ЛАБОРАТОРНАЯ РАБОТА №1
«КРИПТОГРАФИЯ»
Вариант 2

Плотников Антон, А3401

Санкт-Петербург, 2017

Задача 1. Шифровка дихеши с использование военного шифра второй половины XIX века.

1. Зашифровать депешу: ”*Милостивый государь! Войны начинаются в умах людей. Из преамбулы Устава ЮНЕСКО. Целью войны является мир. Аристотель. Москва. С истинным почтением имею честь быть!*”. При шифровании необходимо реализовать все возможности данного алгоритма шифрования, повышающие его криптостойкость.

2. Укажите хотя бы три недостатка используемых шифрообозначений в данном конкретном шифре.

Решение. Для начала исключим из исходного текста частоупотребимые стандартные фразы:

Войны начинаются в умах людей. Из преамбулы Устава ЮНЕСКО. Целью войны является мир. Аристотель.

Зашифруем исходный текст по словарю:

152 640 364 565 364 693 457 140 485 100 520 320 690 185 300 283 400 424 109 139 320 640 494 100 690 369 440 307 554 690 152 640 695 140 329 213 457 351 100 429 440 472 463 320 660

Вставим в шифр несколько пустышек:

152 640 364 752 565 364 693 457 140 831 485 100 520 831 320 690 185 300 900 283 400 424 109 139 320 640 494 845 100 690 369 440 777 307 554 690 152 640 983 695 140 329 213 457 900 351 100 429 900 440 472 765 463 320 799 660

Вставим в шифр несколько намеренных ошибок и групп-уточнителей после них пустышек:

152 640 364 752 565 364 693 457 140 831 485 100 520 831 320 690 185 300 900 283 400 454 675 239 631 424 109 139 320 640 494 845 100 690 369 440 777 307 554 690 152 640 983 695 140 329 213 457 900 351 100 420 675 239 631 429 900 440 472 765 463 320 799 660

Недостатки шифра:

1. Небольшая частотность пустышек в тексте, из-за чего их можно установить.

2. Шифр возможно разгадать с помощью частотного анализа.

3. При шифровании большого числа сообщений таким словарем снижается криптоустойчивость (легче применить частотный анализ).

Задача 2. Зашифровать депешу с использованием секретного телеграфного ключа шефа жандармов.

Ключ № 15.

Императору. Унция эмоций стоит тонны фактов. Джон Джунор. 1 января 1900.

Решение. Решение получено автоматически:

```python
#!/bin/python3

d = {
    'а': '60',
    'б': '73',
    'в': '85',
    'г': '98',
    'д': '11',
    'е': '24',
    'ё': '37',
    'ж': '50',
    'з': '63',
    'и': '76',
    'й': '89',
    'к': '02',
    'л': '15',
    'м': '28',
    'н': '41',
    'о': '54',
    'п': '67',
    'р': '80',
    'с': '93',
    'т': '06',
    'у': '19',
    'ф': '32',
    'х': '45',
    'ц': '58',
    'ч': '71',
    'ш': '84',
    'щ': '97',
    'ъ': '10',
    'ы': '23',
    'ь': '36',
    'э': '49',
    'ю': '62',
    'я': '75'
}

for c in input().lower():
    if c in d:
        print(d[c], end=' ')
```

Зашифрованный текст:

Императору — 15 19 41 58 76 75 49 28 54 58 76 89 93 06 54 76 06 06 54 41 41 23 32 60 02 06 54 85 — Джон Джунор. 1 января 1900.

Задача 3. Зашифровать депешу с использованием агентурного шифра системы ”шифр Цезаря”.

Исходный текст: влияние рассеянного немонохроматичного излучения низкой интенсивности на углеродистые стали (Воздействие лунного света на рельсы).

Решение. Решение получено автоматически:

```
#!/bin/python3

d = {
    'а': '60',
    'б': '73',
    'в': '85',
    'г': '98',
    'д': '11',
    'е': '24',
    'ё': '37',
    'ж': '50',
    'з': '63',
    'и': '76',
    'й': '89',
    'к': '02',
    'л': '15',
    'м': '28',
    'н': '41',
    'о': '54',
    'п': '67',
    'р': '80',
    'с': '93',
    'т': '06',
    'у': '19',
    'ф': '32',
    'х': '45',
    'ц': '58',
    'ч': '71',
    'ш': '84',
    'щ': '97',
    'ъ': '10',
    'ы': '23',
    'ь': '36',
    'э': '49',
    'ю': '62',
    'я': '75'
}

for c in input().lower():
    if c in d:
        print(d[c], end=' ')
```

Зашифрованный текст:

юзеыйеб мьннбыййкяк йбикйксмкиьоеуйкяк едзубйеы йеджкё ейобйнеюйкное йь язбмкаеночб ноьзе юкдабёноюеб зййкяк нюбоь йь мбзшнч

Задача 4. Начинающий криптограф составил шифр простой многозначной замены, который частично приведён ниже. Усовершенствуйте данный шифр, используя таблицу частот встречаемости букв и биграмм в тексте, таким образом, чтобы:

1. повысить криптостойкость шифра
2. устранить избыточность

	1	2	3	4	5
			...		
В	298	434	653	789	
			...		
Ж	867	545	357	875	423
			...		
ка	324	813			
			...		
Т	719	965	693		
			...		
яа	122				

Решение. 1. Буква ”Ж” встречается очень редко (8 %), достаточно использовать два кода для её шифрования.

2. Следует добавить еще кодов для шифрования букв ”Т” и ”В”, поскольку они встречаются в 60 % и 71 % случаев, соответственно.
3. Биграма ”ка” встречается часто (8 раз), следует увеличить число кодов до 3 или 4.
4. Биграма ”яа” вообще ни разу не встречается следует исключить ее из таблицы кодирования.

	1	2	3	4	5
			...		
В	298	434	653	789	423
			...		
Ж	867	545			
			...		
ка	324	813	122		
			...		
Т	719	965	693	875	357
			...		
яа					

Задача 5. Зашифровать слово ”*Криптография*” с использованием книжного шифра, используя все возможности повышения криптостойкости.

Решение. Зашифрованный текст:

6-3 14-4 2-6 2-22 14-6 15-2 4-2 10-1 8-2 1-2 10-19

Задача 6. Зашифровать фразу-палиндром, используя шифр перестановок.
Палиндром: ”*АРГЕНТИНА МАНИТ НЕГРА*”

1	2	3	4	5	6	7
7	6	1	3	2	5	4

Решение. Решение получено автоматически:

```
#!/bin/python3

d = [7, 6, 1, 3, 2, 5, 4]

s = "АРГЕНТИНАМАНИТНЕГРАДО"
result = ['*'] * len(s)

for i, c in enumerate(s):
    result[(d[i % 7] - 1) + 7 * (i // 7)] = c

print(''.join(result))
```

Зашифрованный текст:
ГНЕИТРАМНАТИАНГАРОДЕН

Задача 7. Зашифровать депешу с использованием биграммного шифра.
Депеша: *”СКЗИ — средство криптографической защиты информации.”*

Решение. Расположим текст на транспоранте периода $T = 24$.

с	к	з	и	-	с	р	е	д	с	т	в	о	к	р	и	п	т	о	г	р	а	ф	и
ч	е	с	к	о	й	з	а	щ	и	т	ы	и	н	ф	о	р	м	а	ц	и	и	а	л

Зашифрованный текст:

8980 416 225 234 9981 887 627 2154 3826 1967 843 982 1521 533 4736 744 2924 6132 903 490 629 186 7235 1243 990 168 2789

Задача 8. Зашифровать часть депеши, заключенной в кавычки, используя биклавный шифр.
Часть депеши: ”*Перлюстрация*-”

Решение. Первый ключ: 24-12-1877 $\to$ 13 $\to$ 3
Второй ключ: 2
Составим таблицу ключей для каждого символа

п	е	р	л	ю	с	т	р	а	ц	и	я	-
3	5	2	4	1	3	5	2	4	1	3	5	2

Зашифрованный текст:
6Ы М2 4Е 5А Н2 М7 7Ъ 4Е 9Е Ё8 4Ф 2Ц 7Д

Задача 9. Исправить противоречия в правах доступа.

Решение. Таблица

	File1 (1)	File2 (2)	File3 (3)
User1 (1)	RW	-	W
User2 (2)	-	RW	W
User3 (3)	R	R	RW
User4 (4)	R	RW	W

Задача 10. Определить результаты предоставления доступа в автоматизированной системе с мандатным принципом разграничения доступа.

Решение. Таблица

Субъект	Операция	Объект	Результат
User1	R	File1	+
User1	W	File1	+
User2	R	File4	+
User2	W	File3	-
User3	W	File3	-
Admin	R	File1	-
User4	R	File12	-
User5	W	File11	-

Задача 11. Придумайте запоминающийся лозунг, состоящий из десяти букв, и зашифруйте нижеприведенное сообщение с использованием простого квадратного шифра.

Сообщение: ”*АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ*”

Решение. В качестве лозунга выбрана фраза ”*Хороший мак*”.

	1	2	3	4	5	6	7	8	9	0
1	**х**	ц	ч	ш	щ	ъ	ы	ь	э	ю
2	**о**	п	р	с	т	у	ф	х	ц	ч
3	**р**	с	т	у	ф	х	ц	ч	ш	щ
4	**о**	п	р	с	т	у	ф	х	ц	ч
5	**ш**	щ	ъ	ы	ь	э	ю	я	а	б
6	**и**	й	к	л	м	н	о	п	р	с
7	**й**	к	л	м	н	о	п	р	с	т
8	**м**	н	о	п	р	с	т	у	ф	х
9	**а**	б	в	г	д	е	ё	ж	з	и
0	**к**	л	м	н	о	п	р	с	т	у

Зашифрованный текст:

19 29 39 49 59 69 79 89 99 16 26 36 46 56 66 76 86 96 23 33 43 53 63 73 83 93 25 35 45 55 65 75 85

Задача 12. Придумать запоминающийся периодический ключ и зашифровать сообщение шифром Виженера.
Сообщение: ”*Информационная безопасность*”

Решение. Таблица

п	л	а	н	е	т	а
17	13	1	15	6	20	1

и	н	ф	о	р	м	а	ц	и	о	н	н	а
10	15	22	16	18	14	1	24	10	16	15	15	1
я	б	е	з	о	п	а	с	н	о	с	т	ь
33	2	6	9	16	17	1	19	15	16	19	20	30

Зашифрованный текст:

27 28 23 31 24 34 2 41 23 17 30 21 21 34 19 19 10 31 23 21 20 32 29 20 35 36