Лабораторная работа № 1

Тема: вводное занятие. Элементарные способы защиты информации

Цель: изучить теоретические основы построения классических шифров, на практике осуществить создание ключей в классических шифрах, провести зашифрование открытого и расшифрование закрытого сообщения.

1. Теоретический вопрос

В 1936 году Вольф Фридман (позднее Уильям Фридман) американский криптограф молдавского происхождения спроектировал свою шифровальную машину M-325, также известную как SIGFOY (рис. 1).



Рисунок 1 – М-325

Машина состояла из 3х промежуточных роторов и 1 обратного, а питание обеспечивали 2 батарейки от фонарика. Ключом к шифру являлось начальное положение конкретно выбранных роторов. Имела значительно меньшое количество комбинаций в отличии от конкурентной немецкой шифровальной машины «Энигма», так как ключ ограничивался начальным положением конкретных роторов, и не содержал перестановок символов или каких-то дополнительных мер безопасности.

Несмотря на простоту в период с 1944 по 1946 года более 1100 экземпляров шифровальной машины были поставлены в иностранные службы государственного департамента США. Однако машина не прижилась, так как проблемы с качеством повлекли множество ошибок шифрования, хрупкие батарейки и лампочки мешали использованию на поле боя.

1. Ход шифрования и дешифрования

Необходимо зашифровать фразу «Куркчи Ариф Эрнестович» используя различные виды шифрования.

* 1. Атбаш

В данном методе первая буква алфавита заменяется последней, вторая предпоследней и т.д.

Итоговая фраза будет: «Флофзц Яоцк Восънмрэцз».

Для расшифровки итоговая фраза повторно подвергается преобразованию

* 1. Шифр Цезаря

Для этого метода алфавит замыкается в кольцо и сдвигается влево на количество позиций равных ключу. В шифрованном тексте буква исходного алфавита заменяется на букву, стоящую на той же позиции в смещенном алфавите.

S = 4

Итоговая фраза будет: «ОчфоьмгДфмшгАфсйхутжмь»

Для расшифровки итоговая фраза пропускается через обратный алгоритм, в котором буква смещенного алфавита заменяется на букву исходного алфавита.

* 1. Квадрат Полибия

Для преобразования этим методом достаточно расположить в квадрат буквы алфавита. Каждая буква заменяется 2 цифрами – номер строки и номер столбца ячейки, в которой находится соответствующая буква. В альтернативном варианте каждая буква заменяется находящейся под ней.

Итоговая фраза первым методом будет: «24 41 34 45 23 11 34 23 42 54 34 31 16 35 36 32 13 23 45»

Итоговая фраза вторым методом будет: «Рщцрюп Жцпы Гцумчшфипю»

Обратное преобразование производится по той же таблице, заменяя цифры на соответствующее значение в ячейке (на находящиеся над ними в таблице).

* 1. Шифр четырех квадратов

Строятся 4 квадрата 5x5 или 4x4 (в зависимости от объема алфавита). Преобразования происходят для каждой пары букв исходного текста последовательно. Первая буква пары находится в левой верхней таблице, вторая буква в правой нижней. Итоговые буквы берутся из 2х других таблиц, стоящие других вершинах прямоугольника, образованного исходными.

Итоговая фраза будет: «Рльсхо Оебп Рпццаншфхя»

Расшифровка происходит обратным способом: буквы пары находятся в правой верхней и левой нижней таблицах.

* 1. Перестановка колонок по ключу

Исходная фраза располагается в таблице, по количеству колонок которой выбирается ключ соответствующей длины (желательно без повторяющихся букв). Столбцы переставляются в соответствии с алфавитным порядком букв ключа (таблица 1).

Ключ: «идеал»

Итоговая фраза: «нестчиарифэркуркович»

Расшифровка происходит обратной перестановкой столбцов в соответствии с исходным порядком ключа.

Таблица 1 – Перестановка колонок по ключу

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| и | д | е | а | л |  | а | д | е | и | л |
| 4 | 2 | 3 | 1 | 5 | 1 | 2 | 3 | 4 | 5 |
| к | ч | и | н | о | н | ч | и | к | о |
| у | и | ф | е | в | е | и | ф | у | в |
| р | а | э | с | и | с | а | э | р | и |
| к | р | р | т | ч | т | р | р | к | ч |

* 1. Двойные перестановки

Ключами служат комбинации номеров строк и столбцов, переставленных в любом порядке. Фраза записывается в таблицу, после чего переставляются столбцы и строки (таблица 2).

Ключ столбцов: «6 2 4 10 8 1 5 9 3 7 11»

Ключ строк: «2 1»

Итоговая фраза: «сэври\_иеончиурр\_кичакф»

Расшифровка происходит обратной перестановкой строк и столбцов таблицы.

Таблица 2 – Двойные перестановки

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 6 | 2 | 4 | 10 | 8 | 1 | 5 | 9 | 3 | 7 | 11 |
| 2 | к | у | р | к | ч | и | \_ | а | р | и | ф |
| 1 | \_ | э | р | н | е | с | т | о | в | и | ч |
| Перестановка по столбцам | | | | | | | | | | | |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 2 | и | у | р | р | \_ | к | и | ч | а | к | ф |
| 1 | с | э | в | р | т | \_ | и | е | о | н | ч |
| Перестановка по строкам | | | | | | | | | | | |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 1 | с | э | в | р | т | \_ | и | е | о | н | ч |
| 2 | и | у | р | р | \_ | к | и | ч | а | к | ф |

* 1. Магический квадрат

Ключом выступает квадратная таблица n x n, заполненная числами таким образом, что сумма чисел в каждой строке, столбце и на диагоналях одинакова. Буквы записываются в квадрат, каждая в ячейку число в которой соответствует порядковому номеру буквы в исходной фразе (таблица 3).

Итоговая фраза: «кн\_асртуф\_\_ииорвкэчи\_\_ечр»

Расшифровка происходит расположением букв в порядке возрастания соответствующего числа магического квадрата.

Таблица 3 – Магический квадрат

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 15 | 24 | 8 | 17 |  | к | н | \_ | а | с |
| 9 | 18 | 2 | 11 | 25 | р | т | у | ф | \_ |
| 12 | 21 | 10 | 19 | 3 | \_ | и | и | о | р |
| 20 | 4 | 13 | 22 | 6 | в | к | э | ч | и |
| 23 | 7 | 16 | 5 | 14 | \_ | \_ | е | ч | р |

* 1. Шифр Гронсфельда

Является модификацией шифра Цезаря числовым ключом. Под сообщением циклически выписывается ключ (таблица 5). Каждая буква шифруется методом Цезаря с ключом равным цифре, написанной под буквой (таблица 4).

Ключ: «1997»

Итоговая фраза: «лэщсшсизссюжющцмтьчййа»

Расшифровка состоит в расшифровке каждой буквы методом Цезаря с ключом равным соответствующей цифре ключа.

Таблица 4 – Алфавиты для шифра Гронсфельда

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|  | а | б | в | г | д | е | ж | з | и | й | к | л | м | н | о | п |
| 1 | б | в | г | д | е | ж | з | и | й | к | л | м | н | о | п | р |
| 9 | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш |
| 7 | е | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф |
|  | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |
|  | р | с | т | у | ф | х | ц | ч | ш | щ | ы | ь | э | ю | я | \_ |
| 1 | с | т | у | ф | х | ц | ч | ш | щ | ы | ь | э | ю | я | \_ | а |
| 9 | щ | ы | ь | э | ю | я | \_ | а | б | в | г | д | е | ж | з | и |
| 7 | х | ц | ч | ш | щ | ы | ь | э | ю | я | \_ | а | б | в | г | д |

Таблица 5 – Исходный текст и ключ

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| к | у | р | к | ч | и | \_ | а | р | и | ф | \_ | э | р | н | е | с | т | о | в | и | ч |
| 1 | 9 | 9 | 7 | 1 | 9 | 9 | 7 | 1 | 9 | 9 | 7 | 1 | 9 | 9 | 7 | 1 | 9 | 9 | 7 | 1 | 9 |

* 1. Шифрующие таблицы

Ключом выбирается слово, желательно не содержащее повторяющихся букв алфавита (иначе они пропускаются). Ключ записывается по строкам в таблицу, которая потом дополняется недостающими буквами алфавита (таблица 6). Аналогично методу Полибия каждая буква заменяется стоящей под ней.

Ключ: «монархия»

Итоговая фраза: «ФыгфюеВгеьРгбсшщякею»

Расшифровка состоит в соответствующей замене букв на стоящую над ней в таблице.

Таблица 6 – Шифрующая таблица

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | м | о | н | а | р | х |
| 2 | и | я | б | в | г | д |
| 3 | е | ж | з | к | л | п |
| 4 | с | т | у | ф | ц | ч |
| 5 | ш | щ | ы | ь | э | ю |

* 1. Биграмные шифры

Ключ и таблица (таблица 6) строятся также как и в предыдущем методе. Шифрование происходит для пар букв в соответствии с 4 правилами.

Ключ: «монархия»

Итоговая фраза «зф ал сд рх вс рг мз ту ая дс»

Расшифровка состоит в замене пар по обратным правилам (смещения направо/вниз заменяются на смещения влево/вверх, обратные углы прямоугольника).

* 1. Шифр Уитстона

Составляются 2 таблицы по разным ключам методом составления шифрующих таблиц (таблицы 6 и 7). Первая буква из пары находится в первой таблице, вторая во второй и они парой заменяются на буквы, стоящие на других углах прямоугольника.

Ключи: «монархия» и «маруся»

Итоговая фраза: «ла рл тп со дс щр сб пт ая бш»

Расшифровка состоит в попарной букв замене по обратным правилам.

Таблица 7 – Шифрующая таблица

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | м | а | р | у | с | я |
| 2 | б | в | г | д | е | ж |
| 3 | з | и | к | л | н | о |
| 4 | п | т | у | ф | х | ц |
| 5 | ч | ш | щ | ь | э | ю |

* 1. Шифр ADFGX

Ключом в данном методе выступает таблица 5x5 или 6x6 столбцы и строки которой подписаны соответственно ADFGX или ADFGVX соответственно. Каждая буква исходной фразы кодируется 2 буквами: буква строки и буква столбца (таблица 8). Дополнительно вводится ключ перестановки столбцов. Код записывается посимвольно в таблицу с количеством столбцов равным количеству символов в ключе. Столбцы переставляются в соответствии с алфавитным порядком букв ключа (таблица 9).

Ключ перестановки: «идеал»

Итоговая фраза: «DV AA GG FV AD FF XA GD AF AG AD GX VV DF DG AF DG FG AF VD»

Расшифровка требует обратной перестановки столбцов по ключу перестановки и последующей подстановке значений из соответствующих ячеек таблицы ADFGX/ADFGVX.

Таблица 8 – ADFGVX таблица

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

Таблица 9 – Перестановка столбцов

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| и | д | е | а | л |  | а | д | е | и | л |
| 4 | 2 | 3 | 1 | 5 | 1 | 2 | 3 | 4 | 5 |
| A | V | A | D | G | D | V | A | A | G |
| A | A | V | G | D | G | A | V | A | D |
| A | F | X | F | G | F | F | X | A | G |
| A | A | F | D | G | D | A | F | A | G |
| X | D | G | A | V | A | D | G | X | V |
| D | D | F | V | G | V | D | F | D | G |
| G | F | D | A | F | A | F | D | G | F |
| V | A | F | G | D | G | A | F | V | D |

* 1. Шифр замены небуквенными символами

Для этого шифра необходимо сопоставить каждому символу исходного алфавита любой, не встречающийся ранее, небуквенный символ. (таблица 10).

Ключ: «÷ ≤ ћ ѓ ∆ † … ‘ ! @ ® љ µ њ ° © ₽ ≠ ™ ќ ƒ “ џ ≈ ѕ ў # ~ $ ≥ ђ»

Итоговая фраза: «®ќ₽®≈! ÷₽!ƒ $₽њ†≠™°ћ!≈»

Расшифровка состоит в обратной замене по таблице алфавитов.

Таблица 10 – Небуквенный алфавит

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| а | б | в | г | д | е | ж | з | и | й | к | л | м | н | о | п |
| ÷ | ≤ | ћ | ѓ | ∆ | † | … | ‘ | ! | @ | ® | љ | µ | њ | ° | © |
| 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |  |
| р | с | т | у | ф | х | ц | ч | ш | щ | ы | ь | э | ю | я |  |
| ₽ | ≠ | ™ | ќ | ~~ƒ~~ | “ | џ | ≈ | ѕ | ў | # | ~ | $ | ≥ | ђ |  |

Выводы

В ходе выполнения лабораторной работы были изучены классические шифры. Было проведено шифрование ФИО, а также описан алгоритм дешифрования для каждого приведенного метода. В качестве теоретического вопроса была рассмотрена шифровальная машина «М-325».