Национальный исследовательский университет информационных технологий,
механики и оптики.
Кафедра вычислительной техники.
Методы и средства защиты компьютерной информации.

Лабораторная работа №1

Моноалфавитные подстановки.

11 вариант

Работу выполнил студент группы P3415
Халанский Дмитрий

2017

1. Цель работы

Дешифрация криптограммы, зашифрованной с использованием метода моноалфавитных подстановок, с помощью частотного анализа.

2. Исходный текст

ЗНОЙ БЫЛ НЕСТЕРПИМ ПО ПРЕЖНЕМУ ОН КАК БУДТО ВИСЕЛ НАД САМОЙ ЗЕМЛЕЙ ГУСТЫМ ТЯЖЕЛЫМ СЛОЕМ НА ТЕМНО СИНЕМ НЕБЕ КАЗАЛОСЬ КРУТИЛИСЬ КАКИЕ ТО МЕЛКИЕ СВЕТЛЫЕ ОГОНЬКИ СКВОЗЬ ТОНЧАЙШУЮ ПОЧТИ ЧЕРНУЮ ПЫЛЬ ВСЕ МОЛЧАЛО БЫЛО ЧТО ТО БЕЗНАДЕЖНОЕ ПРИДАВЛЕННОЕ В ЭТОМ ГЛУБОКОМ МОЛЧАНИИ ОБЕССИЛЕННОЙ ПРИРОДЫ Я ДОБРАЛСЯ ДО СЕНОВАЛА И ЛЕГ НА ТОЛЬКО ЧТО СКОШЕННУЮ НО УЖЕ ПОЧТЯ ВЫСОХШУЮ ТРАВУ

3. Ключ

А	Р	**Й**	Б	**Т**	Ы	**Ы**	Й
Б	А	**К**	Н	**У**	И	**Э**	Ж
В	М	**Л**	Т	**Ф**	Д	**Ю**	К
Г	_	**М**	Л	**Х**	З	**Я**	О
Д	Ь	**Н**	Х	**Ц**	Ч	_	П
Е	Э	**П**	С	**Ч**	У		
Ж	Г	**Р**	Я	**Ш**	Ю		
З	В	**С**	Ш	**Щ**	Е		

4. Краткий протокол криптоанализа

Г Заменим на пробел согласно частотному анализу.

Я Заменим на *О* по частотному анализу.

Щ Заменим на *Е* по частотному анализу.

К У нескольких слов `К` и `КК` стоят перед `ОЕ`. Предполагаем, что это `ННОЕ` и `НОЕ`.

У Одно из слов оканчивается на `Н-`, причём последние две буквы одинаковые. Это могут быть `НЕЕ`, `НИИ`, `НЯЯ`. По частотному анализу *И* ближе, чем *Я*.

Б Видим несколько предлогов `Н-`. Так как мы уже нашли буквы *О*, *Е*, *И*, это не «но», «не» или «ни». Остаются варианты «ни», «ну», «на», «ню». Выбираем «на», потому что *А* наиболее близко по частотному анализу.

Й, Х, Ф Видим слово `-Е-НА-Е-НОЕ`. Предполагаем *БЕЗНАДЕЖНОЕ*. Появляется много правильных слов. Делаем вывод, что решение верное.

П, М, Ы Видим слово `ОБЕ-И-ЕННО-`. Предполагаем *ОБЕССИЛЕННОЙ*.