**ЛАБОРАТОРНАЯ РАБОТА 2**

**Шифрование с использованием систем Цезаря**

**и системы Трисемуса**

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

Вариант 4

Задание 1

Зашифруйте сообщение «МЫ ДОЛЖНЫ ПРИЗНАТЬ ОЧЕВИДНОЕ: ПОНИМАЮТ ЛИШЬ ТЕ, КТО ХОЧЕТ ПОНЯТЬ», используя систему Цезаря со значением ключа соответствующим номеру варианта (вариант 4 – ключ K= 4 ).

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **А** | **Б** | **В** | **Г** | **Д** | **Е** | **Е** | **Ж** | **З** | **И** | **Й** | **К** | **Л** | **М** | **Н** | **О** | **П** |
| Д | Е | Е | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У |
| **Р** | **С** | **Т** | **У** | **Ф** | **Х** | **Ц** | **Ч** | **Ш** | **Щ** | **Ъ** | **Ы** | **Ь** | **Э** | **Ю** | **Я** |  |
| Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г |  |

Зашифрованное сообщение :’РЯ ЗТПКСЯ УФМЛСДЦА ТЫИЕМЗСТИ УТСМРДВЦ ПМЬА ЦИ, ОЦТ ЩТЫИЦ УТСГЦА’

Задание 2

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

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

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| t | 2t+10 | t | 2t+10 | t | 2t+10 | t | 2t+10 |
| **А** | Й | **И** | Ы | **С** | М | **Ъ** | Ю |
| **Б** | Л | **Й** | Э | **Т** | О | **Ы** | А |
| **В** | Н | **К** | Я | **У** | Р | **Ь** | В |
| **Г** | П | **Л** | Б | **Ф** | Т | **Э** | Д |
| **Д** | С | **М** | Г | **Х** | Ф | **Ю** | Е |
| **Е** | У | **Н** | Е | **Ц** | Ц | **Я** | З |
| **Е** | Х | **О** | Ж | **Ч** | Ш |  |  |
| **Ж** | Ч | **П** | И | **Ш** | Ъ |  |  |
| **З** | Щ | **Р** | К | **Щ** | Ь |  |  |

Зашифрованное сообщение: «МАГМБ ЧЫЩЕЫ ЕЙЪУЭ – ЕИКУУКАНЕЖУ СНЫЧУЕЫУ»

Задание 3

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

4.k=4, ключевое слово «ЛЕТО».

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| номер |  | | номер |  | | номер |  | | номер |  | |
| 0 | **А** | Ь | 9 | **И** | Б | 18 | **С** | К | 27 | **Ъ** | Ч |
| 1 | **Б** | Э | 10 | **Й** | В | 19 | **Т** | М | 28 | **Ы** | Ч |
| 2 | **В** | Ю | 11 | **К** | Г | 20 | **У** | Н | 29 | **Ь** | Ш |
| 3 | **Г** | Я | 12 | **Л** | Д | 21 | **Ф** | П | 30 | **Э** | Щ |
| 4 | **Д** | Л | 13 | **М** | Е | 22 | **Х** | Р | 31 | **Ю** | Ъ |
| 5 | **Е** | Е | 14 | **Н** | Ж | 23 | **Ц** | С | 32 | **Я** | Ы |
| 6 | **Е** | Т | 15 | **О** | З | 24 | **Ч** | У |  |  |  |
| 7 | **Ж** | О | 16 | **П** | И | 25 | **Ш** | Ф |  |  |  |
| 8 | **З** | А | 17 | **Р** | й | 26 | **Щ** | Х |  |  |  |

Зашифрованное сообщение: «ЙЬАНЕЬ ДБФЬЕМ ЖЕ КЗЕЖЕЖБЕ, Ь НЮЕЙЕЖЖЗКМШ».

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.

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

Зашифрованное сообщение: «ЫЪШЖЭ – БЗИ ХИНПЙ ЗО ПЖМГЗА ЩЙС ЫШЙД, ЧИ ПЖЪГЗА ЩЙС ШИПЧГДЪГ».

**Контрольные вопросы**

1. В чем особенность шифров простой замены?

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

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

4. Для каких шифров простой замены используется составной ключ?

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

1. Особенность шифров простой замены заключается в том, что каждый символ исходного текста заменяется на другой символ фиксированным образом, без учета контекста. Это делает такие шифры относительно простыми для анализа, поскольку частота появления символов сохраняется, что позволяет использовать статистический анализ для их взлома.

2. Отличия системы шифрования Цезаря и аффинной системы подстановок заключаются в том, что шифр Цезаря представляет собой частный случай аффинной системы, где используется только одно преобразование (сдвиг). Аффинная система подстановок включает два параметра: сдвиг (как в шифре Цезаря) и множитель, что позволяет создавать более сложные замены.

3. Требования к выбору ключей для аффинной системы подстановок заключаются в том, что множитель (a) должен быть взаимно прост с размером алфавита (например, 26 для латиницы), чтобы обеспечить возможность обратного преобразования. Сдвиг (b) может быть любым целым числом.

4. Составной ключ используется в шифрах простой замены, таких как шифр Виженера или шифр с переменной подстановкой. В этих системах ключ может состоять из нескольких символов или фраз, которые повторяются в зависимости от длины сообщения, что усложняет анализ.

5. Заполнение таблицы подстановок для шифрования с использованием системы Трисемуса происходит следующим образом: сначала создается квадратная таблица размером 5x5, в которую помещаются буквы алфавита, исключая одну букву (обычно "J", которая объединяется с "I"). Затем для заполнения таблицы используются ключевые слова или фразы, которые записываются в таблицу без повторений, после чего оставшиеся буквы добавляются в порядке их появления в алфавите.