**Лабораторная работа № 2**

**Тема:** шифрование и использованием метода Цезаря и системы Трисемуса.

**Цель работы:** формирование умений шифрования с использованием систем Цезаря и системы Трисемуса.

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).

1. Сначала сформируем таблицу подстановок, содержащую соответствующие пары букв исходного текста и шифртекста с ключ шифрования 17:

Таблица 1 – таблица подстановок (от «а» до «о»)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ↓ | а | б | в | г | д | е | ё | ж | з | и | й | к | л | м | н | о |
| р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я |

Таблица 2 – таблица подстановок (от «п» до «я»)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ↓ | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я |
| а | б | в | г | д | е | ё | ж | з | и | й | к | л | м | н | о | п |

1. Произведём замену букв исходного текста на соответствующие буквы из нижней строки и получим шифртекст «ЭЛФЯЬЧЮЛАБЩШЮРГМЯЗХТЩФЮЯХАПЯЮЩЭРОГЬЩИМГХЫГЯЁЯЗХГАЯЮГМ»

Задание 2. Зашифруйте сообщение «СМЫСЛ ЖИЗНИ НАШЕЙ – НЕПРЕРЫВНОЕ ДВИЖЕНИЕ», используя аффинную систему подстановок Цезаря с ключами, согласно своему варианту

Вариант 17: a = 2, b = 2

1) Построим таблицу соответствия порядковых номеров букв исходного текста и шифртекста в соответствие с формулой (at + b) mod m (таблица 3).

Таблица 3 – Таблица соответсвия порядковых номеров букв исходного текста и шифртекста (m = 33).

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

2) На основании таблицы 3 построим таблицу соответствия конкретной букве исходного текста буквы шифртекста для заданных ключей шифрования (таблица 4).

Таблица 4 – Таблица соответствия конкретной букве исходного текста буквы шифртекста для заданных ключей шифрования.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| → | | → | | → | | → | |
| а | в | и | у | с | е | ъ | ц |
| б | д | й | х | т | ж | ы | ш |
| в | ё | к | ч | у | и | ь | ъ |
| г | з | л | щ | ф | к | э | ь |
| д | й | м | ы | х | м | ю | ю |
| е | л | н | э | ц | о | я | а |
| ё | н | о | я | ч | р |  |  |
| ж | п | п | б | ш | т |  |  |
| з | с | р | г | щ | ф |  |  |

3) Заменим буквы исходного текста «СМЫСЛ ЖИЗНИ НАШЕЙ – НЕПРЕРЫВНОЕ ДВИЖЕНИЕ», получим шифртекст «ЕЫШЕЩПУСЭУЭВТЛХЭЛБГЛГШЁЭЯЛЙЁУПЛЭУЛ»

Задание 3. Выполните шифрование сообщения «РАЗУМА ЛИШАЕТ НЕ СОМНЕНИЕ, А УВЕРЕННОСТЬ», используя систему шифрования Цезаря с ключами, соответствующими варианту.

Вариант 17: k = 17, ключевое слово «МУЗЫКА».

1) Запишем ключевое слово в таблицу подстановок.

Таблица 5 – Таблица подстановок с ключевым словом

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № | → | | № | → | | № | → | | № | → | |
| 0 | а |  | 9 | и |  | 18 | с | у | 27 | ъ |  |
| 1 | б |  | 10 | й |  | 19 | т | з | 28 | ы |  |
| 2 | в |  | 11 | к |  | 20 | у | ы | 29 | ь |  |
| 3 | г |  | 12 | л |  | 21 | ф | к | 30 | э |  |
| 4 | д |  | 13 | м |  | 22 | х | а | 31 | ю |  |
| 5 | е |  | 14 | н |  | 23 | ц |  | 32 | я |  |
| 6 | ё |  | 15 | о |  | 24 | ч |  |  |  |  |
| 7 | ж |  | 16 | п |  | 25 | ш |  |  |  |  |
| 8 | з |  | 17 | р | м | 26 | щ |  |  |  |  |

2) Запишем оставшиеся буквы алфавита

Таблица 6 – Заполненная таблица подстановок

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № | → | | № | → | | № | → | | № | → | |
| 0 | а | н | 9 | и | ч | 18 | с | у | 27 | ъ | е |
| 1 | б | о | 10 | й | ш | 19 | т | з | 28 | ы | ё |
| 2 | в | п | 11 | к | щ | 20 | у | ы | 29 | ь | ж |
| 3 | г | р | 12 | л | ъ | 21 | ф | к | 30 | э | и |
| 4 | д | с | 13 | м | ь | 22 | х | а | 31 | ю | й |
| 5 | е | т | 14 | н | э | 23 | ц | б | 32 | я | л |
| 6 | ё | ф | 15 | о | ю | 24 | ч | в |  |  |  |
| 7 | ж | х | 16 | п | я | 25 | ш | г |  |  |  |
| 8 | з | ц | 17 | р | м | 26 | щ | д |  |  |  |

3) В результате шифрования исходного сообщения «РАЗУМА ЛИШАЕТ НЕ СОМНЕНИЕ, А УВЕРЕННОСТЬ» с использованием данной системы шифрования получим шифртекст:

«МНЦЫЬНЪЧГНТЗЭТУЮЬЭТЭЧТНЫПТМТЭЭЮУЗЖ»

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 («МУЗЫКА»). Размер таблицы подстановок 4 × 8.

1) Построчно впишем ключевое слово в таблицу, затем дополним таблицу не вошедшими в неё буквами алфавита по порядку (таблица 7).

Таблица 7.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| м | у | з | ы | к | а | б | в |
| г | д | е | ж | и | й | л | н |
| о | п | р | с | т | ф | х | ц |
| ч | ш | щ | ъ | ь | э | ю | я |

2) При шифровании с помощью этой таблицы исходного сообщения «УСПЕХ – ЭТО КОГДА ТЫ ДЕВЯТЬ РАЗ УПАЛ, НО ДЕСЯТЬ РАЗ ПОДНЯЛСЯ» будет получен шифртекст:

«ДЪШРЮАЬЧИЧОПЙЬЖПРНВЬКЩЙЕДШЙХЦЧПРНВЬКЩЙЕШЧПЦВХЪВ»

**Контрольные вопросы**

1. В чем особенность шифров простой замены?

При шифровании заменой (подстановкой) символы шифруемого текста заменяются символами того же или другого алфавита с заранее установленным правилом замены. В шифрах простой замены (одноалфавитной подстановки) каждый символ исходного текста заменяется символами того же алфавита одинаково на всем протяжении текста.

2. Чем отличаются система шифрования Цезаря и аффинная система подстановок Цезаря?

Система шифрования Цезаря использует как ключи количество букв алфавита шифруемого слова, уменьшенное на 1, и числа степени смешения заменяющих букв.

Аффинная система подстановок Цезаря в свою очередь использует перестановку в соответствии с порядковым номеров букв в алфавите и формулой (at + b) mod m, определяющей индекс заменяющих букв.

3. Какие требования предъявляются к выбору ключей для аффинной системы подстановок Цезаря?

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.

4. Для каких шифров простой замены используется составной ключ?

Составные ключи используется в системах шифрования Трисемуса (составной ключ содержит некоторое число и ключевое слово) и Цезаря с ключевым словом (составной ключ включает ключевое слово и размер таблицы подстановок).

5. Каким образом заполняется таблица подстановок для шифрования с использованием системы Трисемуса?

В таблицу сначала по строкам вписывается ключевое слово, причем повторно встречающиеся в нем буквы не записываются. Затем эта таблица дополняется не вошедшими в нее буквами алфавита по порядку.