ПОДХОДЫ К РАЗРАБОТКЕ КРИПТОГРАФИЧЕСКОГО ИНТЕГРИРОВАННОГО АЛГОРИТМА ШИФРОВАНИЯ

Протодьяконова Г.Ю.[1], Стручков П.И.[2], Табырынов В.Ю.[3], Соловьев А.И.[4]

[1]Протодьяконова Галина Юрьевна – кандидат педагогических наук, заведующая кафедрой, кафедра эксплуатации и обслуживания информационных систем;
[2]Стручков Павел Иванович – студент;
[3]Табырынов Владислав Юрьевич – студент;
[4]Соловьев Александр Ильич – студент,
Северо–Восточный федеральный университет им. М.К. Аммосова, г. Якутск

Аннотация: *статья посвящена проблеме информационной безопасности, криптографической защите информации, проанализированы различные криптографические алгоритмы. Разработан интенгрированный алгоритм шифрования, который производит шифрование текста.*
Ключевые слова: *анализ, криптографический алгоритм, защита информации, информационная безопасность.*

Проблемы защиты информации настолько актуальны в настоящее время информационного бума, что быстро устаревают имеющиеся методы защиты информации, часто происходит утечка информации разными способами и конфиденциальная информация становится доступной для всех, секретная информация может стать открытой. И опасности в цифровом мире отображают опасности физического мира, также как существуют опасности хищений и растрат, то точно так же они существуют и в цифровом мире [1, с. 11]. Для решения этой проблемы возникает необходимость создания новых и надежных методов криптографической защиты информации.

В данной работе были исследованы и проанализированы методы криптографической защиты информации, проанализированы методы защиты информации, исследованы алгоритмы и методы защиты в криптографии, разработан интегрированный криптографический алгоритм. Шифрование и расшифрование информации производится в данной работе методом криптографии.

В процессе создания метода шифрования и расшифрования информации был использован разработанный нами алгоритм.

В результате исследования мы пришли к выводу, что создаваемый нами алгоритм можно использовать для передачи конфиденциальной информации. Его принцип работы заключается в том, что он шифрует всё за счет преобразования текста в бессмысленный текст.

Для создания криптографического метода при выборе исходного текста можно взять любой текст. Берется требуемый алфавит, русский, английский или какой-либо другой. В данном случае используется русский. Каждая буква алфавита нумеруется арабскими цифрами последовательно (например: а-1, б-2, в-3 и т.д.).

Придумывается ключ - любое число, назовем его «*X»,* дадим ему значение 8. Берем какое-либо слово, которое требуется зашифровать, например «*ГДЕ»*.

Из слова получаем порядковые номера из алфавита, для слова «*ГДЕ»* будет 4, 5 и 6. Каждая буква будет шифроваться по отдельности, назовем текущую букву *«Y».* Используется формула:

$$y*x-x \qquad (1)$$

Если полученное после шифрования число больше количества букв в алфавите, то нужно это число поделить на количество букв в алфавите, в нашем случае 33. Затем округляем полученное число в меньшую сторону, это число будет вторым ключом для расшифрования, а остаток используем в качестве зашифрованной буквы.

Но если число, полученное после шифрования меньше, чем количество букв в алфавите, второй ключ к букве будет равен 0.

После зашифровывания всех букв из слова *«ГДЕ»* мы получили:

Зашифрованные буквы: 24, 32, 7. Вторые ключи к ним: 0, 0, 1.

Приведем пример шифрования буквы Е (рис. 1).

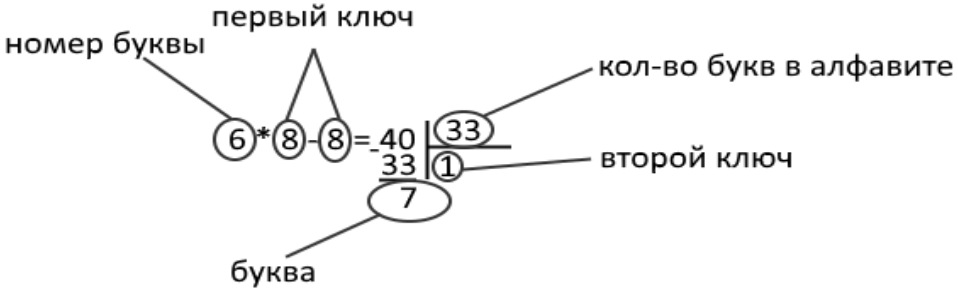

Рис. 1. Пример шифрования буквы Е

Для расшифрования нам потребуется использовать формулу:

$$(((z*33)+y)+x)/x \qquad (2)$$

где z – второй ключ, который мы получили при шифровании.

И после расшифрования мы обратно получили цифры 4, 5 и 6, которые соответствуют по алфавиту буквам Г, Д, Е, которые образуют исходный текст *«ГДЕ»*.

Проведенное исследование подтвердило криптостойкость алгоритма. Таким образом, можно сделать вывод о том, что созданный метод криптографии может быть эффективным средством для защиты информации.

Список литературы

1. *Шнейер Брюс*. Секреты и ложь. Безопасность данных в цифровом мире. Классика Computer Science, 2003. № 2 (42). 256 с.
2. *Панасенко Сергей*. Алгоритмы шифрования. Специальный справочник. БХВ-Петербург, 2009. № 2 (42). 74 с.
3. *Сингх Саймон*. Книга шифров. Безопасность данных в цифровом мире. «Аванта+», 2009. № 2 (42). 90 с.