**ЛАБОРАТОРНАЯ РАБОТА 2**

**ШИФРОВАНИЕ С ИСПОЛЬЗОВАНИЕМ СИСТЕМ ЦЕЗАРЯ**

**И СИСТЕМЫ ТРИСЕМУСА**

***Аффинная система подстановок Цезаря***

При шифровании с использованием аффинной системы подстановок Цезаря буква с порядковым номером *t* в соответствующем алфавите заменяется на букву, порядковый номер которой в этом же алфавите рассчитывается по формуле (*at* + *b*) mod *m*, где *a*, *b* – числовые ключи, а *m* – количество букв в алфавите.

При выборе ключа *a* необходимо учитывать следующее требование: *a* и *m* должны быть взаимно простыми числами, то есть наибольший общий делитель *a* и *m* должен быть равен 1.

Рассмотрим пример шифрования сообщения «ПРИЛЕТАЮ ЗАВТРА» с использованием аффинной системы подстановок Цезаря.

Ключи шифрования примем следующими: *a* = 4, *b* = 2. Так как количество букв в алфавите *m* = 33, то требование к выбору ключа *a* соблюдается.

В первую очередь построим таблицу соответствия порядковых номеров букв исходного текста и шифртекста в соответствии с формулой (табл. 1). Нумерация букв начинается с 0.

Т а б л и ц а 1

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ***t*** | ***4t + 2*** | ***t*** | ***4t + 2*** | ***t*** | ***4t + 2*** | ***t*** | ***4t + 2*** |
| 0 | 2 | 9 | 5 | 18 | 8 | 27 | 11 |
| 1 | 6 | 10 | 9 | 19 | 12 | 28 | 15 |
| 2 | 10 | 11 | 13 | 20 | 16 | 29 | 19 |
| 3 | 14 | 12 | 17 | 21 | 20 | 30 | 23 |
| 4 | 18 | 13 | 21 | 22 | 24 | 31 | 27 |
| 5 | 22 | 14 | 25 | 23 | 28 | 32 | 31 |
| 6 | 26 | 15 | 29 | 24 | 32 |  |  |
| 7 | 30 | 16 | 0 | 25 | 3 |  |  |
| 8 | 1 | 17 | 4 | 26 | 7 |  |  |

Затем на основании табл. 1 построим таблицу соответствия конкретной букве исходного текста буквы шифртекста для заданных ключей шифрования (табл. 2).

Т а б л и ц а 2

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ⇒ | | ⇒ | | ⇒ | | ⇒ | |
| А | в | И | е | С | з | Ъ | к |
| Б | ё | Й | и | Т | л | Ы | о |
| В | й | К | м | У | п | Ь | т |
| Г | н | Л | р | Ф | у | Э | ц |
| Д | с | М | ф | Х | ч | Ю | ъ |
| Е | х | Н | ш | Ц | ы | Я | ю |
| Ё | щ | О | ь | Ч | я |  |  |
| Ж | э | П | а | Ш | г |  |  |
| З | б | Р | д | Щ | ж |  |  |

Соответствующим образом заменив буквы исходного текста

«ПРИЛЕТАЮ ЗАВТРА», получим шифртекст «АДЕРХЛВЪБВЙЛДВ».

**Содержание заданий**

***Задание 1***

Зашифруйте сообщение «МЫ ДОЛЖНЫ ПРИЗНАТЬ ОЧЕВИДНОЕ: ПОНИМАЮТ ЛИШЬ ТЕ, КТО ХОЧЕТ ПОНЯТЬ», используя систему Цезаря со значением ключа соответствующим номеру варианта (например, для варианта 10 – ключ *К* = 10).

***Задание 2***

Зашифруйте сообщение «СМЫСЛ ЖИЗНИ НАШЕЙ – НЕПРЕРЫВНОЕ ДВИЖЕНИЕ», используя аффинную систему подстановок Цезаря с ключами, согласно своему варианту (табл. 3).

Т а б л и ц а 3

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Вариант | Ключ | Вариант | Ключ | Вариант | Ключ |
| 1 | *a* = 5, *b* = 1 | 10 | *a* = 7, *b* = 2 | 19 | *a* = 5, *b* = 4 |
| 2 | *a* = 2, *b* = 5 | 11 | *a* = 8, *b* = 2 | 20 | *a* = 7, *b* = 4 |
| 3 | *a* = 4, *b* = 7 | 12 | *a* = 2, *b* = 3 | 21 | *a* = 8, *b* = 3 |
| 4 | *a* = 2, *b* = 10 | 13 | *a* = 4, *b* = 2 | 22 | *a* = 4, *b* = 6 |
| 5 | *a* = 7, *b* = 1 | 14 | *a* = 5, *b* = 3 | 23 | *a* = 5, *b* = 6 |
| 6 | *a* = 8, *b* = 1 | 15 | *a* = 7, *b* = 3 | 24 | *a* = 7, *b* = 5 |
| 7 | *a* = 2, *b* = 4 | 16 | *a* = 8, *b* = 4 | 25 | *a* = 8, *b* = 6 |
| 8 | *a* = 4, *b* = 10 | 17 | *a* = 2, *b* = 2 |  |  |
| 9 | *a* = 5, *b* = 2 | 18 | *a* = 4, *b* = 5 |  |  |

***Задание 3***

Выполните шифрование сообщения «РАЗУМА ЛИШАЕТ НЕ СОМНЕНИЕ, А УВЕРЕННОСТЬ», используя систему шифрования Цезаря с ключами, соответствующими варианту.

1. *k* = 1, ключевое слово «РАДОСТЬ».

2. *k* = 2, ключевое слово «УСПЕХ».

3. *k* = 3, ключевое слово «УДАЧА».

4. *k* = 4, ключевое слово «ЛЕТО».

5. *k* = 5, ключевое слово «ВЕСНА».

6. *k* = 6, ключевое слово «ЗИМА».

7. *k* = 7, ключевое слово «ОСЕНЬ».

8. *k* = 8, ключевое слово «АЛГОРИТМ».

9. *k* = 9, ключевое слово «ПРОГРАММИРОВАНИЕ».

10. *k* = 10, ключевое слово «КРИПТОГРАФИЯ».

11. *k* = 11, ключевое слово «КРИПТОАНАЛИЗ».

12. *k* = 12, ключевое слово «ШИФРТЕКСТ».

13. *k* = 13, ключевое слово «ОРЕХИ».

14. *k* = 14, ключевое слово «ТЕЛЕФОН».

15. *k* = 15, ключевое слово «КОМПЬЮТЕР».

16. *k* = 16, ключевое слово «ЧАСЫ».

17. *k* = 17, ключевое слово «МУЗЫКА».

18. *k* = 18, ключевое слово «РУЧКА».

19. *k* = 19, ключевое слово «ИНФОРМАЦИЯ».

20. *k* = 20, ключевое слово «РАБОТА».

21. *k* = 21, ключевое слово «СОЛНЦЕ».

22. *k* = 22, ключевое слово «ПЕРЕМЕНЫ».

23. *k* = 23, ключевое слово «ЖИЗНЬ».

24. *k* = 24, ключевое слово «ЛАБОРАТОРНАЯ».

25. *k* = 25, ключевое слово «СПРАВОЧНИК».

***Задание 4***

Выполните шифрование сообщения «УСПЕХ – ЭТО КОГДА ТЫ ДЕВЯТЬ РАЗ УПАЛ, НО ДЕСЯТЬ РАЗ ПОДНЯЛСЯ», используя систему Трисемуса с ключевым словом из задания 3. Размер таблицы подстановок 4 × 8.