фейстеля. Приведены методы эффективной модификации сети Фейстеля и базовых преобразований с увеличением длины ключа, но сохранением базовых преобразований.
3. Обоснованы криптографическая стойкость конструкции и базовых преобразований алгоритмов, не основанных на сети Фейстеля – конструкции AES-FIPS 197. Приведены методы эффективной модификации конструкции алгоритма класса AES-FIPS 197 и базовых преобразований с увеличением длины ключа, сохранением базовых преобразований.

Отмечается, что анализ преобразований алгоритмов класса блочного шифрования симметричным ключом по критериям сформулированного утверждения системным образом периодически углубляется и расширяется с развитием достижения науки, вычислительной техники и технологии.

ИСПОЛЬЗОВАННЫЕ ЛИТЕРАТУРЫ

1. Шнайер Б. (2003). Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: издательство ТРИУМФ, - 816 с.
2. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. (2002). Основы криптографии: Учебное пособие, 2-е изд. М.: Гелиос АРВ,.-480 с.
3. Шенон К. Э. (1963). Теория связи в секретных системах. Работы по теории информации и кибернетике. М.: ИЛ, том 1. С. 333-402.
4. Харин Ю. С., Берник В.И., Матвеев Г. В., Агиевич С. Г. (2003). Математические и комьютерные основы криптологии ООО «Новое знание» г. 381 стр.
5. Ростовцев А. Г., Маховенко Е. Б. (2004). Теоретическая криптография. НПО «Профессионал», Санкт-Петербург. 478 стр.
6. Молдовян А. А., Молдовян Н. А., Советов Б. Я. (2001). Криптография. Санкт-Петербург, Изд. «Лань». 224 с.
7. Акбаров, Д. Е., & Умаров, Ш. А. (2020). Анализ приложения логических операций к криптографическим преобразованиям средств обеспечения информационной безопасности. *Universum: технические науки*, (2-1 (71)).
8. Akbarov, D. E., & Umarov, S. A. (2021). Mathematical characteristics of application of logical operations and table substitution in cryptographic transformations. *Scientific-technical journal*, *4*(2), 6-14.
9. Akbarov D. E., Umarov Sh. A. (2020). Applying Logical Operations and table replacements in modeling basic transformations of Symmetric block encryption algorithms. *International Journal of Mechanical and Production Engineering Research and Development*. 10(3), 15041-15046.

10. Умаров, Ш. А., & Акбаров, Д. Е. (2016). Разработка нового алгоритма шифрования данных с симметричным ключом. *Журнал Сибирского федерального университета. Техника и технологии*, *9*(2).
11. Акбаров, Д. Е., Умаров, Ш. А., & Акбаров, Д. Є. (2016). Новый алгоритм блочного шифрования данных с симметричным ключом. Вісник НТТУ «КПІ». Серия ПРИЛАДОБУДУВАННЯ. Вип. 52(2).
12. Akbarov D. E. (2009). Cryptographic methods of ensuring information security and their application. Tashkent. p. 432.
13. Молдавян А. А., Молдавян Н. А. (2004). Криптография от примитивов к синтезу алгоритмов. СПб.: БХВ Петербург, 448 с.
14. Молдавян А. А., Молдавян Н. А., Гуц Н. Д., Изотов Б. В. (2004). Криптография: скоростные шифры. СПб.: БХВ Петербург, 496 с.
15. Зензин, О. С., & Иванов, М. А. (2002). Стандарт криптографической защиты AES. Конечные поля. *М.: Кудиц-Образ*, *176*, 15.
16. Abdurazakov, A., Makhmudova, N., & Mirzamakhmudova, N. (2021). On one method for solving degenerating parabolic systems by the direct line method with an appendix in the theory of filration.
17. Абдуразаков, А., Махмудова, Н., & Мирзамахмудова, Н. (2020). Численное решение методом прямых интеграла дифференцирования уравнений, связанных с задачами фильтрации газа. *Universum: технические науки*, (7-1 (76)), 32-35.
18. Абдуразаков, А., Махмудова, Н., & Мирзамахмудова, Н. (2019). Решения многоточечной краевой задачи фильтрации газа в многослойных пластах с учетом релаксации. *Universum: технические науки*, (11-1 (68)).
19. Мирзамахмудов, Т., & Умарова, Г. (2014). Некоторые вопросы основ местного самоуправления. In *Теория и практика развития экономики на международном, национальном, региональном уровнях* (pp. 222-224).
20. Мирзамахмудов, Т. М., Рахимов, Н. Р., Мусаев, Э. С., Гафуров, У. А., Бутаев, Т. Б., & Зокиров, Р. З. (1991). Датчик-зонд для определения влажности.
21. Shadimetov, K., & Daliyev, B. (2021, July). Composite optimal formulas for approximate integration of weight integrals. In *AIP Conference Proceedings* (Vol. 2365, No. 1, p. 020025). AIP Publishing LLC.
22. Шадиметов, Х. М., & Далиев, Б. С. (2020). Коэффициенты оптимальных квадратурных формул для приближенного решения общего интегрального уравнения Абеля. *Проблемы вычислительной и прикладной математики*, (2 (26)), 24-31.
23. Hayotov, A. R., Bozarov, B. I., & Abduganiev, A. (2018). Optimal formula for numerical integration on two dimensional sphere. *Uzbek Mathematical Journal*, *3*, 80-89.
24. Bozarov, B. I. (2019). An optimal quadrature formula with sinx weight function in the Sobolev space. *Uzbekistan Academy Of Sciences Vi Romanovskiy Institute Of Mathematics*, 47.
25. Hayotov, A., & Bozarov, B. (2021, July). Optimal quadrature formulas with the trigonometric weight in the Sobolev space. In *AIP Conference Proceedings* (Vol. 2365, No. 1, p. 020022). AIP Publishing LLC.
26. Hayotov, A., & Bozarov, B. (2021, July). Optimal quadrature formulas with the trigonometric weight in the Sobolev space. In AIP Conference Proceedings (Vol. 2365, No. 1, p. 020022). AIP Publishing LLC.

27. Hayotov, A., & Bozarov, B. (2021, July). Optimal quadrature formulas with the trigonometric weight in the Sobolev space. In AIP Conference Proceedings (Vol. 2365, No. 1, p. 020022). AIP Publishing LLC.

28. Alimjonova, G. (2021). Modern competencies in the techno-culture of future technical specialists. Current research journal of pedagogics (2767-3278), 2(06), 78-84.

29. Tillabayev, B., & Bahodirov, N. (2021). Solving the boundary problem by the method of green's function for the simple differential equation of the second order linear. *Academicia: An International Multidisciplinary Research Journal*, *11*(6), 301-304.

30. Kosimov, H., & Tillabaev, B. (2018). Mixed fractional order integral and derivatives for functions of many variables. *Scientific journal of the Fergana State University*, *1*(2), 5-11.

31. Ахмедова, Г. А., & Файзуллаев, Ж. И. (2014). Управление инновационной активностью промышленных предприятий на основе эффективных методов ее оценки и стимулирования. *Актуальные проблемы гуманитарных и естественных наук*, (4-1).

32. Fayzullaev, J. (2020). A systematic approach to the development of mathematical competence among students of technical universities. *European Journal of Research and Reflection in Educational Sciences Vol*, *8*(3).