## Лабораторная работа № 7. Элементы криптографии. Однократное гаммирование

Радикорский Павел Михайлович, НФИбд-03-18

Лабораторная работа № 7. Элементы криптографии. Однократн	oe
гаммирование	11.12.2021
Содержание	
Цели и задачи	4
Выполнение	5

Выводы

7

Список иллюстраций											
гаммирование	11.12.2021										
Лабораторная работа № 7. Элементы криптографии. Однократное											

	_			·
	Список		CTHAILL	<i>A</i> 1 <i>A</i>
١	LINCUR	טונונוע	ківаци	71 PI
			P	

1.	Функция шифрования	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	5
2.	Функция расшифрования .																							5
3.	Функция получения ключа																							6

## Цели и задачи

Цель: Освоить на практике применение режима однократного гаммирования

## Выполнение

Функция шифрования. Задаем алфавит из заглавных, строчных букв русского алфавита, !, ?, ., , и пробела. На вход поступает открытый текст, в виде массива символов, и ключ — гамму. Анализируем длину текста, «растягиваем» гамму до нужного размера и выполняем посимвольное сложение.

```
In [1]: import re

In [19]: alphabet = list ('Aa668errAneeEexx33MuMMKxdnMbdHHOONnPpCcTrYyooxxduv+dBuduabababa39MoRm ,!')

In [22]: def encrypt (text, gamma): textlen = len(text) gammalen = len(gamma)

keyText = [] for in range (textlen // gammalen): for symb in gamma: keyText.append(symb)

for in range (textlen & gammalen): keyText.append(gammalen): code = []

for in range (textlen): code.append(alphabet(alphabet.index(text[i]) + alphabet.index(keyText[i])) % 71])

return (print(*code, sep = ''))

In [26]: encrypt('C Hobbom Fogom, Apysapi', 'AäAAAAAAAAAAAAAAAAAAAA)')

C3Hobbom Fogom, Apysapi'
```

Рис. 1: Функция шифрования

Функция расшифрования Работает аналогично. «Растягиваем» гамму и выполняем посимвольное вычитание ее из текста.

Рис. 2: Функция расшифрования

Функция, которая определяет ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста. Работает аналогично функции расшифрования, но на вход поступает не зашифрованный текст и ключ, а зашифрованный и открытый текст

Рис. 3: Функция получения ключа

## Выводы

В результате выполнения работы я освоил на практике применение режима однократного гаммирования.