МИНОБРНАУКИ РОССИИ
САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
ЭЛЕКТРОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
«ЛЭТИ» ИМ. В.И. УЛЬЯНОВА (ЛЕНИНА)
Кафедра МО ЭВМ

ОТЧЕТ

по лабораторной работе №1

“Изучение классических шифров Caesar, Permutation/Transposition, Hill”

Вариант 8

Студент гр. 8382 Мирончик П.Д.

Преподаватель Племянников А.К.

Санкт-Петербург

2021

Заключение Caesar

Был изучен шифр Caesar и способы работы с ним в программе CrypTool 1.

В качестве примера был зашифрован текст `mironchik` и для сдвига 1 получен результат `njspodijl`. Определено, что Caesar является шифром с заменой, имеет ключ в виде числа, не превышающего мощность алфавита m, и неустойчив к атакам грубой силы, которые имеют сложность $O(m)$. Рассмотрен способ атаки на шифротекст с использованием гистограмм распределения частот на тексте файла `CrypTool-en.txt`, изучен инструмент проведения автоматической атаки, реализованный в CrypTool 1. В результате проведения пробной атаки текст был успешно дешифрован и получен верный исходный текст.

Заключение Permutation/Transposition

В ходе выполнения работы был рассмотрен шифр Permutation/Transposition.

Определено, что шифр Permutation/Transposition является шифром с перестановкой. Ключем к шифру является перестановка столбцов, перестановка строк и очередность выполнения перестановок, а сложность атаки “грубой силы” составляет $O(n! * m!)$, где n, m - количество строк и столбцов матрицы. Рассмотрены инструменты работы с шифром в программе CrypTool 1: шифрование/дешифрование, поиск ключа с учетом известного исходного текста. Также через официальные документ помощи рассмотрены способы атаки на шифр средствами CrypTool 2: алгоритм грубой силы, Crib Analysis, генетический алгоритм и алгоритм восхождения.

Коллегой была проведена успешная атака на текст *DEAR colleague TNAHKS*, зашифрованный одинарной перестановкой по столбцам *(3,4,1,2),* при том, что коллеге были известны префикс и постфикс шифруемого текста, а также то, что перестановка была одинарной.

Заключение Hill

В ходе выполнения работы был исследован шифр Хилла.

Определено, что этот шифр является симметричным блочным шифром с заменой, сложность атаки грубой силы на который составляет n^{m*m} в худшем случае.

В работы описано использование шифра средствами CrypTool 1 на примере зашифрования и расшифрования текста *DEAR MIRONCHIK PAVEL DENISOVICH THANK YOU VERY MUCH* и ключа-матрицы размером 3×3.

Далее была проведена атака на шифр на основе известного исходного текста средствами CrypTool 1 и восстановлен верный ключ зашифрования.

После этого из исходного и зашифрованного текстов была удалена часть, содержащая *MIRONCHIK PAVEL DENISOVICH*, и проведена повторная зашифровка и расшифровка, в результате которой успешно был получен ключ шифрования.

В конце была проведена атака коллеги по тем же принципам: удаление средней, неизвестной части и использование оставшихся частей в качестве текста. В результате атаки так же был успешно получен исходный ключ шифрования.