

Правительство Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»
(НИУ ВШЭ)

Московский институт электроники и математики им. А.Н. Тихонова

ОТЧЕТ
О ПРАКТИЧЕСКОЙ РАБОТЕ № 1
по дисциплине «Математические основы защиты информации»
Подстановочные шифры

Студент гр. БИБ 201
К.Ш.Ёркулов
«19» март 2022 г.

Руководитель
Заведующий кафедрой информационной
безопасности кибер физических систем
канд. техн. наук, доцент
_____ О.О. Евсютин
«__» _____ 2022 г.

Москва 2022

СОДЕРЖАНИЕ

1 Задание на практическую работу	3
2 Краткая теоретическая часть	4
2.1 Описание шифров	4
3 Примеры шифрования	5
4 Программная реализация шифров	6
5 Примеры криптоанализа	7
7 Список использованных источников	9

1 Задание на практическую работу

Целью данной работы является приобретение навыков программной реализации и криптоанализа применительно к блочному шифру Хилла.

В рамках практической работы необходимо выполнить следующее:

Написать программную реализацию для следующих шифров:

1. - шифр простой замены;
2. - аффинный шифр;
3. - аффинный рекуррентный шифр;

Изучить методы криптоанализа моноалфавитных подстановочных шифров с использованием дополнительных источников;

Провести криптоанализ данных шифров;

2 Краткая теоретическая часть

2.1 Описание шифров

Шифр простой замены

Очередной шифр, относящийся к группе одно алфавитных шифров подстановки. Ключом шифра служит перемешанный произвольным образом алфавит. Например, ключом может быть следующая последовательность букв:

XFQABOLYWJGPMRVIHUSDZKNTEC.

При шифровании каждая буква в тексте заменяется по следующему правилу. Первая буква алфавита замещается первой буквой ключа, вторая буква алфавита — второй буквой ключа и так далее. В нашем примере буква *A* будет заменена на *X*, буква *B* на *F*.

При расшифровке буква сперва ищется в ключе и затем заменяется буквой стоящей в алфавите на той же позиции.

Аффинный шифр

Описание [\[править \]](#)

Здесь буквы алфавита размером m сначала сопоставляются с целыми числами в диапазоне $0 \dots m - 1$. Затем он использует модульную арифметику для преобразования целого числа, которому соответствует каждая текстовая буква, в другое целое число, соответствующее букве зашифрованного текста. Функция шифрования для одной буквы

$$E(x) = (ax + b) \bmod m$$

где модуль m — размер алфавита, a и b — ключи шифра. Значение a должно быть выбрано таким образом, чтобы a и m были сопростыми. Функция расшифровки

$$D(x) = a^{-1}(x - b) \bmod m$$

где a^{-1} — модульный мультипликатив, обратный модулю m . Т.е. он удовлетворяет уравнению

$$1 = aa^{-1} \bmod m$$

Мультипликативная обратная a существует только в том случае, если a и m являются копростыми. Следовательно, без ограничения на a расшифровка может быть невозможна. Можно показать следующим образом, что функция расшифровки является обратной функции шифрования,

$$\begin{aligned} D(E(x)) &= a^{-1}(E(x) - b) \bmod m \\ &= a^{-1}((ax + b) \bmod m - b) \bmod m \\ &= a^{-1}(ax + b - b) \bmod m \\ &= a^{-1}ax \bmod m \\ &= x \bmod m \end{aligned}$$

Аффинный рекуррентный шифр

Аффинный рекуррентный шифр похож на простой Аффинный, но в рекуррентном шифре для каждой буквы, начиная с третьей, ключи составляются новые. Новые ключи рассчитываются по формуле:

$$\alpha_i = (\alpha_{i-2} \alpha_{i-1}) \bmod m; \beta_i = (\beta_{i-2} + \beta_{i-1}) \bmod m,$$

А $\alpha_1, \alpha_2, \beta_1, \beta_2$ – исходные ключи шифрования, заданные изначально.

3 Примеры шифрования

Сделаем шифрование для всех 3 шифров слово: LINUX

Шифр простой замены

Мы меняем слово из алфавита на наш ключ алфавит,

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
R	N	M	Z	U	J	C	X	Q	V	K	D	L	S	U	A	T	W	P	F	I	E	B	G	O	H

Слово: LINUX

Полученное слово: DQSIG

Аффинный шифр

Зададим $\alpha = 7$ и $\beta = 13$, все будет проходить по модулю 26, так как используется английский алфавит.

Шифрование будет проходить по формуле $y_i = (\alpha x_i + \beta) \bmod m$

Дешифрование будет проходить по формуле $x_i = (\alpha y_i + \beta) \bmod m$

Процесс шифрования:

X = LINUX

Счет букв начинается с 0 элемента. Например, если будет 15 это будет элемент (P)

X = (11, 8, 13, 20, 23)

$$y_1 = (7 * 11 + 13) \bmod 26 = 12 \text{ (M)}$$

$$y_2 = (7 * 8 + 13) \bmod 26 = 17 \text{ (R)}$$

$$y_3 = (7 * 13 + 13) \bmod 26 = 0 \text{ (A)}$$

$$y_4 = (7 * 20 + 13) \bmod 26 = 23 \text{ (X)}$$

$$y_5 = (7 * 23 + 13) \bmod 26 = 18 \text{ (S)}$$

А при вычислении у мы начинаем с 1 элемента. Например, если будет 26 элемент, то будет первая буква алфавита (А)

Полученное слово: $y = MRAXS$

ПРОЦЕСС ДЕШИФРОВАНИЯ:

Будет осуществляться по формуле $x_i = (y_i - \beta_i)\alpha^{-1}$

α^{-1} Будет вычисляться по расширенному алгоритму Евклида, и значение $7^{-1} = (11) \bmod 26$

$$x_1 = (12 - 13)7^{-1} \bmod 26 = 11(L)$$

$$x_2 = (17 - 13)7^{-1} \bmod 26 = 8(I)$$

$$x_3 = (0 - 13)7^{-1} \bmod 26 = 13(N)$$

$$x_4 = (23 - 13)7^{-1} \bmod 26 = 20(U)$$

$$x_5 = (18 - 13)7^{-1} \bmod 26 = 23(X)$$

На этом и заканчивается процесс шифрования и дешифрования аффинного шифра

Аффинный рекуррентный шифр

Суть аффинного рекуррентного шифра заключается в том, что в рекуррентном шифре для каждой буквы, начиная с третьей, ключи составляются новые. Формула для нее была приведена в пункте 2.1

Зашифруем тоже самое слово LINUX. Для этого добавим значения $\alpha_2 = 11$ и $\beta_2 = 10$, а для $\alpha_1 = 7$ и $\beta_1 = 13$ оставим те же значения.

Начнем процесс шифрования:

$X = LINUX (11, 8, 13, 20, 23)$

$$y_1 = (7 * 11 + 13) \bmod 26 = 12 (M)$$

$$y_2 = (11 * 8 + 10) \bmod 26 = 20 (U)$$

$$y_3 = (25 * 13 + 23) \bmod 26 = 10 (K)$$

$$\alpha_3 = \alpha_2 * \alpha_1 \bmod 26 = 11 * 7 \bmod 26 = 25$$

$$\beta_3 = \beta_2 + \beta_1 \bmod 26 = 13 + 10 \bmod 26 = 23$$

$$y_4 = (15 * 20 + 7) \bmod 26 = 21 (V)$$

$$\alpha_4 = \alpha_3 * \alpha_2 \bmod 26 = 25 * 11 \bmod 26 = 15$$

$$\beta_4 = \beta_3 + \beta_2 \bmod 26 = 23 + 10 \bmod 26 = 7$$

$$y_5 = (11 * 23 + 4) \bmod 26 = 23 (X)$$

$$\alpha_5 = \alpha_4 * \alpha_3 \bmod 26 = 15 * 25 \bmod 26 = 11$$

$$\beta_5 = \beta_4 + \beta_3 \bmod 26 = 7 + 23 \bmod 26 = 4$$

Полученное слово: $y = MUKVX$

ПРОЦЕСС ДЕШИФРОВАНИЯ:

Будет осуществляться по формуле $x_i = (y_i - \beta_i) \alpha_i^{-1}$

$$x_1 = (12 - 13) 7^{-1} \bmod 26 = 11 (L)$$

$$x_2 = (20 - 10) 11^{-1} \bmod 26 = 8 (I)$$

$$x_3 = (10 - 23) 25^{-1} \bmod 26 = 13 (N)$$

$$\alpha_3 = \alpha_2 * \alpha_1 \bmod 26 = 7 * 11 \bmod 26 = 25$$

$$\beta_3 = \beta_2 + \beta_1 \bmod 26 = 13 + 10 \bmod 26 = 23$$

$$x_4 = (21 - 7) 15^{-1} \bmod 26 = 20 (U)$$

$$\alpha_4 = \alpha_3 * \alpha_2 \bmod 26 = 25 * 11 \bmod 26 = 15$$

$$\beta_4 = \beta_3 + \beta_2 \bmod 26 = 23 + 10 \bmod 26 = 7$$

$$x_5 = (6 - 13) 7^{-1} \bmod 26 = 23 (X)$$

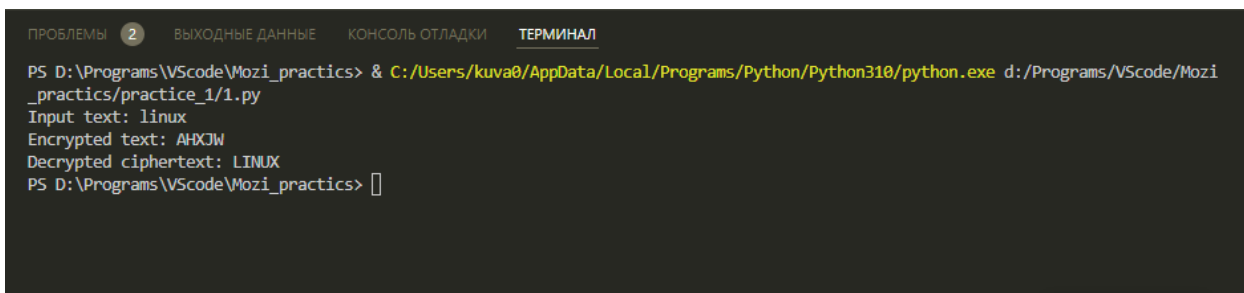
$$\alpha_5 = \alpha_4 * \alpha_3 \bmod 26 = 15 * 25 \bmod 26 = 19$$

$$\beta_5 = \beta_4 + \beta_3 \bmod 26 = 13 + 10 \bmod 26 = 23$$

Получено $X = LINUX$, значит дешифровка была успешна проведена.

4 Программная реализация шифров

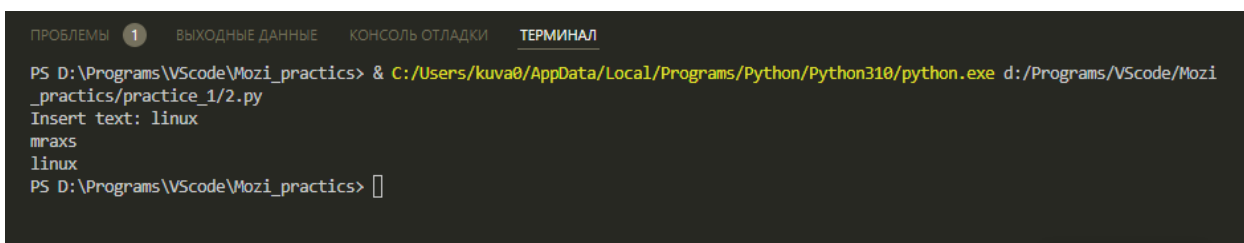
На примере программной реализации **шифра простой замены** мы использовали слово LINUX и далее на скриншотах 1.1 можно увидеть как произошел процесс шифрования и расшифрования соответственно.



```
ПРОБЛЕМЫ 2 ВЫХОДНЫЕ ДАННЫЕ КОНСОЛЬ ОТЛАДКИ ТЕРМИНАЛ
PS D:\Programs\VScode\Mozi_practics> & C:/Users/kuva0/AppData/Local/Programs/Python/Python310/python.exe d:/Programs/VScode/Mozi_practics/practice_1/1.py
Input text: linux
Encrypted text: AHXJW
Decrypted ciphertext: LINUX
PS D:\Programs\VScode\Mozi_practics>
```

Рис 1.1 Шифрование слова LINUX на программной реализации **шифра простой замены**

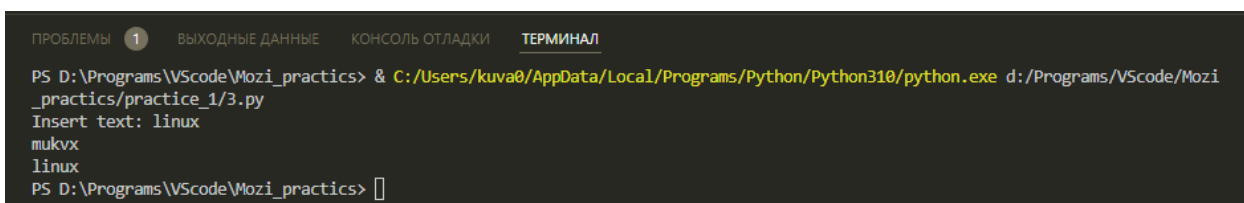
Далее рассмотрим программную реализацию аффинного шифра, тут также будет использовано слово LINUX, а ключом будет $\alpha = 7, \beta = 13$ соответственно.



```
ПРОБЛЕМЫ 1 ВЫХОДНЫЕ ДАННЫЕ КОНСОЛЬ ОТЛАДКИ ТЕРМИНАЛ
PS D:\Programs\VScode\Mozi_practics> & C:/Users/kuva0/AppData/Local/Programs/Python/Python310/python.exe d:/Programs/VScode/Mozi_practics/practice_1/2.py
Insert text: linux
mrxs
linux
PS D:\Programs\VScode\Mozi_practics>
```

Рис 1.2 Шифрование слова LINUX на программной реализации **аффинного шифра**

На последнем этапе рассмотрим программную реализацию аффинного рекуррентного шифра, в данном случае будет использоваться по 2 ключа: $\alpha_1 = 7, \beta_1 = 13; \alpha_2 = 11, \beta_2 = 10$



```
ПРОБЛЕМЫ 1 ВЫХОДНЫЕ ДАННЫЕ КОНСОЛЬ ОТЛАДКИ ТЕРМИНАЛ
PS D:\Programs\VScode\Mozi_practics> & C:/Users/kuva0/AppData/Local/Programs/Python/Python310/python.exe d:/Programs/VScode/Mozi_practics/practice_1/3.py
Insert text: linux
mukvx
linux
PS D:\Programs\VScode\Mozi_practics>
```

Рис 1.3 Шифрование слова LINUX на программной реализации **аффинного рекуррентного шифра**

Подводя итог нужно отметить то что, при ручном шифровании и программной реализации шифрование и расшифрование совпали.

5 Примеры криптоанализа

```
PS D:\Programs\VScode\mozi_practics> python .\crypt_affine.py -i d0rDY
Possible encryption hack:
Key pair A: 7 B: 11
Decrypted message:
linux
```

Рисунок 1.4 Пример криптоанализа зашифрованного текста аффинного шифра

```
Tried Key pair A1: 7 A2: 11 B1: 10 B2: 8 Text: l-s\#
Tried Key pair A1: 7 A2: 11 B1: 10 B2: 9 Text: lr9t!
Tried Key pair A1: 7 A2: 11 B1: 10 B2: 10 Text: lX^~
Tried Key pair A1: 7 A2: 11 B1: 10 B2: 11 Text: l>$E|
Tried Key pair A1: 7 A2: 11 B1: 10 B2: 12 Text: l$I]z
Tried Key pair A1: 7 A2: 11 B1: 10 B2: 13 Text: linux
Possible encryption hack:
Key pair A1: 7 A2: 11 B1: 10 B2: 13
Decrypted message:
linux

Enter D for done, or just press Enter to continue hacking:
> D
```

Рисунок 1.5 Пример криптоанализа зашифрованного текста аффинного рекуррентного шифра

Как можно видеть в обоих шифрах была расшифровка методом грубой силы, и подобраны ключи.

```
PS D:\Programs\VScode\MOZI\Practice_1> & C:/Users/kuva0/AppData/Local/Programs/Python/Python310/python.exe d:/Programs/VScode/MOZI/Practice_1/crypt_sub.py
length of string (only letters) is: 5079398
{'Z': '0.07 %', 'Q': '0.09 %', 'J': '0.13 %', 'X': '0.19 %', 'K': '0.65 %', 'V': '1.03 %', 'B': '1.44 %', 'Y': '1.78 %', 'G': '1.91 %', 'P': '1.95 %', 'W': '1.99 %', 'F': '2.38 %', 'M': '2.5 %', 'U': '2.73 %', 'C': '2.85 %', 'L': '3.91 %', 'D': '4.25 %', 'H': '5.8 %', 'R': '6.09 %', 'S': '6.59 %', 'I': '7.2 %', 'N': '7.26 %', 'O': '7.62 %', 'A': '8.03 %', 'T': '9.07 %', 'E': '12.48 %'}
{'Z': 0.07, 'Q': 0.09, 'J': 0.13, 'X': 0.19, 'K': 0.65, 'V': 1.03, 'B': 1.44, 'Y': 1.78, 'G': 1.91, 'P': 1.95, 'W': 1.99, 'F': 2.38, 'M': 2.5, 'U': 2.73, 'C': 2.85, 'L': 3.91, 'D': 4.25, 'H': 5.8, 'R': 6.09, 'S': 6.59, 'I': 7.2, 'N': 7.26, 'O': 7.62, 'A': 8.03, 'T': 9.07, 'E': 12.48}
PS D:\Programs\VScode\MOZI\Practice_1> 
```

Рисунок 1.6 Пример частотного криптоанализа шифра простой замены

6 Выводы о проделанной работе

Шифр простой замены

Шифр простой замены прост для понимания и применения, эту часть бы я отвел к достоинству данного шифра, недостатком же будет являться то что данный шифр не использует практически никто и он прост для Брут форса и взломать данный шифр можно взломать без тяжелого вреда.

Аффинный шифр

Главной слабостью аффинного шифрования давно признана его недостаточная стойкость к взлому. Основными методами вскрытия шифра являются частотный анализ и полный перебор, хотя могут применяться и иные подходы. Даже при использовании слабой по современным меркам вычислительной техники раскрытие кодовых сообщений происходит моментально. Потому практическое значение аффинных шифров невелико.

Аффинный рекуррентный шифр

Аффинный рекуррентный шифр похож на аффинный, но в аффинном рекуррентном шифре для каждой буквы, начиная с третьей, ключи составляются новые.

Данные шифры не столь трудны в понимании и применении, так как они уже считаются устаревшими. Для начального изучения по рекомендовал бы начать с данных шифров.

7 Список использованных источников

- Шифр простой замены, источник: <https://habr.com/ru/post/271257/>, здесь были еще и другие шифры
- Подробное описание шифра аффинного и шифра простой замены приведены в книге: КРИПТОГРАФИЯ И ВЗЛОМ ШИФРОВ НА PYTHON, *автор*: ЭЛ СВЕЙГАРТ
- Подробное описание и реализация шифров аффинного и шифра простой замены приведены в зарубежном учебнике: Hacking Secret Ciphers with Python, *автор*: Al Sweigart
- Подробное описание аффинного шифра приведено на сайте википедии: [Аффинный шифр — Википедия \(wikipedia.org\)](https://ru.wikipedia.org/wiki/Аффинный_шифр)