МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

НАБЕРЕЖНОЧЕЛНИНСКИЙ ИНСТИТУТ (ФИЛИАЛ)
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО АВТОНОМНОГО
ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «КАЗАНСКИЙ (ПРИВОЛЖСКИЙ) ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

ОТДЕЛЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ЭНЕРГЕТИЧЕСКИХ СИСТЕМ

Направление подготовки: 01.03.02– Прикладная математика и информатитка

ОТЧЕТ
VI СЕМЕСТР

Дисциплина: «Защита информации»

Выполнил:
студент Баходыров У.,
группа 2181101 курс 4

Проверил:
доцент, к.ф.-м.н.
М.Я. Товштейн

Набережные Челны – 2022

СОДЕРЖАНИЕ

1. МОНОАЛФАВИТНАЯ ЗАМЕНА

При такой замене каждой букве алфавита открытого текста ставится в соответствие одна буква шифротекста из этого же алфавита.

Таблица 1 – Замена кириллицы на числа

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
15	16	17	18	19	20	21	22	23	24	25	26	27

Ы	Ь	Э	Ю	Я
28	29	30	31	32

1.1. Шифр атбаш

Принцип метода: первая буква алфавита – А заменяется на последнюю – Я, вторая буква – Б заменяется на предпоследнюю Ю и так далее.

Недостаток этого метода: частота появления букв открытого и шифротекста одна и та же.

Алиса: Баходыров Умиджан

Исходный текст:ЗАЩИТА ИНФОРМАЦИИ

Ключ: русский алфавит(Таб.1)

Шифротекст: ЧЯЁЦМЯ ЦСКРОТЯИЦЦ

Боб: Алиса: Баходыров Умиджан

Шифротекст:ЮЯЧЯ ЫЯССДЙ

*Ключ:*русский алфавит(Таб.1)

Исходный текст:БАЗА ДАННЫХ

1.2. Шифр Цезаря

Тогда шифрование можно выразить формулой:

$$Ш_i = (T_i + K) \bmod N.$$

Расшифрование выполняется по формуле

$$T_i = (Ш_i - K + N) \bmod N.$$

Алиса: Баходыров Умиджан

Исходный текст: МАТЕМАТИКА

Ключ: К = 5, русский алфавит (буквы нумеруются с нуля).

Тогда шифрование можно выразить формулой:

$$Ш_i = (T_i + K) \bmod N.$$

Шифротекст: СЕЧЙСЕЧНПЕ

Боб: Алиса: Баходыров Умиджан

Шифротекст: ЩЛТЛЫХФ

Ключ: К =7, русский алфавит (буквы нумеруются с нуля).$Ш_i = (T_i + K) \bmod N$.

Расшифрование выполняется по формуле

$T_i = (Ш_i - K + N) \bmod N$.

Исходный текст: ТЕЛЕФОН

1.3. Шифр Гронсфельда

Алиса: Баходыров Умиджан

Исходный текст: КОМПЮТЕР

Ключ: пароль – 22729

русский алфавит (буквы нумеруются с нуля).

Шифротекст: МРУСЖФЖЧ

Боб: Алиса: Баходыров Умиджан

Шифротекст: ОФЩЛРЙР

Ключ: пароль –46175, русский алфавит (буквы нумеруются с нуля).

Исходный текст: КОШЕЛЁК

1.4. Шифр Полибия

Таблица 2 – Таблица Полибия для кириллицы

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

Алиса: Баходыров Умиджан

Исходный текст:Я.ТАКСИ

Ключ: таблица Полибия для кириллицы, строк – 7, столбцов – 5 (таблица 2); смещение вверх – 3, смещение влево – 4.

Шифротекст:МО?ТЫ!Ь

Боб: Алиса: Баходыров Умиджан

Шифротекст:ФЛЬЛРЭУР

Ключ: таблица Полибия для кириллицы, строк – 5, столбцов – 7 (таблица 2); смещение вниз –1, смещение вправо – 3.

Исходный текст: КАРАНТИН

1.5. Шифр Тритемия

Алиса: Баходыров Умиджан

Исходный текст: КЛАВИАТУРА

Ключ: таблица Тритемия для кириллицы, строк – 5, столбцов – 7 (таблица 3); каждая буква заменена соответствующей ей снизу, пароль: *МЕГАФОН*

Шифротекст:ХЦЁКТЁЪЬШЁ

Таблица 3 – Таблица Тритемия для кириллицы

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

Боб: ***Алиса:*** Баходыров Умиджан

Шифротекст:ХЧЦПГЧЁ

Ключ: таблица Тритемия для кириллицы, строк – 5, столбцов – 7 (таблица 3); каждая буква заменена соответствующей ей снизу, пароль: ТЕТРАДЬ

Исходный текст:МОНИТОР

Таблица 3.2 – Таблица Тритемия для кириллицы

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