ПРОГРАММА ДЛЯ ИЗУЧЕНИЯ ШИФРОВ ПРОСТОЙ ЗАМЕНЫ

А.М. Абросимов, М.Б. Абросимов

ФГБОУ ВО Саратовский государственный технический университет имени Гагарина Ю.А., Саратов, Россия

ФГБОУ ВО Саратовский научный исследовательский государственный университет имени Н.Г. Чернышевского, Саратов, Россия

Знакомство с шифрами для старшеклассников или студентов младших курсов начинается обычно с простейших шифров простой замены, которыми являются шифры Цезаря и Атбаш [1]. Часто связанные с такими шифрами задачи встречаются и на олимпиадах по криптографии. Для удобства знакомства с шифрами Цезаря и Атбаш была разработана описываемая далее программа, которая позволяет выполнять шифрование, расшифрование, а также помогает в дешифровании.

В классическом варианте шифр Цезаря выполняет замену буквы алфавита на букву, которая расположена в алфавите со сдвигом на заданное число позиций. Таким образом, для русского языка ключом является число от 1 до 33.

В шифре Атбаш происходит замена буквы на букву, которая расположена в такой же позиции как исходная, но с конца алфавита. В исходном варианте шифра Атбаш ключа нет.

В описанных вариантах шифров Цезаря и Атбаш дешифровка не представляет сложности. В Интернете доступны онлайн-калькуляторы, которые справляются с этой задачей. Усилением шифров Цезаря и Атбаш является перемешивание алфавита, которое состоит в том, что в определенную позицию записывается ключевое слово, не содержащее повторяющихся букв, а после выписываются оставшиеся буквы алфавита. В таком варианте дешифровка становится нетривиальной задачей. Если криптограмма является достаточно большой по размеру, то можно применять методы частотного анализа [1], в том числе и автоматизированные с использованием словаря [2]. Однако для коротких криптограмм (длиной меньше 800 символов) это сделать сложно.

Разработанная программа позволяет выполнять шифрование и расшифрование шифрами Цезаря и Атбаш с перемешиванием алфавита. Однако основной интерес представляет функция дешифровки и определения ключа, который был использован при шифровании. Эта функция реализована в полуавтоматическом режиме и позволяет облегчить формирование гипотез и их проверку для выполнения дешифровки, что оказывается наиболее интересным в процессе обучения и понимания криптоанализа для старшеклассников, студентов младших курсов, обучающихся по информационной безопасности, либо студентов иных направлений, у которых есть предмет по информационной безопасности.

Список литературы

1. Введение в криптографию / Под общ. ред. В.В. Ященко. М.: МЦНМО, 2012. 348 с.

2. Абросимов М.Б., Коннова А.Д., Толмилов Д.А. О криптоанализе шифров простой замены с использованием словаря // Технические средства защиты информации : тез. докл. XIX Белорусско-российской науч.-техн. конф., Минск, 8 июня 2021 г. С. 14.