РУХАНИ ЖАҢҒЫРУ

20 АСТАНА

ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Студенттер мен жас ғалымдардың
«ҒЫЛЫМ ЖӘНЕ БІЛІМ - 2018»
XIII Халықаралық ғылыми конференциясы

СБОРНИК МАТЕРИАЛОВ

XIII Международная научная конференция
студентов и молодых ученых
«НАУКА И ОБРАЗОВАНИЕ - 2018»

The XIII International Scientific Conference
for Students and Young Scientists
«SCIENCE AND EDUCATION - 2018»

12th April 2018, Astana

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Студенттер мен жас ғалымдардың «Ғылым және білім - 2018» атты XIII Халықаралық ғылыми конференциясының БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ XIII Международной научной конференции студентов и молодых ученых «Наука и образование - 2018»

PROCEEDINGS of the XIII International Scientific Conference for students and young scholars «Science and education - 2018»

2018 жыл 12 сәуір

Астана

УДК 378

ББК 74.58
Ғ 96

Ғ 96
«Ғылым және білім – 2018» атты студенттер мен жас ғалымдардың XIII Халықаралық ғылыми конференциясы = XIII Международная научная конференция студентов и молодых ученых «Наука и образование - 2018» = The XIII International Scientific Conference for students and young scholars «Science and education - 2018». – Астана: http://www.enu.kz/ru/nauka/nauka-i-obrazovanie/, 2018. – 7513 стр. (қазақша, орысша, ағылшынша).

ISBN 978-9965-31-997-6

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 378

ББК 74.58

ISBN 978-9965-31-997-6

УДК 519.6

ОБ ОДНОМ ПРИМЕНЕНИИ АВТОМОРФИЗМОВ В ШИФРОВАНИИ

Абдулина Ләззат Көшерғалиқызы
abdulina_lazzat@mail.ru
Студент 4 курса механико-математического факультета
ЕНУ им. Л.Н.Гумилева, Астана, Казахстан
Научный руководитель – К. Сулейменов

Одним из хорошо известных методов является кодирование сообщения применением многочлена. При этом многочлен, который используется в качестве ключа, определяется различными методами. К примеру, можно рассматривать примитивные многочлены или многочлены, определяемые как наименьшее общее кратное некоторых определенных многочленов.

В этой работе применяется многочлен, который строится через квазигруппу с единицей, точнее определяется как автоморфизм. Данный ключ рассекретить очень сложно, так как нужно иметь практически все параметры.

Шифрование — обратимое преобразование информации в целях сокрытия от неавторизованных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ней. Главным образом, шифрование служит задачей соблюдения конфиденциальности передаваемой информации. Важной особенностью любого алгоритма шифрования является использование ключа, который утверждает выбор конкретного преобразования из совокупности возможных для данного алгоритма [1-3].

Одно из самых важных понятий в шифровании – ключ. В распространённых схемах шифрования есть закрытый ключ, который хранится в секрете на вашем компьютере и позволяет читать адресованные вам сообщения. С помощью закрытого ключа также можно ставить на отправляемых сообщениях защищённую от подделки цифровую подпись. Открытый ключ – файл, которым вы можете делиться с другими или публиковать. Он позволяет людям обмениваться с вами шифрованными сообщениями и проверять ваши подписи. Закрытый и открытый ключи – парные [3].

В целом, шифрование состоит из двух составляющих — зашифровывание и расшифровывание.

Открытый текст – сообщение, подлежащее передаче адресату.

Автоморфизм – изоморфное отображение множества с данной системой операций и отношений на себя.

Шифром перестановки называется шифр, построенный по правилу: блок размера n, состоящий из символов алфавита открытого текста, меняется местами с другим блоком той же размерности. В результате исходное сообщение представляет собой те же самые блоки, но расставленные в псевдо-произвольном порядке. Ключом в таких криптосистемах является матрица (вектор), заданная в определенном кольце. При шифровании данных преобразуемый блок умножается на ключ. При расшифровке зашифрованные блоки умножаются на матрицу (вектор) обратной перестановки, которая является обратной к введенному в систему ключу.

Пусть $A \subset M_n(Z)$, где A - квадратная матрица $(A = D)$, $M_n(Z) = \{0,1,\ldots,n-1\}$, n – длина открытого сообщения. Если выполняется матричное равенство

$$\hat{x} \cdot A = A \cdot \hat{x},$$

то подстановка x называется автоморфизмом матрицы A.

Пример. Рассмотрим случай для $n=3$. Тогда $\sigma^i \equiv A_{D_i}$, $i=\overline{1,n}$, т.е. $\sigma^1 = E$, $\sigma^2 = A_{D_2}, \ldots, \sigma^n = A_{D_n}$

$$\sigma^1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\sigma^2 = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

$$\sigma^2 = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix}$$

$$\hat{x}_1 = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix}$$

$$\hat{x}_2 = \begin{pmatrix} 1 & 2 & 0 \\ 2 & 0 & 1 \\ 0 & 1 & 2 \end{pmatrix}$$

$$\hat{x}_3 = \begin{pmatrix} 2 & 0 & 1 \\ 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix}$$

Вычислим матрицу K (ключ):

$$K = \sigma^1 \cdot \hat{x}_1 + \sigma^2 \cdot \hat{x}_2 + \sigma^3 \cdot \hat{x}_3$$

$$K = \begin{pmatrix} 8 & 5 & 5 \\ 5 & 8 & 5 \\ 5 & 5 & 8 \end{pmatrix}$$

Выберем некоторую матрицу a - исходное сообщение:

$$a = (5,\ 8,\ 3)$$

$$a \cdot K = b$$

$$a \cdot K = (95,\ 89,\ 104)$$

Для нахождения матрицы a вычислим обратную матрицу K, затем умножим на вектор-строку b:

$$K^{-1} = \begin{pmatrix} 0{,}240741 & -0{,}09259 & -0{,}09259 \\ -0{,}09259 & 0{,}240741 & -0{,}09259 \\ -0{,}09259 & -0{,}09259 & 0{,}240741 \end{pmatrix}$$

$$a = b \cdot K^{-1}$$

Получаем исходное сообщение:

$a = (5,\quad 8,\quad 3)$

Список использованных источников

1. https://ssd.eff.org/ru/module/что-такое-шифрование
2. https://ru.wikipedia.org/wiki/Шифрование
3. Егоров В.Н. О группах автоморфизмов матриц, МГУ им. М.В.Ломоносова, г.Москва, Россия, 2010, 16 с.

ДИНАМИЧЕСКИЕ СВОЙСТВА ПРИВОДОВ ВИБРАЦИОННЫХ МАШИН

Алимжанов М.Д., Қайрош Қ.Қ.

Евразийский национальный университет им. Л.Н. Гумилёва г. Астана

Приводы вибрационных машин составляют важную часть их структуры. В анализе приводов вибрационных машин представляет интерес их самосинхронизация. Самосинхронизацией приводов вибровозбудителей вибрационных машин является установление одинаковой средней угловой скорости дебалансов, которые кинематически не связаны между собой. Синхронное вращение дебалансов в двухвальном механическом вибровозбудителе достигается вследствии взаимодействия их с подвижным несущим телом [1,2]. Согласованное вращение дебалансов, не смотря на различия в параметрах происходит при определенных условиях. Самосинхронизация изучается на основе нелинейной теории колебаний.

Особенности самосинхронизации приведем на примере модели дебаланса установленного в несущем теле (рисунок 1) .

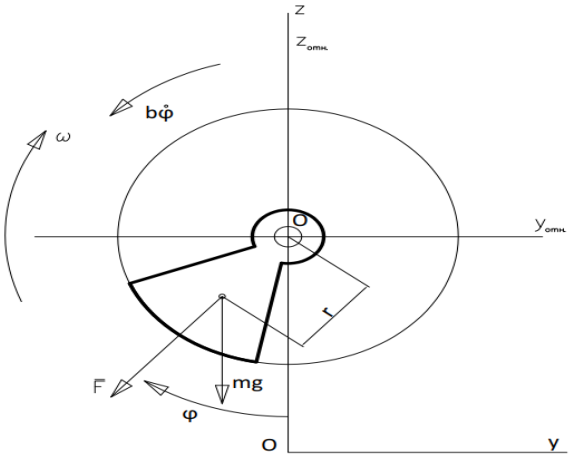

Рисунок 1- Модель дебаланса

Пусть угловые скорости вращения дебаланса и корпуса вибровозбудителя (несущее тело) равны ω. Вертикальные перемещения несущего тела имеют вид:

$$z = A\sin\omega t\,, \qquad (1)$$

где A - амплитуда колебаний,

ω - частота колебаний.

Дифференциальное уравнение относительно движения дебаланса представим так:

$$I\ddot{\varphi} + b\dot{\varphi} + mr\omega^2 A\cos\varphi\sin\omega t = mgr\cos\varphi\,, \qquad (2)$$